

Cisco Prime Network 3.9 Reference Guide

June 13, 2012

Americas Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
http://www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 527-0883

Text Part Number: OL-26499-01

THE SPECIFICATIONS AND INFORMATION REGARDING THE PRODUCTS IN THIS MANUAL ARE SUBJECT TO CHANGE WITHOUT NOTICE. ALL STATEMENTS, INFORMATION, AND RECOMMENDATIONS IN THIS MANUAL ARE BELIEVED TO BE ACCURATE BUT ARE PRESENTED WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED. USERS MUST TAKE FULL RESPONSIBILITY FOR THEIR APPLICATION OF ANY PRODUCTS.

THE SOFTWARE LICENSE AND LIMITED WARRANTY FOR THE ACCOMPANYING PRODUCT ARE SET FORTH IN THE INFORMATION PACKET THAT SHIPPED WITH THE PRODUCT AND ARE INCORPORATED HEREIN BY THIS REFERENCE. IF YOU ARE UNABLE TO LOCATE THE SOFTWARE LICENSE OR LIMITED WARRANTY, CONTACT YOUR CISCO REPRESENTATIVE FOR A COPY.

The Cisco implementation of TCP header compression is an adaptation of a program developed by the University of California, Berkeley (UCB) as part of UCB's public domain version of the UNIX operating system. All rights reserved. Copyright © 1981, Regents of the University of California.

NOTWITHSTANDING ANY OTHER WARRANTY HEREIN, ALL DOCUMENT FILES AND SOFTWARE OF THESE SUPPLIERS ARE PROVIDED "AS IS" WITH ALL FAULTS. CISCO AND THE ABOVE-NAMED SUPPLIERS DISCLAIM ALL WARRANTIES, EXPRESSED OR IMPLIED, INCLUDING, WITHOUT LIMITATION, THOSE OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT OR ARISING FROM A COURSE OF DEALING, USAGE, OR TRADE PRACTICE.

IN NO EVENT SHALL CISCO OR ITS SUPPLIERS BE LIABLE FOR ANY INDIRECT, SPECIAL, CONSEQUENTIAL, OR INCIDENTAL DAMAGES, INCLUDING, WITHOUT LIMITATION, LOST PROFITS OR LOSS OR DAMAGE TO DATA ARISING OUT OF THE USE OR INABILITY TO USE THIS MANUAL, EVEN IF CISCO OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: www.cisco.com/go/trademarks. Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1110R)

Any Internet Protocol (IP) addresses and phone numbers used in this document are not intended to be actual addresses and phone numbers. Any examples, command display output, network topology diagrams, and other figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses or phone numbers in illustrative content is unintentional and coincidental.

Cisco Prime Network 3.9 Reference Guide
© 1999-2012 Cisco Systems, Inc. All rights reserved.



CONTENTS

Preface xxxi

New and Changed Information xxxi

Audience xxxi

Document Organization xxxii

Conventions xxxii

Related Documentation xxxiii

Obtaining Documentation and Submitting a Service Request xxxiii

PART 1 **Cisco VNEs**

CHAPTER 1 **Introduction** 1-1

Introduction to VNEs 1-1

Understanding the Tables 1-1

Software Versions 1-2

Product Versions 1-3

Expedite Legend 1-3

CHAPTER 2 **Overview—Supported Network Elements in Cisco Prime Network 3.9** 2-1

Supported Generic Devices in Cisco Prime Network 3.9 2-1

Supported Cisco DataCentre in Cisco Prime Network 3.9 2-1

Supported Cisco Optical Transport in Cisco Prime Network 3.9 2-2

Supported Cisco Security Appliances in Cisco Prime Network 3.9 2-2

Supported Cisco Access Servers in Cisco Prime Network 3.9 2-3

Supported Cisco Gateways in Cisco Prime Network 3.9 2-3

Supported Cisco Routers in Cisco Prime Network 3.9 2-3

Supported Cisco Switches in Cisco Prime Network 3.9 2-13

CHAPTER 3 **Support Information for Cisco Security Appliances** 3-1

Cisco Adaptive Security Appliance 5550 Series 3-1

Cisco ASA 5550 Series—Supported Software Versions 3-1

Cisco ASA 5550 Series—Supported Topologies 3-2

Cisco ASA 5550 Series—Supported Modules 3-2

Cisco ASA 5550 Series—Supported Technologies 3-2

Cisco ASA 5550 Series—Supported Service Events 3-2
Cisco Adaptive Security Appliance 5580 Series 3-3
Cisco ASA 5580 Series—Supported Software Versions 3-3
Cisco ASA 5580 Series—Supported Topologies 3-4
Cisco ASA 5580 Series—Supported Modules 3-4
Cisco ASA 5580 Series—Supported Technologies 3-4
Cisco ASA 5580 Series—Supported Service Events 3-4
Supported Technologies on Cisco Security Appliances 3-5
IP 3-6
Ethernet 3-9
Hardware 3-14
Serial 3-16

CHAPTER 4 **Support Information for Cisco Access Servers** 4-1
Cisco Access Server 5800 Series 4-1
Cisco AS 5800 Series—Supported Software Versions 4-1
Cisco AS 5800 Series—Supported Topologies 4-2
Cisco AS 5800 Series—Supported Modules 4-2
Cisco AS 5800 Series—Supported Technologies 4-2
Cisco AS 5800 Series—Supported Service Events 4-3
Supported Technologies on Cisco Access Servers 4-3
IP 4-4
Routing Protocols 4-7
Ethernet 4-9
TDM/DSx 4-14
Security 4-17
Hardware 4-18
Serial 4-20

CHAPTER 5 **Support Information for Cisco Gateways** 5-1
Cisco AS5300 Series Universal Gateways 5-1
Cisco AS5300 Series—Supported Software Versions 5-1
Cisco AS5300 Series—Supported Topologies 5-2
Cisco AS5300 Series—Supported Modules 5-2
Cisco AS5300 Series—Supported Technologies 5-2
Cisco AS5300 Series—Supported Service Events 5-3
Supported Technologies on Cisco Gateways 5-3
IP 5-4
Ethernet 5-7

Security 5-12
Hardware 5-12
Serial 5-15
CDP 5-16
Discovery Protocol 5-16

CHAPTER 6 **Support Information for Cisco Routers** 6-1

Cisco 800 Series Routers 6-2
Cisco 800 Series—Supported Software Versions 6-2
Cisco 800 Series—Supported Topologies 6-2
Cisco 800 Series—Supported Technologies 6-3
Cisco 800 Series—Supported Service Events 6-3
Cisco 1000 Series Routers 6-3
Cisco 1000 Series—Supported Software Versions 6-4
Cisco 1000 Series—Supported Topologies 6-4
Cisco 1000 Series—Supported Technologies 6-4
Cisco 1000 Series—Supported Service Events 6-5
Cisco 1600 Series Routers 6-6
Cisco 1600 Series—Supported Software Versions 6-6
Cisco 1600 Series—Supported Topologies 6-6
Cisco 1600 Series—Supported Technologies 6-7
Cisco 1600 Series—Supported Service Events 6-7
Cisco 1700 Series Modular Access Routers 6-8
Cisco 1700 Series—Supported Software Versions 6-9
Cisco 1700 Series—Supported Topologies 6-9
Cisco 1700 Series—Supported Modules 6-9
Cisco 1700 Series—Supported Technologies 6-10
Cisco 1700 Series—Supported Service Events 6-11
Cisco 1800 Series Integrated Services Routers 6-12
Cisco 1800 Series—Supported Software Versions 6-12
Cisco 1800 Series—Supported Topologies 6-12
Cisco 1800 Series—Supported Modules 6-13
Cisco 1800 Series—Supported Technologies 6-14
Cisco 1800 Series—Supported Service Events 6-14
Cisco 2500 Series Routers 6-15
Cisco 2500 Series—Supported Software Versions 6-15
Cisco 2500 Series—Supported Topologies 6-15
Cisco 2500 Series—Supported Modules 6-16
Cisco 2500 Series—Supported Technologies 6-16

Cisco 2500 Series—Supported Service Events 6-16
Cisco 2600 Series Multiservice Platform Routers 6-18
Cisco 2600 Series—Supported Software Versions 6-18
Cisco 2600 Series—Supported Topologies 6-19
Cisco 2600 Series—Supported Modules 6-19
Cisco 2600 Series—Supported Technologies 6-20
Cisco 2600 Series—Supported Service Events 6-21
Cisco 2800 Series Integrated Services Routers 6-22
Cisco 2800 Series—Supported Software Versions 6-22
Cisco 2800 Series—Supported Topologies 6-23
Cisco 2800 Series—Supported Modules 6-23
Cisco 2800 Series—Supported Technologies 6-25
Cisco 2800 Series—Supported Service Events 6-26
Cisco 3600 Series Multiservice Platform Routers 6-27
Cisco 3600 Series—Supported Software Versions 6-27
Cisco 3600 Series—Supported Topologies 6-28
Cisco 3600 Series—Supported Modules 6-28
Cisco 3600 Series—Supported Technologies 6-28
Cisco 3600 Series—Supported Service Events 6-29
Cisco 3700 Series Multiservice Access Routers 6-29
Cisco 3700 Series—Supported Software Versions 6-29
Cisco 3700 Series—Supported Topologies 6-30
Cisco 3700 Series—Supported Modules 6-30
Cisco 3700 Series—Supported Technologies 6-31
Cisco 3700 Series—Supported Service Events 6-31
Cisco 3800 Series Integrated Services Routers 6-32
Cisco 3800 Series—Supported Software Versions 6-33
Cisco 3800 Series—Supported Topologies 6-33
Cisco 3800 Series—Supported Modules 6-34
Cisco 3800 Series—Supported Technologies 6-35
Cisco 3800 Series—Supported Service Events 6-36
Cisco 7200 Series Routers 6-36
Cisco 7200 Series—Supported Software Versions 6-37
Cisco 7200 Series—Supported Topologies 6-40
Cisco 7200 Series—Supported Modules 6-40
Cisco 7200 Series—Supported Technologies 6-43
Cisco 7200 Series—Supported Service Events 6-44
Cisco 7300 Series Routers 6-45
Cisco 7300 Series—Supported Software Versions 6-46

Cisco 7300 Series—Supported Topologies 6-48
Cisco 7300 Series—Supported Modules 6-48
Cisco 7300 Series—Supported Technologies 6-48
Cisco 7300 Series—Supported Service Events 6-49
Cisco 7400 Series Routers 6-49
Cisco 7400 Series—Supported Software Versions 6-50
Cisco 7400 Series—Supported Topologies 6-51
Cisco 7400 Series—Supported Modules 6-51
Cisco 7400 Series—Supported Technologies 6-52
Cisco 7400 Series—Supported Service Events 6-53
Cisco 7500 Series Routers 6-54
Cisco 7500 Series—Supported Software Versions 6-54
Cisco 7500 Series—Supported Topologies 6-56
Cisco 7500 Series—Supported Modules 6-56
Cisco 7500 Series—Supported Technologies 6-56
Cisco 7500 Series—Supported Service Events 6-57
Cisco 7600 Series Routers 6-57
Cisco 7600 Series—Supported Software Versions 6-58
Cisco 7600 Series—Supported Topologies 6-60
Cisco 7600 Series—Supported Modules 6-61
Cisco 7600 Series—Supported Technologies 6-77
Cisco 7600 Series—Supported Service Events 6-78
Cisco 10000 Series Routers 6-81
Cisco 10000 Series—Supported Software Versions 6-81
Cisco 10000 Series—Supported Topologies 6-82
Cisco 10000 Series—Supported Modules 6-82
Cisco 10000 Series—Supported Technologies 6-83
Cisco 10000 Series—Supported Service Events 6-84
Cisco 12000 Series Routers 6-85
Cisco 12000 Series—Supported Software Versions 6-85
Cisco 12000 Series—Supported Topologies 6-86
Cisco 12000 Series—Supported Modules 6-87
Cisco 12000 Series—Supported Technologies 6-92
Cisco 12000 Series—Supported Service Events 6-93
Cisco XR 12000 Series Routers 6-95
Cisco XR 12000 Series—Supported Software Versions 6-95
Cisco XR 12000 Series—Supported Topologies 6-96
Cisco XR 12000 Series—Supported Modules 6-97
Cisco XR 12000 Series—Supported Technologies 6-103

Cisco XR 12000 Series—Supported Service Events 6-104
Cisco CRS Carrier Routing System 6-106
Cisco CRS—Supported Software Versions 6-106
Cisco CRS—Supported Topologies 6-107
Cisco CRS—Supported Modules 6-108
Cisco CRS—Supported Technologies 6-118
Cisco CRS—Supported Service Events 6-119
Cisco CRS—Additional Information 6-120
Cisco Carrier Routing System (CRS) Prerequisite 6-120
SDR Support for CRS 6-120
Multichassis Support for CRS 6-121
Cisco ASR 9000 Series Aggregation Services Routers 6-121
Cisco ASR 9000—Supported Software Versions 6-121
Cisco ASR 9000—Supported Topologies 6-122
Cisco ASR 9000—Supported Modules 6-122
Cisco ASR 9000—Supported Technologies 6-132
Cisco ASR 9000—Supported Service Events 6-132
Cisco ASR 1000 Series Routers 6-134
Cisco ASR 1000 Series—Supported Software Versions 6-134
Cisco ASR 1000 Series—Supported Topologies 6-135
Cisco ASR 1000 Series—Supported Modules 6-136
Cisco ASR 1000 Series—Supported Technologies 6-142
Cisco ASR 1000 Series—Supported Service Events 6-142
Cisco MWR 2900 Series Mobile Wireless Routers 6-143
Cisco MWR 2941—Supported Software Versions 6-143
Cisco MWR 2941—Supported Topologies 6-145
Cisco MWR 2941—Supported Modules 6-145
Cisco MWR 2941—Supported Technologies 6-148
Cisco MWR 2941—Supported Service Events 6-149
Cisco 1900 Series Integrated Services Router 6-151
Cisco ISR 1900 Series—Supported Software Versions 6-151
Cisco ISR 1900 Series—Supported Topologies 6-152
Cisco ISR 1900 Series—Supported Modules 6-152
Cisco ISR 1900 Series—Supported Technologies 6-152
Cisco ISR 1900 Series—Supported Service Events 6-153
Cisco 2900 Series Integrated Services Router 6-154
Cisco ISR 2900 Series—Supported Software Versions 6-155
Cisco ISR 2900 Series—Supported Topologies 6-155
Cisco ISR 2900 Series—Supported Modules 6-155

Cisco ISR 2900 Series—Supported Technologies 6-156
Cisco ISR 2900 Series—Supported Service Events 6-157
Cisco 3900 Series Integrated Service Routers 6-158
Cisco ISR 3900 Series—Supported Software Versions 6-158
Cisco ISR 3900 Series—Supported Topologies 6-159
Cisco ISR 3900 Series—Supported Modules 6-159
Cisco ISR 3900 Series—Supported Technologies 6-160
Cisco ISR 3900 Series—Supported Service Events 6-160
Cisco Universal Broadband Router 7200 Series 6-161
Cisco UBR7200 Series—Supported Software Versions 6-162
Cisco UBR7200 Series—Supported Topologies 6-162
Cisco UBR7200 Series—Supported Modules 6-162
Cisco UBR7200 Series—Supported Technologies 6-163
Cisco UBR7200 Series—Supported Service Events 6-163
Cisco Univeral Broadband Router 10000 Series 6-165
Cisco UBR10000 Series—Supported Software Versions 6-165
Cisco UBR10000 Series—Supported Topologies 6-165
Cisco UBR10000 Series—Supported Modules 6-165
Cisco UBR10000 Series—Supported Technologies 6-166
Cisco UBR10000 Series—Supported Service Events 6-167
Cisco 4700 Series Routers 6-168
Cisco 4700 Series—Supported Topologies 6-168
Cisco 4700 Series—Supported Technologies 6-169
Cisco 4700 Series—Supported Service Events 6-169
Cisco ASR901 Series Mobile Wireless Routers 6-170
Cisco ASR901—Supported Software Versions 6-171
Cisco ASR901—Supported Topologies 6-171
Cisco ASR901—Supported Modules 6-173
Cisco ASR901—Supported Technologies 6-181
Cisco ASR901—Supported Service Events 6-182
Cisco ASR903 Series Routers 6-185
Cisco ASR903 Series—Supported Software Versions 6-185
Cisco ASR903 Series—Supported Topologies 6-186
Cisco ASR903 Series—Supported Modules 6-186
Cisco ASR903 Series—Supported Technologies 6-189
Cisco ASR903 Series—Supported Service Events 6-189
Cisco ASR 5000 Series Routers 6-196
Cisco ASR 5000 Series—Supported Software Versions 6-196
Cisco ASR 5000 Series—Supported Topologies 6-196

Cisco ASR 5000 Series—Supported Modules 6-197
Cisco ASR 5000 Series—Supported Technologies 6-197
Supported Technologies on Cisco Routers 6-198
IP 6-199
Routing Protocols 6-202
Ethernet 6-205
ATM 6-213
Frame Relay 6-217
PPP 6-219
HDLC 6-220
SONET/SDH 6-220
TDM/DSx 6-222
MPLS 6-226
MPLS-TE 6-228
MPLS-TP 6-231
VPN (VRF) 6-233
PWE3 6-235
Security 6-237
Hardware 6-238
Serial 6-242
Additional Technologies 6-243
IPoDWDM 6-243
LocalSwitching 6-245
BFD 6-246
Carrier Ethernet 6-247
CDP 6-249
Discovery Protocol 6-249
Ethernet OAM 6-250
CGN 6-254
SBC 6-256
AccessGatewayService 6-262
6PE 6-264
6rd 6-264
MLACP 6-265
IPSec 6-266
Mobile 6-266

CHAPTER 7 **Support Information for Cisco Switches** 7-1
Cisco Catalyst 1900 Series Switches 7-2

Catalyst 1900—Supported Software Versions 7-2
Catalyst 1900—Supported Topologies 7-2
Catalyst 1900—Supported Technologies 7-2
Catalyst 1900—Supported Service Events 7-3
Cisco Catalyst 2900 Series Switches 7-3
Cisco Catalyst 2900 Series—Supported Software Versions 7-4
Cisco Catalyst 2900 Series—Supported Topologies 7-4
Cisco Catalyst 2900 Series—Supported Modules 7-4
Cisco Catalyst 2900 Series—Supported Technologies 7-5
Cisco Catalyst 2900 Series—Supported Service Events 7-5
Cisco ME 3400 Series Ethernet Access Switches 7-6
Cisco ME 3400 Series—Supported Software Versions 7-6
Cisco ME 3400 Series—Supported Topologies 7-7
Cisco ME 3400 Series—Supported Modules 7-7
Cisco ME 3400 Series—Supported Technologies 7-8
Cisco ME 3400 Series—Supported Service Events 7-9
Cisco Catalyst 3500 XL Series Switches 7-9
Cisco Catalyst 3500 XL Series—Supported Software Versions 7-10
Cisco Catalyst 3500 XL Series—Supported Topologies 7-10
Cisco Catalyst 3500 XL Series—Supported Modules 7-10
Cisco Catalyst 3500 XL Series—Supported Technologies 7-10
Cisco Catalyst 3500 XL Series—Supported Service Events 7-11
Cisco Catalyst 3550 Series Switches 7-12
Cisco Catalyst 3550 Series—Supported Software Versions 7-12
Cisco Catalyst 3550 Series—Supported Topologies 7-12
Cisco Catalyst 3550 Series—Supported Technologies 7-13
Cisco Catalyst 3550 Series—Supported Service Events 7-13
Cisco Catalyst 3560 Series Switches 7-14
Cisco Catalyst 3560 Series—Supported Software Versions 7-14
Cisco Catalyst 3560 Series—Supported Topologies 7-15
Cisco Catalyst 3560 Series—Supported Modules 7-15
Cisco Catalyst 3560 Series—Supported Technologies 7-16
Cisco Catalyst 3560 Series—Supported Service Events 7-16
Cisco Catalyst 3750 Series Switches 7-17
Cisco 3750 Series—Supported Software Versions 7-17
Cisco 3750 Series—Supported Topologies 7-18
Cisco 3750 Series—Supported Modules 7-18
Cisco 3750 Series—Supported Technologies 7-18
Cisco 3750 Series—Supported Service Events 7-19

Cisco Catalyst 3750 Metro Series Switches 7-19
Cisco Catalyst 3750 Metro Series—Supported Software Versions 7-20
Cisco Catalyst 3750 Metro Series—Supported Topologies 7-20
Cisco Catalyst 3750 Metro Series—Supported Modules 7-21
Cisco Catalyst 3750 Metro Series—Supported Technologies 7-21
Cisco Catalyst 3750 Metro Series—Supported Service Events 7-22
Cisco Catalyst 4000 Series Switches 7-22
Cisco Catalyst 4000 Series—Supported Software Versions 7-23
Cisco Catalyst 4000 Series—Supported Topologies 7-23
Cisco Catalyst 4000 Series—Supported Modules 7-23
Cisco Catalyst 4000 Series—Supported Technologies 7-25
Cisco Catalyst 4000 Series—Supported Service Events 7-25
Cisco Catalyst 4500 Series Switches 7-26
Cisco Catalyst 4500 Series—Supported Software Versions 7-26
Cisco Catalyst 4500 Series—Supported Topologies 7-27
Cisco Catalyst 4500 Series—Supported Modules 7-28
Cisco Catalyst 4500 Series—Supported Technologies 7-32
Cisco Catalyst 4500 Series—Supported Service Events 7-33
Cisco Catalyst 4900 Series Switches 7-34
Cisco Catalyst 4900 Series—Supported Software Versions 7-34
Cisco Catalyst 4900 Series—Supported Topologies 7-35
Cisco Catalyst 4900 Series—Supported Modules 7-35
Cisco Catalyst 4900 Series—Supported Technologies 7-40
Cisco Catalyst 4900 Series—Supported Service Events 7-41
Cisco ME 4900 Series Ethernet Switch 7-43
Cisco 4924 ME—Supported Software Versions 7-44
Cisco 4924 ME—Supported Topologies 7-44
Cisco 4924 ME—Supported Modules 7-44
Cisco 4924 ME—Supported Technologies 7-46
Cisco 4924 ME—Supported Service Events 7-46
Cisco Catalyst 5000 Series Switches 7-49
Cisco 5000 Series—Supported Software Versions 7-50
Cisco 5000 Series—Supported Topologies 7-50
Cisco 5000 Series—Supported Technologies 7-50
Cisco 5000 Series—Supported Service Events 7-50
Cisco Catalyst 6500 Series (CatOS) Switches 7-51
Cisco Catalyst 6500 Series (CatOS)—Supported Software Versions 7-51
Cisco Catalyst 6500 Series (CatOS)—Supported Topologies 7-52
Cisco Catalyst 6500 Series (CatOS)—Supported Modules 7-52

Cisco Catalyst 6500 Series (CatOS)—Supported Technologies 7-55
Cisco Catalyst 6500 Series (CatOS)—Supported Service Events 7-55
Cisco Catalyst 6500 Series (IOS) Switches 7-56
Cisco Catalyst 6500 Series (IOS)—Supported Software Versions 7-56
Cisco Catalyst 6500 Series (IOS)—Supported Topologies 7-57
Cisco Catalyst 6500 Series (IOS)—Supported Modules 7-58
Cisco Catalyst 6500 Series (IOS)—Supported Technologies 7-65
Cisco Catalyst 6500 Series (IOS)—Supported Service Events 7-66
Cisco ME 6500 Series Ethernet Switches (6524) 7-69
Cisco ME 6500 Series (6524)—Supported Software Versions 7-70
Cisco ME 6500 Series (6524)—Supported Topologies 7-70
Cisco ME 6500 Series (6524)—Supported Modules 7-70
Cisco ME 6500 Series (6524)—Supported Technologies 7-71
Cisco ME 6500 Series (6524)—Supported Service Events 7-71
Cisco ME 3600X Ethernet Access Switch 7-72
Cisco ME 3600X—Supported Software Versions 7-72
Cisco ME 3600X—Supported Topologies 7-72
Cisco ME 3600X—Supported Modules 7-73
Cisco ME 3600X—Supported Technologies 7-74
Cisco ME 3600X—Supported Service Events 7-74
Cisco ME 3800X Carrier Ethernet Switches 7-75
Cisco ME 3800X—Supported Software Versions 7-75
Cisco ME 3800X—Supported Topologies 7-76
Cisco ME 3800X—Supported Modules 7-76
Cisco ME 3800X—Supported Technologies 7-77
Cisco ME 3800X—Supported Service Events 7-78
Cisco Nexus 7000 Series Switches 7-78
Cisco Nexus 7000—Supported Software Versions 7-79
Cisco Nexus 7000—Supported Topologies 7-79
Cisco Nexus 7000—Supported Modules 7-79
Cisco Nexus 7000—Supported Technologies 7-80
Cisco Nexus 7000—Supported Service Events 7-81
Cisco Nexus 5000 Series Switches 7-81
Cisco Nexus 5000—Supported Software Versions 7-82
Cisco Nexus 5000—Supported Topologies 7-82
Cisco Nexus 5000—Supported Modules 7-82
Cisco Nexus 5000—Supported Technologies 7-83
Cisco Nexus 5000—Supported Service Events 7-83
Cisco Nexus 1000 Series Switches 7-84

Cisco Nexus 1000v—Supported Software Versions 7-84
Cisco Nexus 1000v—Supported Modules 7-85
Cisco Nexus 1000v—Supported Technologies 7-85
Cisco ACE 4700 Series Access Control Engine 7-85
Cisco ACE 4700—Supported Software Versions 7-86
Cisco ACE 4700—Supported Topologies 7-86
Cisco ACE 4700—Supported Technologies 7-86
Cisco ACE 4700—Supported Service Events 7-86
Cisco Service Control Engines 7-90
Cisco SCE—Supported Topologies 7-91
Cisco SCE—Supported Technologies 7-91
Cisco SCE—Supported Service Events 7-91
Supported Technologies on Cisco Switches 7-92
IP 7-92
Routing Protocols 7-96
Ethernet 7-99
ATM 7-105
Frame Relay 7-108
PPP 7-110
HDLC 7-111
SONET/SDH 7-111
TDM/DSx 7-112
MPLS 7-116
MPLS-TE 7-118
VPN (VRF) 7-120
PWE3 7-121
Security 7-122
Hardware 7-124
Serial 7-127
Additional Technologies 7-128
LocalSwitching 7-128
BFD 7-129
Carrier Ethernet 7-129
LLDP 7-131
CDP 7-132
Discovery Protocol 7-132
Ethernet OAM 7-133

CHAPTER 8 **Support Information for Cisco Optical Transport** 8-1

Cisco Carrier Packet Transport Series Devices 8-1

Cisco CPT Devices—Supported Software Versions 8-1

Cisco CPT Devices—Supported Topologies 8-2

Cisco CPT Devices—Supported Modules 8-2

Cisco CPT Devices—Supported Technologies 8-6

Cisco CPT Devices—Supported Service Events 8-7

Supported Technologies on Cisco Optical Transport 8-8

IP 8-8

Routing Protocols 8-11

Ethernet 8-13

MPLS 8-18

MPLS-TE 8-20

MPLS-TP 8-22

PWE3 8-24

Security 8-25

Hardware 8-26

Serial 8-28

BFD 8-29

Carrier Ethernet 8-30

CDP 8-31

Discovery Protocol 8-31

Ethernet OAM 8-31

CHAPTER 9 **Support Information for Cisco DataCentre** 9-1

Cisco UCS 61xx Series Switches 9-1

CiscoUCS 6120—Supported Software Versions 9-1

CiscoUCS 6120—Supported Modules 9-2

CiscoUCS 6120—Supported Technologies 9-3

CiscoUCS 6120—Supported Service Events 9-3

Supported Technologies on Cisco DataCentre 9-4

IP 9-5

Hardware 9-8

CDP 9-11

CHAPTER 10 **Support Information for Generic Devices** 10-1

Understanding the Generic VNE 10-1

Physical Inventory Model 10-2

Logical Inventory Model 10-2

Generic VNE—Supported Traps 10-3
Generic VNE—Supported Events 10-4
Generic VNE Limitations 10-4
Generic VNE—Supported Technologies 10-4
Generic VNE—Supported Service Events 10-4
Supported Technologies on Generic Devices 10-5
IP 10-5
Ethernet 10-8
Hardware 10-13
Serial 10-15

PART 2 Technology Support

CHAPTER 11 Supported Technologies 11-1

CHAPTER 12 Prime Network VNE Topology 12-1
Supported Topology Types 12-1
ATM 12-2
BFD 12-2
BGP 12-2
Business 12-2
Ethernet 12-2
LAG 12-3
Frame Relay 12-3
MPLS 12-4
PPP or HDLC 12-4
MLPPP 12-4
VLAN 12-4
Physical Layer 12-5
Pseudowire 12-5
GRE Tunnel 12-5
VPN 12-5
VLAN Service Links 12-6
MPLS-TE Tunnel 12-6
MPLS-TP Tunnel 12-6
Discovery Techniques 12-6
ATM VC Counters 12-7
Same Active VCs 12-7
VC Traffic Signature 12-7

CDP (Cisco Discovery Protocol) 12-8
LLDP (Link Layer Discovery Protocol) 12-8
PNNI Information 12-8
BFD Session Source and Destination 12-8
BGP Information 12-8
MAC 12-8
REP 12-9
LACP 12-9
OAM 12-9
MLPPP Endpoint Identifier 12-9
GRE Tunnel Information 12-9
Pseudowire Information 12-9
VLAN ID Matching 12-10
Route Targets 12-10
Physical Layer Counters 12-10
IP Testing 12-10
STP (Spanning Tree Protocol) 12-11

PART 3 **Alarms and Events**

CHAPTER 13 **System Events** 13-1

CHAPTER 14 **Security Events** 14-1

CHAPTER 15 **Service Alarms** 15-1

Service Alarms 15-2
Adaptive Polling 15-4
All IP Interfaces Down 15-5
ATM IMA Service 15-5
BFD Connectivity Down 15-6
BFD Neighbor Loss 15-6
BGP Link Down 15-7
BGP Neighbor Loss 15-9
BGP Process Down 15-10
Broken LSP Discovered 15-11
Card Down 15-14
Card Out 15-14
CFM Domain Fault 15-15
Carrier Grade NAT Translations Create Rate 15-16

Carrier Grade NAT Translations Delete Rate 15-17
Carrier Grade NAT Inside-to-Outside Forward Rate 15-18
Carrier Grade NAT Outside-to-Inside Forward Rate 15-18
Carrier Grade NAT Inside-to-Outside Drops Port Limit Exceeded 15-19
Carrier Grade NAT Inside-to-Outside Drops System Limit Reached 15-20
Carrier Grade NAT Inside-to-Outside Drops Resource Depletion 15-21
Chassis Disconnected 15-22
Cloud Problem 15-22
Component Unreachable 15-23
CPU Utilization 15-26
Device Unsupported 15-27
Discard Packets 15-27
Dropped Packets 15-28
DS0 Bundle Service Alarm 15-29
DS1 Path Link Down 15-29
DS1 Path Port Down 15-30
DS3 Path Link Down 15-30
DS3 Path Port Down 15-31
Dual Stack IP Changed 15-31
DWDM Controller Down 15-32
DWDM G709 Status Down 15-32
EFP Down 15-33
ESMC Process Down 15-33
Fan-Tray Down 15-34
Fan-Tray Out 15-34
GRE Keepalive 15-35
GRE Tunnel Down 15-35
HSRP Group Status Changed 15-36
Interface Status 15-37
Investigation State 15-39
L2TP Peer Not Established 15-39
L2TP Sessions Threshold 15-40
Lag Down 15-41
Lag Link Down 15-41
Layer 2 Tunnel Down 15-42
LDP Neighbor Loss 15-43
Link Down 15-44
Link Utilization 15-45
Log Archive is Disabled on the Device 15-45
Local Switching Down 15-46

Logical Port Down 15-46
LSP Down 15-47
Members Changed 15-48
Memory Utilization 15-49
MLPPP Bundle 15-49
MPLS Black Hole Found 15-50
MPLS TP Bandwidth Mismatch 15-51
MPLS Interface Removed 15-51
MPLS TE FRR State Changed 15-52
MPLS TE Tunnel Down 15-53
MPLS TP Tunnel Down 15-54
Network-Clock Synchronization 15-55
OSPF Neighbor State Change 15-56
Port Down 15-56
Power Supply Down 15-57
Power Supply Out 15-57
Pluggable Transceiver Out 15-58
REP Port Role Change 15-58
Rx Dormant 15-59
Rx Utilization 15-60
Shelf Out 15-60
SONET Path Link Down 15-61
SONET Path Port Down 15-62
Subinterface Down 15-62
Tx Dormant 15-63
Tx Utilization 15-64
VSI Down 15-64
Registry Parameters 15-65
Adaptive Polling 15-67
All IP Interfaces Down 15-69
ATM IMA Down 15-70
BFD Connectivity Down 15-74
BFD Neighbor Loss 15-75
BGP Link Down 15-76
BGP Neighbor Loss 15-78
BGP Process Down 15-81
Broken LSP Discovered 15-82
Card Down 15-82
Card Out 15-83
Carrier Grade NAT Translations Create Rate 15-85

Carrier Grade NAT Translations Delete Rate **15-86**
Carrier Grade NAT Inside-to-Outside Forward Rate **15-88**
Carrier Grade NAT Outside-to-Inside Forward Rate **15-89**
Carrier Grade NAT Inside-to-Outside Drops Port Limit Exceeded **15-91**
Carrier Grade NAT Inside-to-Outside Drops System Limit Reached **15-92**
Carrier Grade NAT Inside-to-Outside Drops Resource Depletion **15-94**
CFM Domain Fault **15-95**
Chassis Disconnected **15-97**
Cloud Problem **15-99**
Component Unreachable **15-100**
CPU Utilization **15-101**
Device Unsupported **15-102**
Discard Packets **15-103**
Dropped Packets **15-104**
DS0 Bundle **15-105**
DS1 Path Link Down **15-107**
DS1 Path Port Down **15-111**
DS3 Path Link Down **15-113**
DS3 Path Port Down **15-117**
Dual Stack IP Changed **15-119**
DWDM Controller **15-121**
DWDM G709 Status **15-122**
EFP Down **15-124**
ESMC Process Down **15-126**
Fan-Tray Down **15-127**
Fan-Tray Out **15-128**
GRE Keepalive **15-130**
GRE Tunnel Down **15-131**
HSRP Group Status Changed **15-132**
Interface Status **15-134**
Investigation State **15-137**
L2TP Peer Not Established **15-137**
L2TP Sessions Threshold **15-139**
Lag Down **15-140**
Lag Link Down **15-142**
Layer 2 Tunnel Down **15-144**
LDP Neighbor Loss **15-145**
Link Down **15-146**
Link Utilization **15-149**
Local Switching Down **15-151**

Logical Port Down 15-152
LSP Down 15-153
Members Changed 15-155
Memory Utilization 15-157
MLPPP Bundle 15-158
MPLS Black Hole Found 15-162
MPLS TP Bandwidth Mismatch 15-163
15-163
MPLS Interface Removed 15-163
MPLS TE FRR State Changed 15-164
MPLS TE Tunnel Down 15-166
MPLS TP Tunnel Down 15-171
Network-Clock Synchronization 15-172
OSPF Neighbor State Change 15-173
Port Down 15-174
Power Supply Down 15-177
Power Supply Out 15-178
Pluggable Transceiver Out 15-179
REP Port Role Change 15-180
Rx Dormant 15-181
Rx Utilization 15-182
Shelf Out 15-183
SONET Path Link Down 15-184
SONET Path Port Down 15-187
Subinterface Down 15-190
Tx Dormant 15-192
Tx Utilization 15-193
VSI Down 15-194
Alarm Source OIDs 15-196
BFD Connectivity Down OID 15-197
BFD Neighbor Loss OID 15-197
BGP Neighbor Entry OID (IBgpNeighborEntryOid) 15-197
Carrier Grade NAT OID (ICgnServiceOid) 15-197
Chassis Oid (ChassisId) 15-198
DS0 Bundle OID (IDS0BundleOid) 15-198
DS1 Path OID (IDS1PathOid) 15-198
DS3 Path OID (IDS3PathOid) 15-199
DWDM Controller OID (IDWDMOid) 15-199
EFP OID (IEFPOID) 15-199
Fan Tray OID 15-200

IMA Service (IIMAGroupOid) 15-200
IP Interface OID (IPInterfaceOid) 15-200
Lag Down OID 15-201
Lag Link Down OID 15-201
L2TP Peer OID (IL2tpPeerOid) 15-201
Local Switching Entry Down OID 15-201
Logical Port OID (ILogicalPortOid) 15-202
LSP Endpoint OID (LSP EndPoint OID) 15-202
LSE Entry OID (IMplsEntryOid) 15-203
LSE OID (ILseOid) 15-203
Alarm Differentiators 15-203
Managed Element OID (IManagedElementOid) 15-204
Members Changed OID (IDataLinkAggregationOid) 15-204
MLPPP OID (IMLPPPOid) 15-205
Module OID (IModuleOid) 15-205
MPBGP OID (IMpBgpOid) 15-205
MPLS TE Tunnel OID (IMplsTETunnelOid) 15-206
TP Tunnel Endpoint OID (TP Tunnel EndPoint OID) 15-206
ISyncEOID 15-206
OSPF Neighbor State Change OID 15-207
Port OID 15-207
Power Supply OID 15-207
Physical Layer OID (IPhysicalLayerOid) 15-207
Shelf OID (IShelfOid) 15-208
SONET Path Port Down OID 15-208
SONET Path Link Down OID 15-208
Topological Link OID (ITopologicalLinkOid) 15-208
Supported Alarms with Topological Link OID Source 15-209
Link Down Endpoint OID Structure 15-209
GRE Tunnel Endpoint OID Structure 15-210
Layer 2 MPLS Tunnel Endpoint OID Structure 15-210
BGP Link Down Endpoint OID Structure 15-210
VLAN Tagged Interface OID (IVlanTaggedInterfaceOID) 15-211
VSI OID (IVSIOID) 15-211

CHAPTER 16 **Traps** 16-1
Cisco ASR 9000 V1 Traps 16-3
Cisco ASR 9000 V2/V3 Traps 16-4
Cisco IOS V1 Traps 16-6

Cisco IOS V2/V3 Traps 16-61
Cisco IOX V1 Traps 16-89
Cisco IOX V2/V3 Traps 16-103
Cisco MIB2 V1 Traps 16-119
Cisco MIB2 V2/V3 Traps 16-129
Cisco ACE V1 Traps 16-138
Cisco ACE V2/V3 Traps 16-140
Cisco Nexus V1 Traps 16-141
Cisco Nexus V2/V3 Traps 16-154
Cisco CPT V2 Traps 16-160
Cisco ASR 5000 Series V2 Traps 16-161
Cisco Unified Computing System V2 Traps 16-186
Cisco ASR 1000 V2 Traps 16-197
Cisco ASR 9000 V1 Trap Registry Parameters 16-197
Cisco ASR 9000 V2/V3 Registry Parameters 16-198
Cisco IOS V1 Trap Registry Parameters 16-199
Cisco IOS V2/V3 Trap Registry Parameters 16-223
Cisco IOX V1 Trap Registry Parameters 16-244
Cisco IOX V2/V3 Trap Registry Parameters 16-253
Cisco MIB2 V1 Trap Registry Parameters 16-263
Cisco MIB2 V2/V3 Trap Registry Parameters 16-270
Cisco ACE V1 Trap Registry Parameters 16-278
Cisco ACE V2/V3 Trap Registry Parameters 16-279
Cisco Nexus V1 Trap Registry Parameters 16-280
Cisco Nexus V2/V3 Trap Registry Parameters 16-284
Cisco CPT V2 Trap Registry Parameters 16-288
Cisco ASR 5000 Series V2 Trap Registry Parameters 16-289
Cisco Unified Computing System V2 Trap Registry Parameters 16-311
Cisco ASR 1000 V2 Trap Registry Parameters 16-322

CHAPTER 17 **Syslogs** 17-1

Cisco ASR 9000 Syslogs 17-2
Cisco ASR 1000 Syslogs 17-4
Cisco IOS Syslogs 17-4
Cisco IOX Syslogs 17-21
Cisco ACE Syslogs 17-35

Cisco Nexus Syslogs 17-39
Cisco ASR 9000 Syslog Registry Parameters 17-43
Cisco ASR 1000 Registry Parameters 17-46
Cisco IOS Syslog Registry Parameters 17-47
Cisco IOX Syslog Registry Parameters 17-71
Cisco ACE Syslog Registry Parameters 17-85
Cisco Nexus Syslog Registry Parameters 17-89

PART 4 Commands

CHAPTER 18 Using Connectivity Fault Management Commands 18-1
Supported Network Elements 18-2
Configuring CFM Components 18-3
Configure CFM Maintenance Domain 18-3
Configure CFM Global Parameters 18-4
Configure CFM MIP 18-5
Configure CFM Continuity Check 18-6
Configure CFM Service ID 18-8
Configure CFM MEP 18-8
Enable CFM Continuity Check 18-10
Enable CFM SNMP Server Traps 18-10
Diagnose CFM Components 18-11
Diagnose CFM with Show MEP Status 18-11
Diagnose CFM with Show MEP Crosscheck Status 18-12
Diagnose CFM with Ping Remote MEP with MAC 18-12
Diagnose CFM with Ping Remote MEP with MPID 18-13
Diagnose CFM with Ping Remote MEP with Multicast 18-14
Diagnose CFM with Traceroute Remote MEP with MAC 18-14
Diagnose CFM with Traceroute Remote MEP with MPID 18-15

CHAPTER 19 Using Resilient Ethernet Protocol Command 19-1
Supported Network Elements 19-2
Displaying REP Segment Data 19-3

CHAPTER 20 Using Cisco Carrier Grade NAT Commands 20-1
Supported Network Elements 20-2
Configuring Carrier Grade NAT Instance 20-2
Removing a Carrier Grade NAT instance 20-3

Displaying Pool Utilization 20-3
Adding 6rd Forwarding 20-4
Adding Carrier Grade Nat 64 Forwarding 20-5

CHAPTER 21 **Using Pseudowire Virtual Circuit Connectivity Verification Commands** 21-1
Supported Network Elements 21-2
Pinging the Peer Router from a Single Segment or Multisegment Pseudowire 21-2
Displaying Pseudowire Information 21-3

CHAPTER 22 **Using Ethernet Operations, Administration and Maintenance Operations Commands** 22-1
Supported Network Elements 22-1
Configuring L-OAM Components 22-2
Applying Template on an Interface 22-2
Create Template 22-3
22-4
Disabling OAM on an Interface 22-4
Enabling OAM on an Interface 22-5
Configuring OAM Parameters on an Interface 22-5
Starting the Remote Loopback 22-6
Stopping the Remote Loopback 22-6

CHAPTER 23 **Using Ethernet Local Management Interface Commands** 23-1
Supported Network Elements 23-1
Configuring Ethernet LMI Components 23-2
Enabling Ethernet LMI Globally 23-2
Configuring Multipoint-to-Multipoint or Point-to-Point Ethernet Virtual Connection 23-3
Configuring UNI on an Interface 23-3
Enabling Ethernet LMI on an Interface 23-4
Configuring the Service Instance VLAN ID on an Interface 23-5

CHAPTER 24 **Using MPLS-TP Commands** 24-1
Supported Network Elements 24-1
Configuring MPLS-TP Components 24-2
Tunnel Ping 24-2
Tunnel Trace 24-3
LSP Path Lockout 24-3
LSP Ping 24-4
Lsp Trace 24-5

Lsp Lockout 24-5
Lsp Path No Lockout 24-6
Add Global Configuration 24-6
Remove Global Configuration 24-7
Update Global Configuration 24-8
Add Link Configuration 24-8
Remove Link Configuration 24-9
Add BFD Template Configuration 24-10
Remove BFD Template Configuration 24-11
Show BFD Template 24-11
Show BFD Template At Tunnel 24-12
Add Label Range Configuration 24-12
Remove Label Range Configuration 24-13
BFD Global Configuration 24-14

CHAPTER 25 **Using mLACP Commands** 25-1
Supported Network Elements 25-1
Show Group 25-2
Show MPLS LDP 25-2
Show Channel 25-2
Show LACP Internal 25-3

CHAPTER 26 **Using the Session Border Controller Commands** 26-1
Configuring SBC Components 26-1
Add Commands 26-2
Adding SIP Adjacency 26-2
Adding SIP Adjacency Outbound AuthRealm 26-7
Adding a Blacklist 26-8
Adding a Blacklist Reason 26-9
Adding a CAC Policy Set 26-10
Adding a CAC Policy Table 26-11
Adding a CAC Rule Entry to a CAC Policy Table 26-11
Adding a Call Policy Set 26-14
Adding a Call Policy Table to a Call Policy Set 26-15
Adding a Call Rule Entry to a Call Policy Table 26-16
Adding a Codec List 26-17
Adding an Entry to a Codec List 26-18
Adding a Media Address 26-19
Adding a QoS Profile 26-19

Adding a SIP Header Profile 26-20
Adding a Header to an Existing SIP Header Profile 26-21
Adding an Entry to a SIP Header Profile Header 26-22
Adding a Condition to a SIP Header Profile Header Entry 26-23
Adding a SIP Option Profile 26-24
Adding a SIP Parameter Profile 26-25
Adding a Parameter to a SIP Parameter Profile 26-25
Adding a Media Address DBE 26-26
Delete Commands 26-27
Deleting a Blacklist 26-28
Deleting a Blacklist Reason 26-28
Deleting a CAC Policy Set 26-29
Deleting a CAC Policy Table 26-30
Deleting a CAC Rule Entry 26-31
Deleting a Call Policy Set 26-31
Deleting a Call Policy Table 26-32
Deleting a Call Rule Entry 26-33
Deleting a Codec List 26-33
Deleting an Entry From a Codec List 26-34
Deleting a Media Address 26-35
Deleting a QoS Profile 26-35
Deleting a SIP Header Profile 26-36
Deleting an Entry From a Header of a SIP Header Profile 26-37
Deleting a Header From a SIP Header Profile 26-38
Deleting a SIP Adjacency 26-38
Deleting a SIP Adjacency Authentication Realm 26-39
Deleting a SIP Option Profile 26-40
Deleting a SIP Parameter Profile 26-40
Deleting a Parameter From a SIP Parameter Profile 26-41
Update Commands 26-42
Updating a Blacklist Reason 26-42
Updating a CAC Policy Set 26-43
Updating a CAC Policy Table 26-44
Updating a CAC Rule Entry 26-45
Updating a Call Policy Set 26-47
Updating a Call Policy Table 26-48
Updating a Call Rule Entry 26-49
Updating a Codec List Entry 26-50
Updating a QoS Profile 26-51
Updating a SIP Adjacency 26-52

Updating a SIP Header Profile 26-56
Updating a SIP Header Profile Entry 26-56
Updating a SIP Option Profile 26-57
Updating a Parameter in a SIP Parameter Profile 26-58
Updating SIP Adjacency Outbound AuthRealm 26-59
Monitoring the Performance of SBC Components 26-60
Showing SBC CPS Data 26-60
Showing SBC Components 26-61
Showing SBC Current 15 Minute Stats 26-61
Showing SBC Current 5 Minute Stats 26-62
Showing SBC Current Day Stats 26-62
Showing SBC Current Hour Stats 26-62
Showing SBC H248 Stats 26-63
Showing SBC Previous 15 Minute Stats 26-63
Showing SBC Previous 5 Minute Stats 26-64
Showing SBC Previous Day Stats 26-64
Showing SBC Previous Hour Stats 26-65
Showing SBC Media Stats 26-65

CHAPTER 27 **Using the DWDM and SONET Commands** 27-1
Supported Network Elements 27-1
Running SONET Commands 27-2
Displaying BER Threshold 27-2
Displaying SONET Controller Data 27-3
Displaying TCA Threshold 27-3
Displaying Line PM Counters 27-3
Displaying Medium PM Counters 27-4
Displaying Path PM Counters 27-4
Displaying Section PM Counters 27-5
Displaying Trace Details 27-6
Clearing SONET Counters 27-6
Setting BER Threshold 27-7
Setting Clock Source 27-7
Setting TCA Threshold 27-8
Running DWDM Commands 27-9
Displaying DWDM Controller Data 27-10
Displaying DWDM PM History Data 27-10
Displaying DWDM RTPM Counters 27-11
Displaying DWDM RTPM Threshold 27-11

Displaying DWDM Wavelength Map 27-12
Clearing DWDM Counters 27-12
Setting DWDM Channel 27-13
Setting DWDM FEC Mode 27-13
Setting DWDM G.709 ODU 27-14
Setting DWDM G.709 OTU 27-14
Setting DWDM G.709 TTI 27-15
Setting DWDM G.709 Wrapper 27-16
Setting DWDM Laser State 27-17
Setting DWDM Loopback 27-17
Setting DWDM PM FEC Data 27-18
Setting DWDM PM Optics Data 27-19
Setting DWDM PM OTN Data 27-20
Setting DWDM Transmit Power 27-21
Setting Rx LOS Threshold 27-22
Displaying IM Trace Details 27-23
Displaying Device Log 27-23

CHAPTER 28 **Using the Prime Network Basic Operation Commands** 28-1

Configuration Commands 28-2
Add Interface Configuration 28-3
Remove Interface Configuration 28-4
Update Interface Configuration 28-4
Add Loopback Interface 28-5
Add Port Description 28-6
Remove Port Description 28-6
Update Port Description 28-7
Change Port Status 28-8
Enable traps 28-8
Remove Access List 28-9
Remove Access List Entry 28-9
Remove Rate Limit 28-10
Write Memory 28-10
Disable Interface 28-11
Enable Interface 28-11
Assign Port To Vlan 28-11
DeAssign Port To Vlan 28-12
Add Host Name 28-12
Remove Host Name 28-13
Add DNS Server 28-13

Remove DNS Server 28-14
Add NTP Server 28-15
Remove NTP Server 28-15
Syslog Host Logging 28-16
Add Traps 28-16
Remove Traps 28-17
Add Radius Server 28-18
Remove Radius Server 28-18
Add Tacacs Server 28-19
Remove Tacacs Server 28-20
Add Tacacs+ Server 28-20
Remove Tacacs+ Server 28-21
Add SNMP Configuration 28-21
Remove SNMP Configuration 28-22
Update SNMP Configuration 28-23
Show Commands 28-24
Interface Brief 28-24
IP Route 28-25
VRF IP Route 28-25
Running Config 28-26
Running Config from File 28-26
Startup Config 28-26
Users (Telnet Sessions) 28-27
Tools Commands 28-27
From FTP 28-28
From TFTP 28-28
To FTP 28-29
To TFTP 28-29
OAM Commands 28-30
Destination From Device 28-30
Ping VRF 28-31
Trace Route From Device 28-31
Trace Route VRF 28-32
Scheduling a Command 28-32

INDEX



Preface

This guide provides reference information on Cisco Prime Network (Prime Network) 3.9. This information is presented in four parts:

- Part 1—Cisco VNEs: Supplies detailed information on all of the Virtual Network Elements (VNEs) supplied with Prime Network.
- Part 2—Technology Support: Details the level of functionality Prime Network provides for each of the networking technologies it supports.
- Part 3—Alarms and Events: Lists and describes all of the Prime Network alarms, events, SNMP traps, and syslogs, supported in this version of Prime Network.
- Part 4—Commands: Lists, describes, and explains how to use the commands supplied with Prime Network. Includes the list of the basic operations that you can perform on a selected VNE.

New and Changed Information

The following table describes information that has been added or changed since the initial release of the *Cisco Prime Network 3.9 Reference Guide*.

Table 1 New and Changed Information in this Guide

Date Released	Revision	Location
August 24, 2012	Added supported software versions for Cisco ASR 9000 routers (CSCub72395).	Cisco ASR 9000—Supported Software Versions, page 121
August 20, 2012	Replaced a subtype event for the Adaptive Polling service alarm (CSCua77244).	Adaptive Polling, page 4
July 23, 2012	Updated technology support information for Cisco ASR 903 device series based on the changed prospectus (CSCub12900).	Supported Technologies on Cisco Routers, page 198

Audience

The intended audience for this guide includes system engineers involved in the customization, extension, management, and networking operations of Prime Network.

Document Organization

This guide includes the following parts:

Part	Title	Description
Part 1	Cisco VNEs	Provides an overview of Virtual Network Elements in Cisco Prime Network and the key information for VNE support.
Part 2	Technology Support	Provides an overview of the level of functionality that Prime Network provides for each technology it supports.
Part 3	Alarms and Events	Provides details about system events that appear in the Prime Network Events System tab.
Part 4	Commands	Provides details of technologies supported by Prime Network.

Conventions

This document uses the following conventions:

Table 2 Conventions

Convention	Description
string	A string is a nonquoted set of characters. For example, when setting an SNMP community string to **public**, do not use quotation marks around the string, or the string will include the quotation marks.
^ or Ctrl	^ or Ctrl represents the Control key. For example, the key combination ^D or **Ctrl-D** means hold down the **Control** key while you press the **D** key. Alphabetic character keys are indicated in capital letters but are not case sensitive.
< >	Angle brackets show nonprinting characters, such as passwords.
!	An exclamation point at the beginning of a line indicates a comment line.
[ ]	Square brackets indicate optional elements of a command.
{ }	Braces group alternative, mutually exclusive elements that are part of a required choice.
|	A vertical bar, also known as a pipe, separates alternative, mutually exclusive elements of a choice.
boldface font	Indicates a button name, command, keyword, key combination, or menu item.
boldface screen font	**Courier bold** shows an example of text that you must enter.
Italic text	Indicates a variable or attribute value, including enumerated values.
italic screen font	Indicates variables for which you must enter a value.
screen font	Courier plain shows an example of information displayed on the screen.
Blue text	Indicates a link or reference to a section, table or object elsewhere in this guide or on the World Wide Web.
Option > Network Preferences	Indicates menu items to be selected, and the order in which to select them.

Related Documentation

Note We sometimes update the documentation after original publication. Therefore, you should also review the documentation on Cisco.com for any updates.

For all the related documentation for Cisco Prime Network 3.9, see the *Cisco Prime Network 3.9 Documentation Guide.*

The Prime Network Technology Center is an online resource for additional downloadable Prime Network support content, including help for integration developers who use Prime Network application programming interfaces (APIs). The website provides information, guidance, and examples to help you integrate your applications with Prime Network. It also provides a platform for you to interact with subject matter experts. To view the information on the Prime Network Technology Center website, you must have a Cisco.com account with partner level access, or you must be a Prime Network licensee. You can access the Prime Network Technology Center at: *http://developer.cisco.com/web/prime-network/docs/-/document_library/view/2356901*.

Obtaining Documentation and Submitting a Service Request

For information on obtaining documentation, submitting a service request, and gathering additional information, see the monthly *What's New in Cisco Product Documentation*, which also lists all new and revised Cisco technical documentation, at:

http://www.cisco.com/en/US/docs/general/whatsnew/whatsnew.html

Subscribe to the *What's New in Cisco Product Documentation* as a Really Simple Syndication (RSS) feed and set content to be delivered directly to your desktop using a reader application. The RSS feeds are a free service and Cisco currently supports RSS version 2.0.



PART 1

Cisco VNEs



CHAPTER 1

Introduction

This chapter introduces Virtual Network Elements (VNEs) and describes the types of information available in this guide.

This chapter contains the following topics:

- Introduction to VNEs, page 1-1
- Understanding the Tables, page 1-1

Introduction to VNEs

VNEs (Virtual Network Elements) are independent software processes that run on the Prime Network Unit Servers. Each VNE is assigned to manage a single network element (NE) using the NE's management interfaces (for example, SNMP and/or Telnet). The VNEs maintain a live model, or abstraction, of each NE and the entire network.

As the VNE loads, it starts investigating the NE and automatically builds a live model of the NE, including its physical and logical inventory, its configuration and its status. After modeling the NE, the VNE begins negotiating with peer VNEs, which represent the peer NEs, in order to determine NE connectivity and topology at different layers. This model of the network topology, NE state, and NE inventory is constantly being updated by the VNEs, which track every change that occurs in the NEs and the network.

The VNEs communicate between themselves to analyze end-to-end flows, which provide information for root-cause and impact analysis, service path tracing, and more.

Understanding the Tables

This section describes key information that can be found in the VNE support information chapters in this guide.

This section contains the following topics:

- Software Versions, page 1-2
- Product Versions, page 1-3
- Expedite Legend, page 1-3

Software Versions

The Software Version column in the tables in this guide identifies the NE software versions that are compatible with Prime Network and that can be running on the NEs that Prime Network supports. For example: The "Cisco 7600 Series—Supported Software Versions" table lists Cisco IOS software version 12.2(18)SXD. This means that Prime Network will work with any supported Cisco 7600-series router (such as the Cisco 7603) that is running IOS release 12.2(18)SXD.

Prime Network may support subsequent maintenance releases of NE software versions, but only if these later NE software versions do not require changes in Prime Network to maintain compatibility. Changes in any of the following NE software components can affect compatibility with Prime Network, and may require Prime Network software changes: XML interfaces, SNMP commands, MIBs, and CLI commands. In cases where a new NE software version remains compatible without requiring changes in Prime Network, support will include recognition of the new NE software version. However, it may not include support for additional software and features (such as new hardware modules) in the NE software version.

Also, for Prime Network to recognize a later NE software image, the name of the NE software rebuild should be similar to a software image in the train already supported in Prime Network. For example, Cisco ANA 3.7 supports IOS 12.2(33)SRC4 for 7600 devices. If IOS 12.2(33)SRC5 is released, ANA will recognize IOS 12.2.(33)SRC5 with the same level of support as IOS 12.2(33)SRC4 on 7600 devices. But Cisco ANA will not support any additional software or hardware features introduced in IOS 12.2(33)SRC5.

Prime Network will not recognize any other maintenance or special build whose version string does not match the indicated naming pattern. For example: IOS 12.2(33)SRC4xyz (or any other variation) will not be recognized.

When an NE software release is not recognized, Prime Network attempts to model the NE using the default version for that device series. The default version is a device-specific fallback set of commands and MIB instrumentation that allows Prime Network to discover and query for basic device properties, including:

- Managed element information.
- Basic physical inventory.
- Logical Inventory (including the Routing Table, ARP, BGP and OSPF information). Modelling of other technologies is done on a best-effort basis.

The default version does not correspond to any specific supported NE software version. Building of the physical model and its containment structure depends on the instrumentation (MIB and CLI commands) used by the default version. The default version may show you different containment structures (modules and cards) from what you will see for an explicitly supported NE software version. You can discover whether the default version is being used for a particular VNE by looking in the AVM log located in *install directory*/main/logs (search for ***default version***).

Cisco frequently qualifies new NE software versions for compatibility with Prime Network, and updates the online version of this guide accordingly. If you are not sure whether the current version of Prime Network supports a recently released NE software version, check the online version of this guide on Cisco.com for an update. The NE software version should appear in the updated version of this guide if it has been qualified as compatible with this Prime Network release. If the online version of this guide does not list the new software version, contact Cisco Professional Services or your Cisco Sales Representative.

Product Versions

Product Version column found in tables in this guide lists the earliest versions of Cisco Prime Network or VNE Device Package or Cisco ANA in which the specified feature was supported. Feature may be a Network Element Type or Module or Software Version or Technology or Topology or Service Event.

Product versions, containing the string DP, indicate the earliest VNE Device Package versions supporting the feature.Latter versions of VNE Device Packages will contain support for that particular feature. For example, if Product Version is mentioned as PrimeNetwork-3.8.X-DP2 for a feature, it means PrimeNetwork-3.8.X-DP2 is the earliest Cisco Prime Network 3.8 and Cisco Prime Network 3.8.1 compatible VNE Device Package supporting that feature . Similarly, if Product Version is mentioned as Cisco-ANA3.7.X-DP9 for a feature, it means Cisco-ANA3.7.X-DP9 is the earliest Cisco ANA 3.7.2 and Cisco ANA 3.7.3 compatible VNE Device Package supporting that feature.

Cisco Prime Network 3.9 supports all the features supported upto PrimeNetwork-3.8.X-DP4 VNE Device Package. Features supported upto Cisco-ANA3.7.X-DP13 are supported in Cisco Prime Network 3.9 as well as in PrimeNetwork-3.8.X-DP4 Device package. However, features with Product Versions PrimeNetwork-3.8.X-DP5 and PrimeNetwork-3.8.X-DP6 are compatible with Cisco Prime Network 3.8 and Cisco Prime Network 3.8.1 only. Cisco Prime Network 3.9 support for these features will be available with Cisco Prime Network 3.9 compatible VNE Device Package which will be released by June 2012.

Product Versions prior to Cisco ANA 3.7.2 indicate the earliest Cisco ANA release supporting the feature. Latter versions of Cisco ANA will contain support for the feature.For example: If the guide indicates that Cisco 7600 routers are supported on Cisco ANA 3.6.0, they are also supported on Cisco ANA 3.6.1, Cisco ANA 3.6.2, and so on. These features are also supported in Cisco Prime Network 3.9 as well as in PrimeNetwork-3.8.X-DP4 VNE Device Package.

Expedite Legend

Table 1-1 describes the meaning of the Expedite column found in the service event (service alarm) tables in this Reference guide.

Table 1-1 Expedite Legend in Service Event Tables

Value	Descriptions
Y	The service event is expedited by a syslog or trap generated by the device. This means that the syslog or trap causes the VNE to poll the device without waiting for the usual polling cycle, thus enabling quicker detection of the event.
N	The service event is not expedited.This means that the VNE will poll this device during the next regularly scheduled polling cycle.



CHAPTER 2

Overview—Supported Network Elements in Cisco Prime Network 3.9

This chapter provides an overview of network elements (NEs) that are supported by Cisco Prime Network 3.9 and includes the following sections:

- Supported Generic Devices in Cisco Prime Network 3.9, page 2-1
- Supported Cisco DataCentre in Cisco Prime Network 3.9, page 2-1
- Supported Cisco Optical Transport in Cisco Prime Network 3.9, page 2-2
- Supported Cisco Security Appliances in Cisco Prime Network 3.9, page 2-2
- Supported Cisco Access Servers in Cisco Prime Network 3.9, page 2-3
- Supported Cisco Gateways in Cisco Prime Network 3.9, page 2-3
- Supported Cisco Routers in Cisco Prime Network 3.9, page 2-3
- Supported Cisco Switches in Cisco Prime Network 3.9, page 2-13

Supported Generic Devices in Cisco Prime Network 3.9

This document includes support information for the following Generic devices:

- Generic VNE

Table 2-1 Supported Generic Devices in Cisco Prime Network 3.9

NE Type	Product Name	SysOID	Product_Version
Generic VNE			
Generic device		1.3.999.3	

Supported Cisco DataCentre in Cisco Prime Network 3.9

This document includes support information for the following Cisco DataCentre:

- Cisco UCS 61xx Series Switches

Table 2-2 Supported Cisco DataCentre in Cisco Prime Network 3.9

NE Type	Product Name	SysOID	Product_Version
Cisco UCS 61xx Series Switches			
Cisco UCS 6120XP	Cisco UCS 6100 Series Fabric Interconnects	1.3.6.1.4.1.9.12.3.1.3.847	Prime Network 3.9

Supported Cisco Optical Transport in Cisco Prime Network 3.9

This document includes support information for the following Cisco Optical Transport:

- Cisco Carrier Packet Transport Series Devices

Table 2-3 Supported Cisco Optical Transport in Cisco Prime Network 3.9

NE Type	Product Name	SysOID	Product_Version
Cisco Carrier Packet Transport Series Devices			
CPT600	Cisco CPT 600 series device	1.3.6.1.4.1.3607.1.20.10.80	3.8
CPT200	Cisco CPT 200 series device	1.3.6.1.4.1.3607.1.20.10.70	3.8

Supported Cisco Security Appliances in Cisco Prime Network 3.9

This document includes support information for the following Cisco Security appliances:

- Cisco Adaptive Security Appliance 5550 Series
- Cisco Adaptive Security Appliance 5580 Series

Table 2-4 Supported Cisco Security Appliances in Cisco Prime Network 3.9

NE Type	Product Name	SysOID	Product_Version
Cisco Adaptive Security Appliance 5550 Series			
ciscoASA5550	Cisco ASA 5550 Security Appliance	1.3.6.1.4.1.9.1.753	3.6.3[1]
ciscoASA5550sc	Cisco ASA 5550 Security Appliance	1.3.6.1.4.1.9.1.763	3.6.3[2]
Cisco Adaptive Security Appliance 5580 Series			
ciscoASA5580	Cisco ASA 5580 Adaptive Security Appliance	1.3.6.1.4.1.9.1.914	3.7[3]

[1, 2, 3]Only Single context is supported in ASA devices.

Supported Cisco Access Servers in Cisco Prime Network 3.9

This document includes support information for the following Cisco access servers:

- Cisco Access Server 5800 Series

Table 2-5 Supported Cisco Access Servers in Cisco Prime Network 3.9

NE Type	Product Name	SysOID	Product_Version
Cisco Access Server 5800 Series			
ciscoAS5800	Cisco Access Server 5800	1.3.6.1.4.1.9.1.188	3.7.1

Supported Cisco Gateways in Cisco Prime Network 3.9

This document includes support information for the following Cisco gateways:

- Cisco AS5300 Series Universal Gateways

Table 2-6 Supported Cisco Gateways in Cisco Prime Network 3.9

NE Type	Product Name	SysOID	Product_Version
Cisco AS5300 Series Universal Gateways			
ciscoAS5300	Cisco AS5300 Access Server	1.3.6.1.4.1.9.1.162	3.6.0

Supported Cisco Routers in Cisco Prime Network 3.9

This document includes support information for the following Cisco routers:

- Cisco 800 Series Routers
- Cisco 1000 Series Routers
- Cisco 1600 Series Routers
- Cisco 1700 Series Modular Access Routers
- Cisco 1800 Series Integrated Services Routers
- Cisco 2500 Series Routers
- Cisco 2600 Series Multiservice Platform Routers
- Cisco 2800 Series Integrated Services Routers
- Cisco 3600 Series Multiservice Platform Routers
- Cisco 3700 Series Multiservice Access Routers
- Cisco 3800 Series Integrated Services Routers
- Cisco 7200 Series Routers
- Cisco 7300 Series Routers
- Cisco 7400 Series Routers

- Cisco 7500 Series Routers
- Cisco 7600 Series Routers
- Cisco 10000 Series Routers
- Cisco 12000 Series Routers
- Cisco XR 12000 Series Routers
- Cisco CRS Carrier Routing System
- Cisco ASR 9000 Series Aggregation Services Routers
- Cisco ASR 1000 Series Routers
- Cisco MWR 2900 Series Mobile Wireless Routers
- Cisco 1900 Series Integrated Services Router
- Cisco 2900 Series Integrated Services Router
- Cisco 3900 Series Integrated Service Routers
- Cisco Universal Broadband Router 7200 Series
- Cisco Univeral Broadband Router 10000 Series
- Cisco 4700 Series Routers
- Cisco ASR901 Series Mobile Wireless Routers
- Cisco ASR903 Series Routers
- Cisco ASR 5000 Series Routers

Table 2-7 Supported Cisco Routers in Cisco Prime Network 3.9

NE Type	Product Name	SysOID	Product_Version
Cisco 800 Series Routers			
cisco801	Cisco 801 ISDN Router	1.3.6.1.4.1.9.1.212	3.6.0
cisco802	Cisco 802 ISDN Router	1.3.6.1.4.1.9.1.213	3.6.0
cisco803	Cisco 803 ISDN Router	1.3.6.1.4.1.9.1.214	3.6.0
cisco804	Cisco 804 ISDN Router	1.3.6.1.4.1.9.1.215	3.6.0
cisco805	Cisco 805 Serial Router	1.3.6.1.4.1.9.1.245	3.6.0
cisco802J	Cisco 802 ISDN Router	1.3.6.1.4.1.9.1.295	3.6.1
cisco804J	Cisco 804 ISDN Router	1.3.6.1.4.1.9.1.296	3.6.1
cisco826QuadV	Cisco 826 ADSL Router	1.3.6.1.4.1.9.1.321	3.6.1
cisco806	Cisco 806 Broadband Router	1.3.6.1.4.1.9.1.384	3.6.0
cisco811	Cisco 811 ISDN Router	1.3.6.1.4.1.9.1.395	3.6.0
cisco813	Cisco 813 ISDN Router	1.3.6.1.4.1.9.1.396	3.6.0
cisco826	Cisco 826 ADSL Router	1.3.6.1.4.1.9.1.322	3.6.0
cisco827	Cisco 827 ADSL Router	1.3.6.1.4.1.9.1.284	3.6.0
cisco827H	Cisco 827 H ADSL Router	1.3.6.1.4.1.9.1.446	3.6.0
cisco827QuadV	Cisco 827-4V ADSL Router	1.3.6.1.4.1.9.1.270	3.6.0

Table 2-7 Supported Cisco Routers in Cisco Prime Network 3.9 (continued)

NE Type	Product Name	SysOID	Product_Version
cisco828	Cisco 828 G.SHDSL Router	1.3.6.1.4.1.9.1.382	3.6.0
cisco831	Cisco 831 Ethernet Broadband Router	1.3.6.1.4.1.9.1.497	3.6.0
cisco836	Cisco 836 ADSL over ISDN Broadband Router	1.3.6.1.4.1.9.1.499	3.6.0
cisco837	Cisco 837 ADSL Broadband Router	1.3.6.1.4.1.9.1.495	3.6.1
cisco876	Cisco 876 Integrated Services Router	1.3.6.1.4.1.9.1.568	3.6.1
cisco877	Cisco 877 Integrated Services Router	1.3.6.1.4.1.9.1.569	3.6.1
cisco878	Cisco 878 Integrated Services Router	1.3.6.1.4.1.9.1.570	3.6.1
cisco871	Cisco 871 Integrated Services Router	1.3.6.1.4.1.9.1.571	3.6.1
Cisco 1000 Series Routers			
cisco1003	Cisco 1003 Router	1.3.6.1.4.1.9.1.41	3.5.2
cisco1004	Cisco 1004 Router	1.3.6.1.4.1.9.1.44	3.5.2
cisco1005	Cisco 1005 Router	1.3.6.1.4.1.9.1.49	3.5.2
Cisco 1600 Series Routers			
cisco1601	Cisco 1601 Router	1.3.6.1.4.1.9.1.113	3.6.1
cisco1602	Cisco 1602 Router	1.3.6.1.4.1.9.1.114	3.6.1
cisco1603	Cisco 1603 Router	1.3.6.1.4.1.9.1.115	3.6.1
cisco1604	Cisco 1604 Router	1.3.6.1.4.1.9.1.116	3.6.1
ciscoPro1601	Cisco Pro 1601	1.3.6.1.4.1.9.1.117	3.6.1
ciscoPro1602	Cisco Pro 1602	1.3.6.1.4.1.9.1.118	3.6.1
ciscoPro1603	Cisco Pro 1603	1.3.6.1.4.1.9.1.119	3.6.1
cisco1605	Cisco 1605 Router	1.3.6.1.4.1.9.1.172	3.6.1
Cisco 1700 Series Modular Access Routers			
cisco1701ADSLBRI	Cisco 1701 ADSL Security Access Router	1.3.6.1.4.1.9.1.550	3.6.1
cisco1710	Cisco 1710 Security Access Router	1.3.6.1.4.1.9.1.200	3.6.1
cisco1711	Cisco 1711 Security Access Router	1.3.6.1.4.1.9.1.538	3.6.1
cisco1712	Cisco 1712 Security Access Router	1.3.6.1.4.1.9.1.539	3.6.1
cisco1720	Cisco 1720 Modular Access Router	1.3.6.1.4.1.9.1.201	3.6.1

Table 2-7 Supported Cisco Routers in Cisco Prime Network 3.9 (continued)

NE Type	Product Name	SysOID	Product_Version
cisco1721	Cisco 1721 Modular Access Router	1.3.6.1.4.1.9.1.444	3.6.1
cisco1750	Cisco 1750 Modular Access Router	1.3.6.1.4.1.9.1.216	3.6.1
cisco1760	Cisco 1760-V Modular Access Router	1.3.6.1.4.1.9.1.416	3.6.1
cisco1751	Cisco 1751 Modular Access Router	1.3.6.1.4.1.9.1.326	3.6.1
Cisco 1800 Series Integrated Services Routers			
cisco1801	Cisco 1801 Integrated Services Router	1.3.6.1.4.1.9.1.638	3.6.0
cisco1802	Cisco 1802 Integrated Services Router	1.3.6.1.4.1.9.1.639	3.6.0
cisco1803	Cisco 1803 Integrated Services Router	1.3.6.1.4.1.9.1.640	3.6.0
cisco1811	Cisco 1811 Integrated Services Router	1.3.6.1.4.1.9.1.641	3.6.0
cisco1812	Cisco 1812 Integrated Services Router	1.3.6.1.4.1.9.1.642	3.6.0
cisco1841	Cisco 1841 Integrated Services Router	1.3.6.1.4.1.9.1.620	3.6.0
Cisco 2500 Series Routers			
cisco2500	Cisco 2500 Router	1.3.6.1.4.1.9.1.13	3.6.0
cisco2501	Cisco 2501 Router	1.3.6.1.4.1.9.1.17	3.6.0
cisco2501FRADFX	Cisco 2501 Router	1.3.6.1.4.1.9.1.165	3.6.0
cisco2501LANFRADFX	Cisco 2501 Router	1.3.6.1.4.1.9.1.166	3.6.0
cisco2502	Cisco 2502 Router	1.3.6.1.4.1.9.1.18	3.6.0
cisco2502LANFRADFX	Cisco 2502 Router	1.3.6.1.4.1.9.1.167	3.6.0
cisco2503	Cisco 2503 Router	1.3.6.1.4.1.9.1.19	3.6.0
cisco2504	Cisco 2504 Router	1.3.6.1.4.1.9.1.20	3.6.0
cisco2505	Cisco 2505 Router	1.3.6.1.4.1.9.1.21	3.6.0
cisco2506	Cisco 2506 Router	1.3.6.1.4.1.9.1.22	3.6.0
cisco2507	Cisco 2507 Router	1.3.6.1.4.1.9.1.23	3.6.0
cisco2508	Cisco 2508 Router	1.3.6.1.4.1.9.1.24	3.6.0
cisco2509	Cisco 2509 Router	1.3.6.1.4.1.9.1.25	3.6.0
cisco2510	Cisco 2510 Access Server	1.3.6.1.4.1.9.1.26	3.6.0
cisco2511	Cisco 2511 Router	1.3.6.1.4.1.9.1.27	3.6.0

Table 2-7 Supported Cisco Routers in Cisco Prime Network 3.9 (continued)

NE Type	Product Name	SysOID	Product_Version
cisco2512	Cisco 2512 Access Server	1.3.6.1.4.1.9.1.28	3.6.0
cisco2513	Cisco 2513 Router	1.3.6.1.4.1.9.1.29	3.6.0
cisco2514	Cisco 2514 Router	1.3.6.1.4.1.9.1.30	3.6.0
cisco2515	Cisco 2515 Router	1.3.6.1.4.1.9.1.31	3.6.0
cisco2516	Cisco 2516 Router	1.3.6.1.4.1.9.1.42	3.6.0
cisco2517	Cisco 2517 Router	1.3.6.1.4.1.9.1.67	3.6.0
cisco2518	Cisco 2518 Router	1.3.6.1.4.1.9.1.68	3.6.0
cisco2519	Cisco 2519 Router	1.3.6.1.4.1.9.1.69	3.6.0
cisco2520	Cisco 2520 Router	1.3.6.1.4.1.9.1.70	3.6.0
cisco2521	Cisco 2521 Router	1.3.6.1.4.1.9.1.71	3.6.0
cisco2522	Cisco 2522 Router	1.3.6.1.4.1.9.1.72	3.6.0
cisco2523	Cisco 2523 Router	1.3.6.1.4.1.9.1.73	3.6.0
cisco2524	Cisco 2524 Router	1.3.6.1.4.1.9.1.74	3.6.0
cisco2525	Cisco 2525 Router	1.3.6.1.4.1.9.1.75	3.6.0
ciscoPro2501	Cisco Pro 2501	1.3.6.1.4.1.9.1.56	3.6.0
Cisco 2600 Series Multiservice Platform Routers			
cisco2610	Cisco 2610	1.3.6.1.4.1.9.1.185	3.6.0
cisco2610XM	Cisco 2610XM	1.3.6.1.4.1.9.1.466	3.6.0
cisco2610XM	Cisco 2610XM-DC	1.3.6.1.4.1.9.1.466	3.6.0
cisco2610XM	Cisco 2610XM-RP5	1.3.6.1.4.1.9.1.466	3.6.0
cisco2611	Cisco 2611	1.3.6.1.4.1.9.1.186	3.6.0
cisco2611XM	Cisco 2611XM	1.3.6.1.4.1.9.1.467	3.6.0
cisco2611XM	Cisco 2611XM-DC	1.3.6.1.4.1.9.1.467	3.6.0
cisco2611XM	Cisco 2611XM-RP5	1.3.6.1.4.1.9.1.467	3.6.0
cisco2612	Cisco 2612	1.3.6.1.4.1.9.1.187	3.6.0
cisco2613	Cisco 2613	1.3.6.1.4.1.9.1.195	3.6.0
cisco2620	Cisco 2620	1.3.6.1.4.1.9.1.208	3.6.0
cisco2620XM	Cisco 2620XM	1.3.6.1.4.1.9.1.468	3.6.0
cisco2620XM	Cisco 2620XM-DC	1.3.6.1.4.1.9.1.468	3.6.0
cisco2620XM	Cisco 2620XM-RP5	1.3.6.1.4.1.9.1.468	3.6.0
cisco2621	Cisco 2621	1.3.6.1.4.1.9.1.209	3.6.0
cisco2621XM	Cisco 2621XM	1.3.6.1.4.1.9.1.469	3.6.0
cisco2621XM	Cisco 2621XM-DC	1.3.6.1.4.1.9.1.469	3.6.0
cisco2621XM	Cisco 2621XM-RP5	1.3.6.1.4.1.9.1.469	3.6.0
cisco2650	Cisco 2650	1.3.6.1.4.1.9.1.319	3.6.0

Table 2-7 Supported Cisco Routers in Cisco Prime Network 3.9 (continued)

NE Type	Product Name	SysOID	Product_Version
cisco2650XM	Cisco 2650XM	1.3.6.1.4.1.9.1.470	3.6.0
cisco2650XM	Cisco 2650XM-DC	1.3.6.1.4.1.9.1.470	3.6.0
cisco2650XM	Cisco 2650XM-RP5	1.3.6.1.4.1.9.1.470	3.6.0
cisco2651	Cisco 2651	1.3.6.1.4.1.9.1.320	3.6.0
cisco2651XM	Cisco 2651XM	1.3.6.1.4.1.9.1.471	3.6.0
cisco2651XM	Cisco 2651XM-DC	1.3.6.1.4.1.9.1.471	3.6.0
cisco2651XM	Cisco 2651XM-RP5	1.3.6.1.4.1.9.1.471	3.6.0
cisco2691	Cisco 2691	1.3.6.1.4.1.9.1.413	3.6.0
cisco2610M	Cisco 2610M	1.3.6.1.4.1.9.1.418	3.6.0
cisco2610	Cisco2610	1.3.6.1.4.1.9.1.185	3.6.2
Cisco 2800 Series Integrated Services Routers			
cisco2801	Cisco 2801 Integrated Services Router	1.3.6.1.4.1.9.1.619	3.6.0
cisco2811	Cisco 2811 Integrated Services Router	1.3.6.1.4.1.9.1.576	3.6.0
cisco2821	Cisco 2821 Integrated Services Router	1.3.6.1.4.1.9.1.577	3.6.0
cisco2851	Cisco 2851 Integrated Services Router	1.3.6.1.4.1.9.1.578	3.6.0
cisco2811 DC	Cisco 2811 Integrated Services Router with DC power	1.3.6.1.4.1.9.1.576	3.7
cisco2821 DC	Cisco 2821-DC Integrated Services Router	1.3.6.1.4.1.9.1.577	3.7
Cisco 3600 Series Multiservice Platform Routers			
cisco3620	Cisco 3620 Multiservice Platform	1.3.6.1.4.1.9.1.122	3.6.0
cisco3640	Cisco 3640 Multiservice Platform	1.3.6.1.4.1.9.1.110	3.6.0
cisco3660	Cisco 3660 Multiservice Platform	1.3.6.1.4.1.9.1.205	3.6.0
cisco3661Ac	Cisco 3661Ac Multiservice Platform	1.3.6.1.4.1.9.1.338	3.6.0
cisco3661Dc	Cisco 3661Dc Multiservice Platform	1.3.6.1.4.1.9.1.339	3.6.0
cisco3662Ac	Cisco 3662Ac Multiservice Platform	1.3.6.1.4.1.9.1.340	3.6.0
cisco3662AcCo	Cisco 3662AcCo Multiservice Platform	1.3.6.1.4.1.9.1.342	3.6.0

Table 2-7 Supported Cisco Routers in Cisco Prime Network 3.9 (continued)

NE Type	Product Name	SysOID	Product_Version
cisco3662Dc	Cisco 3662Dc Multiservice Platform	1.3.6.1.4.1.9.1.341	3.6.0
cisco3662DcCo	Cisco 3662DcCo Multiservice Platform	1.3.6.1.4.1.9.1.343	3.6.0
ciscoSC3640	Cisco SC3640 Multiservice Platform	1.3.6.1.4.1.9.1.189	3.6.0
Cisco 3700 Series Multiservice Access Routers			
cisco3725	Cisco 3725 Multiservice Access Router	1.3.6.1.4.1.9.1.414	3.6.0
cisco3745	Cisco 3745 Multiservice Access Router	1.3.6.1.4.1.9.1.436	3.6.0
Cisco 3800 Series Integrated Services Routers			
cisco3825	Cisco 3825 Integrated Services Router	1.3.6.1.4.1.9.1.543	3.6.0
cisco3845	Cisco 3845 Integrated Services Router	1.3.6.1.4.1.9.1.544	3.6.0
Cisco 7200 Series Routers			
cisco7202	Cisco 7202 Router	1.3.6.1.4.1.9.1.194	3.6.0
cisco7206	Cisco 7206 Router	1.3.6.1.4.1.9.1.108	3.6.0
cisco7204	Cisco 7204 Router	1.3.6.1.4.1.9.1.125	3.6.0
cisco7204VXR	Cisco 7204 VXR Router	1.3.6.1.4.1.9.1.223	3.6.0
cisco7206VXR	Cisco 7206 VXR Router	1.3.6.1.4.1.9.1.222	3.6.0
cisco7201	cisco 7201 Router	1.3.6.1.4.1.9.1.821	3.6.4
Cisco 7300 Series Routers			
cisco7304	Cisco 7304 Router	1.3.6.1.4.1.9.1.439	3.7
cisco7301	Cisco 7301 Router	1.3.6.1.4.1.9.1.476	3.7
Cisco 7400 Series Routers			
cisco7401ASR	Cisco 7401ASR	1.3.6.1.4.1.9.1.403	3.6.0
Cisco 7500 Series Routers			
cisco7505	Cisco 7505 Router	1.3.6.1.4.1.9.1.48	3.7
cisco7507	Cisco 7507 Router	1.3.6.1.4.1.9.1.45	3.7
cisco7507MX	Cisco 7507MX Router	1.3.6.1.4.1.9.1.290	3.7
cisco7507Z	Cisco 7507Z Router	1.3.6.1.4.1.9.1.288	3.7
cisco7513	Cisco 7513 Router	1.3.6.1.4.1.9.1.46	3.7
cisco7513MX	Cisco 7513MX Router	1.3.6.1.4.1.9.1.291	3.7
cisco7513Z	Cisco 7513Z Router	1.3.6.1.4.1.9.1.289	3.7
cisco7576	Cisco 7576 Router	1.3.6.1.4.1.9.1.204	3.7
Cisco 7600 Series Routers			

Table 2-7 Supported Cisco Routers in Cisco Prime Network 3.9 (continued)

NE Type	Product Name	SysOID	Product_Version
cicso7604sysID	Cisco 7604 sysID Router	1.3.6.1.4.1.9.5.63	3.6.1
cisco7603	Cisco OSR 7603 Router	1.3.6.1.4.1.9.1.401	3.6.1
cisco7603S	Cisco 7603S Router	1.3.6.1.4.1.9.1.862	3.6.1
cisco7604	Cisco 7604 Router	1.3.6.1.4.1.9.1.658	3.6.0
cisco7606	Cisco 7606 Router	1.3.6.1.4.1.9.1.402	3.6.0
cisco7606s	Cisco 7606S Router	1.3.6.1.4.1.9.1.863	3.6.1
cisco7606sysID	Cisco 7606 sysID Router	1.3.6.1.4.1.9.5.54	3.6.1
cisco7609	Cisco 7609 Router	1.3.6.1.4.1.9.1.509	3.6.0
cisco7609S	Cisco 7609S Router	1.3.6.1.4.1.9.1.864	3.6.1
cisco7609sysID	Cisco 7609 sysID Router	1.3.6.1.4.1.9.5.55	3.6.1
cisco7613	Cisco 7613 Router	1.3.6.1.4.1.9.1.528	3.6.0
cisco7613sysID	Cisco 7613 sysID Router	1.3.6.1.4.1.9.5.60	3.6.1
cisco763sysID	Cisco 763 sysID Router	1.3.6.1.4.1.9.5.53	3.6.1
Cisco 10000 Series Routers			
cisco10005	Cisco 10005 Router	1.3.6.1.4.1.9.1.437	3.6.0
cisco10008	Cisco 10008 Router	1.3.6.1.4.1.9.1.438	3.6.0
Cisco 12000 Series Routers			
cisco12004	Cisco 12004 Router	1.3.6.1.4.1.9.1.181	3.6.0
cisco12006	Cisco 12006 Router	1.3.6.1.4.1.9.1.590	3.6.0
cisco12008	Cisco 12008 Router	1.3.6.1.4.1.9.1.182	3.6.0
cisco12010	Cisco 12010 Router	1.3.6.1.4.1.9.1.348	3.6.0
cisco12012	Cisco 12012 Router	1.3.6.1.4.1.9.1.173	3.6.0
cisco12016	Cisco 12016 Router	1.3.6.1.4.1.9.1.273	3.6.0
cisco12404	Cisco 12404 Router	1.3.6.1.4.1.9.1.423	3.6.0
cisco12406	Cisco 12406 Router	1.3.6.1.4.1.9.1.388	3.6.0
cisco12410	Cisco 12410 Router	1.3.6.1.4.1.9.1.394	3.6.0
cisco12416	Cisco 12416 Router	1.3.6.1.4.1.9.1.385	3.6.0
cisco12810	Csico 12810 Router	1.3.6.1.4.1.9.1.478	3.6.0
cisco12816	Cisco 12816 Router	1.3.6.1.4.1.9.1.477	3.6.0
Cisco XR 12000 Series Routers			
cisco12012	Cisco 12012 Router	1.3.6.1.4.1.9.1.173	3.6.0
cisco12004	Cisco 12004 Router	1.3.6.1.4.1.9.1.181	3.6.0
cisco12008	Cisco 12008 Router	1.3.6.1.4.1.9.1.182	3.6.0
cisco12016	Cisco 12016 Router	1.3.6.1.4.1.9.1.273	3.6.0
cisco12010	Cisco 12010 Router	1.3.6.1.4.1.9.1.348	3.6.0
cisco12416	Cisco 12416 Router	1.3.6.1.4.1.9.1.385	3.6.0

Table 2-7 Supported Cisco Routers in Cisco Prime Network 3.9 (continued)

NE Type	Product Name	SysOID	Product_Version
cisco12406	Cisco 12406 Router	1.3.6.1.4.1.9.1.388	3.6.0
cisco12410	Cisco 12410 Router	1.3.6.1.4.1.9.1.394	3.6.0
cisco12816	Cisco 12816 Router	1.3.6.1.4.1.9.1.477	3.6.0
cisco12810	Cisco 12810 Router	1.3.6.1.4.1.9.1.478	3.6.0
cisco12006	Cisco 12006 Router	1.3.6.1.4.1.9.1.590	3.6.0
cisco12404	Cisco 12404 Router	1.3.6.1.4.1.9.1.423	3.6.5
Cisco CRS Carrier Routing System			
ciscoCrs16S	Cisco CRS-1 16-Slot Carrier Routing System	1.3.6.1.4.1.9.1.613	3.6.0
ciscoCrs8S	Cisco CRS-1 8-Slot Single-Shelf System	1.3.6.1.4.1.9.1.643	3.6.0[1]
ciscoCrs4S	Cisco CRS-1 4-Slot Single-Shelf System	1.3.6.1.4.1.9.1.822	3.6.0
CiscoCRS16SB	CISCO_CRS16SB	1.3.6.1.4.1.9.1.1331	3.7.3,3.8
Cisco ASR 9000 Series Aggregation Services Routers			
ciscoASR9010	Cisco ASR 9010 chassis	1.3.6.1.4.1.9.1.1017	3.6.5
ciscoASR9006	Cisco ASR 9006 chassis with DC Power	1.3.6.1.4.1.9.1.1018	3.6.6
ciscoASR9006	Cisco ASR 9006 chassis with AC Power	1.3.6.1.4.1.9.1.1018	3.6.6
Cisco ASR 1000 Series Routers			
ciscoASR1002	Cisco ASR1002 Chassis,4 built-in GE, Dual P/S,4GB DRAM	1.3.6.1.4.1.9.1.923	
ciscoASR1006	Cisco ASR1006 Chassis, Dual P/S	1.3.6.1.4.1.9.1.925	
ciscoASR1004	Cisco ASR1004 Chassis, Dual P/S	1.3.6.1.4.1.9.1.924	
ciscoASR1002F	Cisco ASR 1002-F	1.3.6.1.4.1.9.1.1116	
ciscoASR1013	Cisco ASR1013 Chassis	1.3.6.1.4.1.9.1.1166	
ciscoASR1001	Cisco ASR1001 Chassis	1.3.6.1.4.1.9.1.1165	
Cisco MWR 2900 Series Mobile Wireless Routers			
ciscoMWR2941	MWR-2941-DC	1.3.6.1.4.1.9.1.1014	3.6.6
ciscoMWR2941DCA	MWR-2941-DC-A	1.3.6.1.4.1.9.1.1215	3.7.0.1
Cisco 1900 Series Integrated Services Router			
Cisco1941W-A/K9	CISCO1941W-A/K9	1.3.6.1.4.1.9.1.1095	3.7.1.0.4[2]
Cisco1941W-E/K9	CISCO1941W-E/K9	1.3.6.1.4.1.9.1.1172	3.7.1.0.4[3]
Cisco1941W-N/K9	CISCO1941W-N/K9	1.3.6.1.4.1.9.1.1174	3.7.1.0.4[4]

Table 2-7 Supported Cisco Routers in Cisco Prime Network 3.9 (continued)

NE Type	Product Name	SysOID	Product_Version
Cisco1941W-P/K9	CISCO1941W-P/K9	1.3.6.1.4.1.9.1.1173	3.7.1.0.4[5]
Cisco1941W-C/K9	CISCO1941W-C/K9	1.3.6.1.4.1.9.1.1220	3.7.1.0.4[6]
Cisco 1941/K9	CISCO1941/K9	1.3.6.1.4.1.9.1.1047	3.7.1.0.4[7]
Cisco 2900 Series Integrated Services Router			
cisco2901	CISCO2901/K9	1.3.6.1.4.1.9.1.1046	3.7.1[8]
cisco2911	CISCO2911/K9	1.3.6.1.4.1.9.1.1045	3.7.1[9]
cisco2921	CISCO2921/K9	1.3.6.1.4.1.9.1.1044	3.7.1[10]
cisco2951	CISCO2951/K9	1.3.6.1.4.1.9.1.1043	3.7.1[11]
Cisco 3900 Series Integrated Service Routers			
ciscoISR3945	Cisco ISR 3945 Router	1.3.6.1.4.1.9.1.1041	3.7.1[12]
ciscoISR3925	Cisco ISR 3925/K9 Router	1.3.6.1.4.1.9.1.1042	3.7.1[13]
Cisco Universal Broadband Router 7200 Series			
ciscoUBR7246VXR	Cisco UBR7246VXR	1.3.6.1.4.1.9.1.271	3.7.1
Cisco Univeral Broadband Router 10000 Series			
ciscoUBR10012	Cisco UBR 10012	1.3.6.1.4.1.9.1.317	3.7.1
Cisco 4700 Series Routers			
cisco4700	Cisco 4700 Router	1.3.6.1.4.1.9.1.50	3.7.1
Cisco ASR901 Series Mobile Wireless Routers			
Cisco ASR903 Series Routers			
cicsoAsr903sysID	Cisco ASR903 sysID Router	1.3.6.1.4.1.9.1.1441	3.8
Cisco ASR 5000 Series Routers			
ciscoASR5000	Cisco ASR5000 Chassis	1.3.6.1.4.1.8164	
ciscoASR5500	Cisco ASR5500 Chassis	1.3.6.1.4.1.9.1.1457	

[1]The CRS-8S slots power-shelf racks will list the status as Unknown since the power-shelf is a virtual object and it is NOT FRU-able

[2]Cisco 1941 Router w/ 802.11 a/b/g/n FCC Compliant, 2 onboard GE, 2 EHWIC slots, 256MB CF default, 512MB DRAM default, IP Base

[3]Cisco 1941 Router w/ 802.11 a/b/g/n ETSI Compliant, 2 onboard GE, 2 EHWIC slots, 256MB CF default, 512MB DRAM default, IP Base

[4]Cisco 1941 Router w/ 802.11 a/b/g/n Aus and NZ Compliant, 2 onboard GE, 2 EHWIC slots, 256MB CF default, 512MB DRAM default, IP Base

[5]Cisco 1941 Router w/ 802.11 a/b/g/n Japan Compliant, 2 onboard GE, 2 EHWIC slots, 256MB CF default, 512MB DRAM default, IP Base

[6]Cisco 1941 Router w/ 802.11 a/b/g/n China Compliant, 2 onboard GE, 2 EHWIC slots, 256MB CF default, 512MB DRAM default, IP Base

[7]Cisco 1941 with 2 onboard GE, 2 EHWIC slots, 1 ISM slot, 256MB CF default, 512MB DRAM default, IP Base

[8]Cisco 2901 with 2 onboard GE, 4 EHWIC slots, 2 DSP slots, 1 ISM slot, 256MB CF default , 512MB DRAM default, IP Base

[9]Cisco 2911 with 3 onboard GE, 4 EHWIC slots, 2 DSP slots, 1 ISM slot, 256MB CF default , 512MB DRAM default, IP Base

[10]Cisco 2921 with 3 onboard GE, 4 EHWIC slots, 3 DSP slots, 1 ISM slot, 256MB CF default , 512MB DRAM default, IP Base

[11]Cisco 2951 with 3 onboard GE, 4 EHWIC slots, 3 DSP slots, 1 ISM slot, 256MB CF default , 512MB DRAM default, IP Base

[12]Cisco 3945 with 3 onboard GE, C3900-SPE150/K9, 4 EHWIC slots, 4 DSP slots, 1 ISM slot, 4 SM slots, 256MB CF default, 1 GB DRAM default, IP Base

[13]Cisco 3925 with 3 onboard GE, C3900-SPE100/K9, 4 EHWIC slots, 4 DSP slots, 1 ISM slot, 2 SM slots, 256MB CF default, 1 GB DRAM default, IP Base

Supported Cisco Switches in Cisco Prime Network 3.9

This document includes support information for the following Cisco switches:

- Cisco Catalyst 1900 Series Switches
- Cisco Catalyst 2900 Series Switches
- Cisco ME 3400 Series Ethernet Access Switches
- Cisco Catalyst 3500 XL Series Switches
- Cisco Catalyst 3550 Series Switches
- Cisco Catalyst 3560 Series Switches
- Cisco Catalyst 3750 Series Switches
- Cisco Catalyst 3750 Metro Series Switches
- Cisco Catalyst 4000 Series Switches
- Cisco Catalyst 4500 Series Switches
- Cisco Catalyst 4900 Series Switches
- Cisco ME 4900 Series Ethernet Switch
- Cisco Catalyst 5000 Series Switches
- Cisco Catalyst 6500 Series (CatOS) Switches
- Cisco Catalyst 6500 Series (IOS) Switches
- Cisco ME 6500 Series Ethernet Switches (6524)
- Cisco ME 3600X Ethernet Access Switch
- Cisco ME 3800X Carrier Ethernet Switches
- Cisco Nexus 7000 Series Switches
- Cisco Nexus 5000 Series Switches
- Cisco Nexus 1000 Series Switches
- Cisco ACE 4700 Series Access Control Engine
- Cisco Service Control Engines

Table 2-8 Supported Cisco Switches in Cisco Prime Network 3.9

NE Type	Product Name	SysOID	Product_Version
Cisco Catalyst 1900 Series Switches			
wsc1900LiteFxsysID	catalyst1900	1.3.6.1.4.1.9.5.175	3.7
wsc1900sysID	catalyst1900	.1.3.6.1.4.1.9.5.18	3.7
wsc1900csysID	catalyst1912C	1.3.6.1.4.1.9.5.28	3.7
wsc1900isysID	catalyst1900	1.3.6.1.4.1.9.5.31	3.7
catalyst1912C	catalyst1912C	1.3.6.1.4.1.9.1.175	3.7
Cisco Catalyst 2900 Series Switches			
wsc2948gsysID	Cisco Catalyst WS-C2948 Switch	1.3.6.1.4.1.9.5.42	3.6.0
wsc2900sysID	Cisco Catalyst WS-C2900 Switch	1.3.6.1.4.1.9.5.12	3.6.0
catalyst296024TT	Cisco Catalyst 2960-24TT Switch	1.3.6.1.4.1.9.1.716	3.6.0
catalyst2950t24	Cisco Catalyst 2950T 24 Switch	1.3.6.1.4.1.9.1.359	3.6.0
catalyst295048T	Cisco Catalyst 2950T 48 SI Switch	1.3.6.1.4.1.9.1.559	3.6.0
catalyst295048G	Cisco Catalyst 2950G 48 EI Switch	1.3.6.1.4.1.9.1.429	3.6.0
catalyst295024S	Cisco Catalyst 2950 24S Switch	1.3.6.1.4.1.9.1.430	3.6.0
catalyst295024GDC	Cisco Catalyst 2950G 24 EI DC Switch	1.3.6.1.4.1.9.1.472	3.6.0
catalyst295024G	Cisco Catalyst 2950G 24 EI Switch	1.3.6.1.4.1.9.1.428	3.6.0
catalyst295024C	Cisco Catalyst 2950C 24 Switch	1.3.6.1.4.1.9.1.325	3.6.0
catalyst295024	Cisco Catalyst 2950 24 Switch	1.3.6.1.4.1.9.1.324	3.6.0
catalyst295012G	Cisco Catalyst 2950G 12 EI Switch	1.3.6.1.4.1.9.1.427	3.6.0
catalyst295012	Cisco Catalyst 2950 12 Switch	1.3.6.1.4.1.9.1.323	3.6.0
catalyst2924XLv	Cisco Catalyst 2924 XL Switch	1.3.6.1.4.1.9.1.217	3.6.0
catalyst2924XL	Cisco Catalyst 2924 XL Switch	1.3.6.1.4.1.9.1.183	3.6.0
catalyst2924MXL	Cisco Catalyst 2924M XL Switch	1.3.6.1.4.1.9.1.220	3.6.0
catalyst2924CXLv	Cisco Catalyst 2924C XL Switch	1.3.6.1.4.1.9.1.218	3.6.0
catalyst2924CXL	Cisco Catalyst 2924C XL Switch	1.3.6.1.4.1.9.1.184	3.6.0
catalyst2916m-xl	Cisco Catalyst 2916M XL Switch	1.3.6.1.4.1.9.1.171	3.6.0
catalyst2912XL	Cisco Catalyst 2912 XL Switch	1.3.6.1.4.1.9.1.219	3.6.0

Table 2-8 Supported Cisco Switches in Cisco Prime Network 3.9 (continued)

NE Type	Product Name	SysOID	Product_Version
catalyst2912MfXL	Cisco Catalyst 2912MF XL Switch	1.3.6.1.4.1.9.1.221	3.6.0
catalyst2908xl	Cisco Catalyst 2908 XL Switch	1.3.6.1.4.1.9.1.170	3.6.0
cat2948gL3Dc	Cisco Catalyst C2948G-L3 Ethernet Switch	1.3.6.1.4.1.9.1.386	3.6.0
cat2948gL3	Cisco Catalyst C2948G-L3 Ethernet Switch	1.3.6.1.4.1.9.1.275	3.6.0
c2960-24TC-L	Cisco Catalyst 2960-24TC Switch	1.3.6.1.4.1.9.1.694	3.7.1
catalyst296048	Cisco Catalyst 2960-48TC Switch	1.3.6.1.4.1.9.1.695	3.7.2
c2960S-48TS-L	Cisco Catalyst 2960S-48TS-L	1.3.6.1.4.1.9.1.1266	3.7.2
c2960S-24TS-L	Cisco Catalyst 2960S-24TS-L	1.3.6.1.4.1.9.1.1267	3.7.2
Cisco ME 3400 Series Ethernet Access Switches			
3400-24TS	Cisco Me 3400 Switch-24 10/100 + 2 SFP DC PS	1.3.6.1.4.1.9.1.736	3.6.1[1]
3400-24TS AC	Cisco Me 3400 Software 24PT-10/100 Plus 2PT SFP AC PS	1.3.6.1.4.1.9.1.736	3.6.1[2]
3400-24TS DC	Cisco Me 3400 Software 24PT-10/100 Plus 2PT SFP DC PS	1.3.6.1.4.1.9.1.736	3.6.1[3]
cisco340024TSA	Cisco ME 3400-24TS-A Switch	1.3.6.1.4.1.9.1.736	3.6.1
cisco340024TSD	Cisco ME 3400-24TS-D Switch	1.3.6.1.4.1.9.1.737	3.6.1
3400G-12CS	Cisco ME 3400G-12CS Ethernet Access Switch	1.3.6.1.4.1.9.1.780	3.6.1[4]
ciscoMe3400g12CsA	Cisco ME 3400G-12CS AC Ethernet Access Switch	1.3.6.1.4.1.9.1.780	3.6.1
ciscoMe3400g12CsD	Cisco ME 3400G-12CS DC Ethernet Access Switch	1.3.6.1.4.1.9.1.781	3.6.1
3400G-2CS	Cisco ME 3400-2CS Ethernet Access Switch	1.3.6.1.4.1.9.1.825	3.6.1[5]
ciscoMe3400g2csA	Cisco ME 3400-2CS AC Ethernet Access Switch	1.3.6.1.4.1.9.1.825	3.6.1
ciscoMe3400eg2csA	Cisco ME 3400EG-2CS Ethernet Access Switch	1.3.6.1.4.1.9.1.1007	3.6.5
ciscoMe3400eg12Csm	Cisco ME 3400EG-12CS-M Ethernet Access Switch chassis	1.3.6.1.4.1.9.1.1008	3.6.5
ciscoMe3400e24Tsm	Cisco ME 3400E-24TS-M Ethernet Access Switch chassis	1.3.6.1.4.1.9.1.1009	3.6.5

Table 2-8 Supported Cisco Switches in Cisco Prime Network 3.9 (continued)

NE Type	Product Name	SysOID	Product_Version
Cisco Catalyst 3500 XL Series Switches			
cat3524tXLEn	Cisco Catalyst 3524 PWR XL Switch	1.3.6.1.4.1.9.1.287	3.6.0
cat3548XL	Cisco Catalyst 3548 XL Switch	1.3.6.1.4.1.9.1.278	3.6.0
catalyst3508GXL	Cisco Catalyst 3508G XL Switch	1.3.6.1.4.1.9.1.246	3.6.0
catalyst3512XL	Cisco Catalyst 3512 XL Switch	1.3.6.1.4.1.9.1.247	3.6.0
catalyst3524XL	Cisco Catalyst 3524 XL Switch	1.3.6.1.4.1.9.1.248	3.6.0
catalystC3524PWRXLEn	catalystC3524PWRXLEn	1.3.6.1.4.1.9.1.515	3.6.1
Cisco Catalyst 3550 Series Switches			
catalyst355024	Cisco Catalyst 3550 24 Switch	1.3.6.1.4.1.9.1.366	3.6.0
catalyst355048	Cisco Catalyst 3550 48 Switch	1.3.6.1.4.1.9.1.367	3.6.0
catalyst355012T	Cisco Catalyst 3550 12T Switch	1.3.6.1.4.1.9.1.368	3.6.0
catalyst355012G	Cisco Catalyst 3550 12G Switch	1.3.6.1.4.1.9.1.431	3.6.0
cat355024Dc	Cisco Catalyst 3550 24 DC SMI Switch	1.3.6.1.4.1.9.1.452	3.6.0
cat355024Mmf	Cisco Catalyst 3550 24 FX SMI Switch	1.3.6.1.4.1.9.1.453	3.6.1
catalyst355024PWR	Cisco Catalyst 3550 24 PWR Switch	1.3.6.1.4.1.9.1.485	3.6.0
Cisco Catalyst 3560 Series Switches			
catalyst356024PS	Cisco Catalyst 3560-24PS Switch	1.3.6.1.4.1.9.1.563	3.6.1
catalyst356048PS	Cisco Catalyst 3560-48PS Switch	1.3.6.1.4.1.9.1.564	3.6.0
catalyst3560G24PS	Cisco Catalyst 3560G-24PS Switch	1.3.6.1.4.1.9.1.614	3.6.1
catalyst3560G24TS	Cisco Catalyst 3560G-24TS Switch	1.3.6.1.4.1.9.1.615	3.6.1
catalyst3560G48PS	Cisco Catalyst 3560G-48PS Switch	1.3.6.1.4.1.9.1.616	3.6.1
catalyst3560G48TS	Cisco Catalyst 3560G-48TS Switch	1.3.6.1.4.1.9.1.617	3.6.0
catalyst356024TS	Cisco Catalyst 3560-24TS Switch	1.3.6.1.4.1.9.1.633	3.6.1
catalyst3560X	Cisco Catalyst 3560X	1.3.6.1.4.1.9.1.1227	ANA3.8.X-DP6, ANA3.7.X-DP15

Table 2-8 Supported Cisco Switches in Cisco Prime Network 3.9 (continued)

NE Type	Product Name	SysOID	Product_Version
Cisco Catalyst 3750 Series Switches			
catalyst37xxStack	Catalyst 3750-48/-24/-24T/-24TS/-24FS/ Stack	1.3.6.1.4.1.9.1.516	3.6.0
catalyst375024	Cisco Catalyst 3750-24	1.3.6.1.4.1.9.1.511	3.6.4
catalyst375024PS	Cisco Catalyst 3750-24PS	1.3.6.1.4.1.9.1.536	3.6.4
catalyst375024T	Cisco Catalyst 3750-24T	1.3.6.1.4.1.9.1.514	3.6.4
catalyst375024TS	Cisco Catalyst 3750 - 24TS	1.3.6.1.4.1.9.1.513	3.6.4
catalyst375048	Cisco Catalyst 3750-48	1.3.6.1.4.1.9.1.512	3.6.4
catalyst375048PS	Cisco Catalyst 3750-48PS	1.3.6.1.4.1.9.1.535	3.6.4
catalyst3750G16TD	Cisco Catalyst 3750G-16TD	1.3.6.1.4.1.9.1.591	3.6.4
catalyst3750G24PS	Cisco Catalyst 3750G-24PS	1.3.6.1.4.1.9.1.602	3.6.4
catalyst3750G24TS1U	Cisco Catalyst 3750G-24TS-1U	1.3.6.1.4.1.9.1.624	3.6.4
catalyst3750G48PS	Cisco Catalyst 3750G-48PS	1.3.6.1.4.1.9.1.603	3.6.4
catalyst3750G48TS	Cisco Catalyst 3750G-48TS	1.3.6.1.4.1.9.1.604	3.6.4
catalyst3750Ge12Sfp	Cisco Catalyst 3750G-12Sfp	1.3.6.1.4.1.9.1.530	3.6.4
catalyst3750Ge12SfpDc	Cisco catalyst 3750G-12S-SD	1.3.6.1.4.1.9.1.688	3.6.4
catalyst3750G24WS50	Cisco Catalyst 3750G-24WS-50	1.3.6.1.4.1.9.1.779	3.6.4
catalyst3750E48TD	Cisco Catalyst 3750E-48TD	1.3.6.1.4.1.9.1.790	3.6.4
catalyst3750E24PD	Cisco Catalyst 3750E-24PD	1.3.6.1.4.1.9.1.792	3.6.4
catalyst3750E24TD	Cisco Catalyst 3750E-24TD	1.3.6.1.4.1.9.1.789	3.6.4
catalyst3750E48PD	Cisco Catalyst 3750E-48PD	1.3.6.1.4.1.9.1.791	3.6.4
catalyst3750G24WS25	Cisco Catalyst 3750G-24WS-25	1.3.6.1.4.1.9.1.778	3.6.4
catalyst3750X	Cisco Catalyst 3750X	1.3.6.1.4.1.9.1.1405	ANA3.8.X-DP6, ANA3.7.X-DP15
Cisco Catalyst 3750 Metro Series Switches			
catalyst375024ME	Cisco Catalyst 3750 Metro 24-DC Switch	1.3.6.1.4.1.9.1.574	3.6.0
Cisco Catalyst 4000 Series Switches			
wsc4003sysID	Cisco Catalyst 4003 Switch	1.3.6.1.4.1.9.5.40	3.6.0
wsc4006sysID	Cisco Catalyst 4006 Switch	1.3.6.1.4.1.9.5.46	3.6.0
catalyst4kGateway	Cisco Catalyst 4604 Access Gateway	1.3.6.1.4.1.9.1.318	3.6.0

Table 2-8 Supported Cisco Switches in Cisco Prime Network 3.9 (continued)

NE Type	Product Name	SysOID	Product_Version
cat4232L3	Cisco Catalyst 4006 Switch	1.3.6.1.4.1.9.1.300	3.6.0
cat4840gL3	Cisco Catalyst 4840G Switch	1.3.6.1.4.1.9.1.312	3.6.0
cisco4000	Cisco Catalyst 4000 Switch	1.3.6.1.4.1.9.1.7	3.6.0
Cisco Catalyst 4500 Series Switches			
cisco4500	Cisco Catalyst 4500 switch	1.3.6.1.4.1.9.1.14	3.6.0
cat4506	Cisco Catalyst 4506 switch	1.3.6.1.4.1.9.1.502	3.6.0
wsc4506sysID	Cisco Catalyst 4506 switch	1.3.6.1.4.1.9.5.59	3.6.0
cat4507	Cisco Catalyst 4507 switch	1.3.6.1.4.1.9.1.501	3.6.0
cat4503	Cisco Catalyst 4503 switch	1.3.6.1.4.1.9.1.503	3.6.0
wsc4503sysID	Cisco Catalyst 4503 Switch	1.3.6.1.4.1.9.5.58	3.6.3
WS-C4503-E	Cisco Catalyst 4503E Switch	1.3.6.1.4.1.9.1.874	3.6.6
WS-C4507R-E	Cisco Catalyst 4507R-E Switch	1.3.6.1.4.1.9.1.876	3.6.6
WS-C4506-E	Cisco Catalyst 4506-E Switch	1.3.6.1.4.1.9.1.875	3.6.7
WS-C4510R	Cisco Catalyst 4510R Switch	1.3.6.1.4.1.9.1.537	3.6.7
WS-C4510R-E	Cisco Catalyst 4510R-E Switch	1.3.6.1.4.1.9.1.877	3.6.7
WS-C4507R+E	Cisco Catalyst 4507R+E Switch	1.3.6.1.4.1.9.1.1286	3.7.2
WS-C4510R+E	Cisco Catalyst 4510R+E Switch	1.3.6.1.4.1.9.1.1287	3.7.2
Cisco Catalyst 4900 Series Switches			
catalyst4948	Cisco Catalyst 4948 Switch	1.3.6.1.4.1.9.1.626	3.6.1
catalyst494810GE	Cisco Catalyst 4948 10 Gigabit Ethernet Switch	1.3.6.1.4.1.9.1.659	3.6.1
WS-C4900M	Base System with 8-port (X2) and 2 Half Slots	1.3.6.1.4.1.9.1.917	3.7
WS-C4948E	Cisco Catalyst 4948E Switch	1.3.6.1.4.1.9.1.1178	3.7.1
WS-C4948E-F	Cisco Catalyst 4948E-F Switch	1.3.6.1.4.1.9.1.1327	ANA-3.7.2-DP4
Cisco ME 4900 Series Ethernet Switch			
ME-4924-10GE	Cisco ME 4924-10GE Ethernet Aggregation Switch	1.3.6.1.4.1.9.1.788	3.6.1
Cisco Catalyst 5000 Series Switches			
cisco5002	Cisco Catalyst 5002 Switch	1.3.6.1.4.1.9.5.29	3.7
cisco5000	Cisco Catalyst 5000 Switch	1.3.6.1.4.1.9.5.7	3.7
catalyst5500	Cisco Catalyst 5500 Switch	1.3.6.1.4.1.9.5.17	3.7
catalyst5505	Cisco Catalyst 5505 Switch	1.3.6.1.4.1.9.5.34	3.7
catalyst5509	Cisco Catalyst 5509 Switch	1.3.6.1.4.1.9.5.36	3.7
Cisco Catalyst 6500 Series (CatOS) Switches			
wsc6009sysID	Catalyst 6009	1.3.6.1.4.1.9.5.39	3.6.0

Table 2-8 Supported Cisco Switches in Cisco Prime Network 3.9 (continued)

NE Type	Product Name	SysOID	Product_Version
wsc6506sysID	Catalyst 6506	1.3.6.1.4.1.9.5.45	3.6.0
wsc6509nebasysID	Catalyst 6509NEBA	1.3.6.1.4.1.9.5.61	3.6.4
wsc6509nebsysID	Catalyst 6509-NEB	1.3.6.1.4.1.9.5.47	3.6.0
wsc6513sysID	Catalyst 6513	1.3.6.1.4.1.9.5.50	3.6.0
wsc6509sysID	Catalyst 6509	1.3.6.1.4.1.9.5.44	3.6.0
wsc6509esysID	Catalyst 6509-E	1.3.6.1.4.1.9.5.44	3.6.0
wsc6504esysID	Catalyst 6504-E	1.3.6.1.4.1.9.5.64	3.6.1
wsc6503sysID	Catalyst 6503	1.3.6.1.4.1.9.5.56	3.6.1
cat6500FirewallSm	Catalyst 6500 Firewall Services Module	1.3.6.1.4.1.9.1.522	3.6.1
cat6500SslSm	Catalyst 6500 SSL Services Module	1.3.6.1.4.1.9.1.554	3.6.1
Cisco Catalyst 6500 Series (IOS) Switches			
WS-C6509-NEB-A	Cisco Catalyst 6509-NEB-A Switch	1.3.6.1.4.1.9.1.534	3.6.0
WS-C6509-NEB	Cisco Catalyst 6509-NEB Switch	1.3.6.1.4.1.9.1.310	3.6.0
WS-C6503	Cisco Catalyst 6503 Switch	1.3.6.1.4.1.9.1.449	3.6.0
WS-C6506	Cisco Catalyst 6506 Switch	1.3.6.1.4.1.9.1.282	3.6.0
WS-C6509	Cisco Catalyst 6509 Switch	1.3.6.1.4.1.9.1.283	3.6.0
WS-C6504-E	Cisco Catalyst 6504-E Switch Chassis	1.3.6.1.4.1.9.1.657	3.6.0
WS-C6513	Cisco Catalyst 6513 Switch	1.3.6.1.4.1.9.1.400	3.6.0
cisco6500VSS	Cisco Catalyst 6500 VSS	1.3.6.1.4.1.9.1.896	3.6.3
WS-C6509VE	Cisco Catalyst 6509-V-E hassis	1.3.6.1.4.1.9.1.832	ANA 3.7.x-DP09
Cisco ME 6500 Series Ethernet Switches (6524)			
cisco6524 (ME-C6524GS-8S)	Cisco ME 6524	1.3.6.1.4.1.9.1.719	3.6.0
cisco6524 (ME-C6524GT-8S)	Cisco ME 6524	1.3.6.1.4.1.9.1.720	3.6.0
Cisco ME 3600X Ethernet Access Switch			
ciscoME3600x24FSM	Cisco ME-3600X-24FSM	1.3.6.1.4.1.9.1.1250	3.7.1
ciscoME3600x24TSM	Cisco ME-3600X-24TSM	1.3.6.1.4.1.9.1.1251	3.7.1
Cisco ME 3800X Carrier Ethernet Switches			

Table 2-8 Supported Cisco Switches in Cisco Prime Network 3.9 (continued)

NE Type	Product Name	SysOID	Product_Version
ciscoME3800X24FSM	Cisco ME-3800X-24FSM	1.3.6.1.4.1.9.1.1252	3.7.1
Cisco Nexus 7000 Series Switches			
N7K-C7010	Cisco Nexus 7000 Series 10 Slot Chassis	1.3.6.1.4.1.9.12.3.1.3.612	3.7.1
N7K-C7018	Cisco Nexus 7000 Series 18 Slot Chassis	1.3.6.1.4.1.9.12.3.1.3.777	3.7.1
Cisco Nexus 5000 Series Switches			
N5K-C5020P-BF	Cisco Nexus 5000 2RU Chassis no PS, 5 Fan Modules, 40 ports (req SFP+)	1.3.6.1.4.1.9.12.3.1.3.719	3.7.2
cevChassisN5kC5020pBd	Cisco Nexus 5020 Switch	1.3.6.1.4.1.9.12.3.1.3.720	3.7.2
N5K-C5010P-BF	Cisco Nexus 5000 1RU Chassis no PS, 2 Fan Modules, 20 ports (req SFP+)	1.3.6.1.4.1.9.12.3.1.3.798	ANA 3.7.x-DP08
Cisco Nexus 1000 Series Switches			
Nexus 1000V	Nexus 1000 Virtual Network Switch	1.3.6.1.4.1.9.12.3.1.3.840	ANA 3.7.x-DP09, CiscoPrimeNetwork-3.8-DP1
Cisco ACE 4700 Series Access Control Engine			
ciscoACE4710	Cisco ACE 4710 Switch	1.3.6.1.4.1.9.1.824	3.7.1
Cisco Service Control Engines			
sce2000	Cisco SCE 2000 Series Service Control Engine	1.3.6.1.4.1.5655.1.3	3.7

[1, 2, 3]Same as cisco340024TSA.Differs based on chassis/power supply.

[4]Same as ciscoMe3400g12CsA.Differs based on chassis/power supply.

[5]Same as ciscoMe3400g2csA.Differs based on chassis/power supply.



CHAPTER 3

Support Information for Cisco Security Appliances

This chapter contains support information for Virtual Network Elements (VNEs) that manage Cisco security appliances in Cisco Prime Network 3.9.

- Cisco Adaptive Security Appliance 5550 Series, page 3-1
- Cisco Adaptive Security Appliance 5580 Series, page 3-3
- Supported Technologies on Cisco Security Appliances, page 3-5

Note For more information about the technologies described in this chapter , see Part 2 Technology Support.

Cisco Adaptive Security Appliance 5550 Series

This section includes the following information about Cisco ASA 5550 Series security appliances (for information on the NE types supported in Cisco Prime Network 3.9, see Cisco Adaptive Security Appliance 5550 Series):

- Cisco ASA 5550 Series—Supported Software Versions, page 3-1
- Cisco ASA 5550 Series—Supported Topologies, page 3-2
- Cisco ASA 5550 Series—Supported Modules, page 3-2
- Cisco ASA 5550 Series—Supported Technologies, page 3-2
- Cisco ASA 5550 Series—Supported Service Events, page 3-2

Cisco ASA 5550 Series—Supported Software Versions

Table 3-1 Supported Software Versions for Cisco ASA 5550 Series—Cisco Prime Network 3.9

Software Version	Product_Version
7.2(3)12	3.6.3

Cisco ASA 5550 Series—Supported Topologies

Table 3-2 Supported Topologies for Cisco ASA 5550 Series—Cisco Prime Network 3.9

Topology Type	Link Type	Product_Version
Ethernet	Ethernet	3.6.3

Cisco ASA 5550 Series—Supported Modules

Table 3-3 Supported Modules for Cisco ASA 5550 Series—Cisco Prime Network 3.9

Module Name	Product_Version	Module Description
SSM-4GE-INC	3.6.3	SSM-4GE Included with ASA 5550 System

Cisco ASA 5550 Series—Supported Technologies

The following technologies are supported by the Cisco ASA 5550 Series in Cisco Prime Network 3.9:

- IP, page 3-6
- Ethernet, page 3-9
- Hardware, page 3-14
- Serial, page 3-16

Cisco ASA 5550 Series—Supported Service Events

Table 3-4 Supported Service Events for Cisco ASA 5550 Series—Cisco Prime Network 3.9

Event Name	Product_Version	Expedited
Active IP Interfaces Found	3.6.3	Y
All IP Interfaces Down	3.6.3	Y
BGP process up	3.6.3	N
Card Down	3.6.3	Y
Card In	3.6.3	Y
Card Out	3.6.3	Y
Card Up	3.6.3	Y
CPU utilization exceeded upper threshold	3.6.3	N
Device Unsupported	3.6.3	N
Keepalive configured	3.6.3	N

Table 3-4 Supported Service Events for Cisco ASA 5550 Series—Cisco Prime Network 3.9

Event Name	Product_Version	Expedited
Keepalive not configured	3.6.3	N
Layer 2 Tunnel Down	3.6.3	N
Link up	3.6.3	N
Memory utilization exceeded upper threshold	3.6.3	N
Module Unsupported	3.6.3	N
Rx utilization exceeded upper threshold	3.6.3	N
Tx utilization exceeded upper threshold	3.6.3	N
fan-tray down	Prime Network 3.8	N
fan-tray out	Prime Network 3.8	N
power-supply down	Prime Network 3.8	N

Cisco Adaptive Security Appliance 5580 Series

This section includes the following information about Cisco ASA 5580 Series security appliances (for information on the NE types supported in Cisco Prime Network 3.9, see Cisco Adaptive Security Appliance 5580 Series):

This section contains the following topics:

- Cisco ASA 5580 Series—Supported Software Versions, page 3-3
- Cisco ASA 5580 Series—Supported Topologies, page 3-4
- Cisco ASA 5580 Series—Supported Modules, page 3-4
- Cisco ASA 5580 Series—Supported Technologies, page 3-4
- Cisco ASA 5580 Series—Supported Service Events, page 3-4

Cisco ASA 5580 Series—Supported Software Versions

Table 3-5 Supported Software Versions for Cisco ASA 5580 Series—Cisco Prime Network 3.9

Software Version	Product_Version
8.1(2)	3.7

Table 3-5 Supported Software Versions for Cisco ASA 5580 Series—Cisco Prime Network 3.9

Software Version	Product_Version
8.1(2)12	3.7

Cisco ASA 5580 Series—Supported Topologies

Table 3-6 Supported Topologies for Cisco ASA 5580 Series—Cisco Prime Network 3.9

Topology Type	Link Type	Product_Version
Ethernet	Ethernet	3.7

Cisco ASA 5580 Series—Supported Modules

Table 3-7 Supported Modules for Cisco ASA 5580 Series—Cisco Prime Network 3.9

Module Name	Product_Version	Module Description
ASA5580-4GE-CU	3.7	Cisco ASA 5580 4-port 10/100/1000 Ethernet interface card, RJ45
ASA5580-4GE-FI	3.7	Cisco ASA 5580 4-port Gigabit Ethernet fiber interface card, SR, LC
ASA5580-2X10GE-SR	3.7	Cisco ASA 5580 2-port 10 Gigabit Ethernet fiber interface card, SR, LC

Cisco ASA 5580 Series—Supported Technologies

The following technologies are supported by the Cisco ASA 5580 Series in Cisco Prime Network 3.9:

- IP, page 3-6
- Ethernet, page 3-9
- Hardware, page 3-14
- Serial, page 3-16

Cisco ASA 5580 Series—Supported Service Events

Table 3-8 Supported Service Events for Cisco ASA 5580 Series—Cisco Prime Network 3.9

Event Name	Product_Version	Expedited
Active IP Interfaces Found	3.7	Y

Table 3-8 Supported Service Events for Cisco ASA 5580 Series—Cisco Prime Network 3.9

Event Name	Product_Version	Expedited
All IP Interfaces Down	3.7	Y
BGP process up	3.7	N
Card Down	3.7	Y
Card In	3.7	Y
Card Out	3.7	Y
Card Up	3.7	Y
CPU utilization exceeded upper threshold	3.7	N
Device Unsupported	3.7	N
Keepalive configured	3.7	N
Keepalive not configured	3.7	N
Layer 2 Tunnel Down	3.7	N
Link up	3.7	N
Memory utilization exceeded upper threshold	3.7	N
Module Unsupported	3.7	N
Rx utilization exceeded upper threshold	3.7	N
Tx utilization exceeded upper threshold	3.7	N
fan-tray down	Prime Network 3.8	N
fan-tray out	Prime Network 3.8	N
power-supply down	Prime Network 3.8	N

Supported Technologies on Cisco Security Appliances

The following sections list the objects and attributes that are supported on Cisco security appliances in Cisco Prime Network 3.9 per technology:

- IP, page 3-6
- Ethernet, page 3-9
- Hardware, page 3-14
- Serial, page 3-16

IP

Table 3-9 IP Attribute Support on Cisco Security Appliances—Cisco Prime Network 3.9

Attribute	ASA5550	ASA5580
IMO Name—IIPInterface		
IP Address	Y	Y
Subnetwork Mask	Y	Y
IP Interface Addresses Array	Y	Y
Interface Name	Y	Y
Interface Description	Y	Y
IP Interface State	Y	Y
OSPF Interface Cost		
Broadcast Address		
MTU		
Lookup Method		
Address Resolution Type		
ARP Timeout		
Secured ARP		
ICMP Mask Reply		
IGMP Proxy		
HSRP Groups		
IP Multiplexing Table		
IANA Type		
Containing CTPs		
Contained CTPs		
IMO Name—IIPMuxEntry		
Termination Point		
Destination IP Subnet		
IMO Name—IRoutingEntity		
Routing Table	Y	Y
ARP Entity	Y	Y
Routing Table Changes		
Name	Y	Y
Logical Sons	Y	Y
IMO Name—IRoutingEntry		
Destination IP Subnet	Y	Y
Next Hop IP Address	Y	Y

Table 3-9 IP Attribute Support on Cisco Security Appliances—Cisco Prime Network 3.9

Attribute	ASA5 550	ASA5 580
Type	Y	Y
Routing Protocol Type	Y	Y
Outgoing Interface Name	Y	Y
IMO Name—IARPEntity		
ARP Table	Y	Y
IMO Name—IARPEntry		
IP Address	Y	Y
MAC Address	Y	Y
Port	Y	Y
Entry Type	Y	Y
IMO Name—IIPPool		
IP Address Pool Entries		
Name		
Index		
IMO Name—IIPRangeBasedIPPoolEntry		
Start IP Address		
End IP Address		
Unused Addresses		
Used Addresses		
Reserved Addresses		
IMO Name—IIPSubnetBasedIPPoolEntry		
IP Subnet		
Unused Addresses		
Used Addresses		
Reserved Addresses		
IMO Name—HSRPGroupEntry		
Group Number		
Port Description		
Priority		
Coupled Router		
State		
Tracking Interfaces		
Virtual IP Address		
Virtual MAC Address		
IMO Name—ITunnelGRE		
Name		

Table 3-9 IP Attribute Support on Cisco Security Appliances—Cisco Prime Network 3.9

Attribute	ASA5550	ASA5580
Tunnel Destination and Source		
IP Address		
IP Interface State		
IANA Type		
Containing CTPs		
Contained CTPs		
Keep Alive Time		
Keep Alive Retry		
IMO Name—IVrrpGroupEntry		
Group Number		
State		
Port Description		
Master IP Address		
Primary IP Address		
Priority		
Virtual Mac Address		
Preempt Mode		
Admin State		
Advertisement Interval		
Tracking Interfaces		
IMO Name—IIPSLAResponderService		
responderStatus		
TWAMPResponderStatus		
tcpConnect		
udpEcho		
IMO Name—IIPAddressPortPair		
type		
ipAddress		
port		

Ethernet

Table 3-10 Ethernet Attribute Support on Cisco Security Appliances—Cisco Prime Network 3.9

Attribute	ASA5550	ASA5580
IMO Name—ILinkAggregationGroup802dot3ad		
dot3adAggMACAddress		
dot3adAggActorSystemPriority		
dot3adAggActorSystemID		
dot3adAggActorAdminKey		
dot3adAggActorOperKey		
dot3adAggPartnerSystemID		
dot3adAggPartnerSystemPriority		
dot3adAggPartnerOperKey		
dot3adAggCollectorMaxDelay		
GroupNumber		
AggregationProtocolType		
MacAddress		
ChannelAdminStatus		
ChannelOperStatus		
IMO Name—IEthernet		
MAC Address	Y	Y
Duplex Mode		
Output Flow Control		
Input Flow Control		
IANA Type	Y	Y
Containing CTPs		
Contained CTPs		
Port Type		
isElmiEnabled		
isLOAMEnabled		
IMO Name—IVlanInterface		
Mode		
Native VLAN Identification		
Virtual LAN Table		
IANA Type		
Containing CTPs		
Contained CTPs		

Table 3-10 Ethernet Attribute Support on Cisco Security Appliances—Cisco Prime Network 3.9

Attribute	ASA5550	ASA5580
vlanAdminType		
vlanencapType		
getAccess		
Allowed Vlans		
IMO Name—IVlanEncapMux		
IANA Type		
Containing CTPs		
Contained CTPs		
IMO Name—IVlanMapping		
direction		
vlanMatchCriteria		
vlanRewriteDefinition		
Drop		
Vlan		
innerVlan		
translatedVlan		
translatedInnerVlan		
IMO Name—IIEEE802		
VLAN Identification		
Binding Information		
Binding Status		
IANA Type		
Containing CTPs		
Contained CTPs		
IMO Name—IStpService		
StpProtocol		
StpMaxAge		
StpHelloTime		
StpBridgeForwardDelay		
StpInstanceInfoTable		
Same as ISystemService		
StpUplinkFastState		
StpBackboneFastState		
StpForwardDelay		
StpBridgeMaxAge		
StpBridgeHelloTime		

Table 3-10 Ethernet Attribute Support on Cisco Security Appliances—Cisco Prime Network 3.9

Attribute	ASA5550	ASA5580
IMO Name—IMstService		
MstProperties		
Same as IStpService		
IMO Name—IPvstpService		
UpLinkFast		
BackboneFast		
IMO Name—IMstProperties		
MstForceVersion		
MstCfgIdFmtSel		
MstExternalRootCost		
MstMaxInstances		
MstCfgIdName		
MstCfgIdRevLevel		
IMO Name—IStpInstanceInfo		
Object Identification		
StpBridgeId		
BridgePriority		
Designated Parent and Root Bridges		
StpRootCost		
IsRoot		
StpRootPort		
StpPortInfoTable		
STP Instance Id		
Vlan Id		
StpDesignatedBridge		
StpDesignatedRoot		
IMO Name—IMstInstanceInfo		
MstVlanIds		
Same as IStpInstanceInfo		
IMO Name—IPvstpInstanceInfo		
Protocol Type		
StpBridgeMaxAge		
StpBridgeHelloTime		
StpBridgeForwardDelay		
StpProtocolSpecification		
StpVlanId		

Table 3-10 Ethernet Attribute Support on Cisco Security Appliances—Cisco Prime Network 3.9

Attribute	ASA5550	ASA5580
StpForwardDelay		
StpMaxAge		
IMO Name—IRstpInstanceInfo		
StpForceVersion		
Same as IStpInstanceInfo		
IMO Name—IStpPortInfo		
StpPort		
StpPortPriority		
StpPortState		
StpPortPathCost		
StpPortEdgePort		
StpPortPointToPoint		
StpPortRole		
StpDesignatedPortIdentifier		
StpDesignatedBridge		
StpPortIdentifier		
StpPortBpduGuardState		
StpPortBpduFilterState		
IMO Name—IMstPortInfo		
MstPortHelloTime		
Same as IStpPortInfo		
IMO Name—IPvstpPortInfo		
PvstpPortFastState		
IMO Name—IEthernetChannel		
Group Number		
Bandwidth		
Aggregation Protocol		
IANA Type		
Containing CTPs		
Contained CTPs		
Mac Address		
Admin Status		
Oper Status		
IMO Name—ITokenRingLayer2		
MAC Address		
IANA Type		

Table 3-10 Ethernet Attribute Support on Cisco Security Appliances—Cisco Prime Network 3.9

Attribute	ASA5550	ASA5580
Containing CTPs		
Contained CTPs		
IMO Name—ITokenRingLayer1		
Same as IPhysicalLayer		
IMO Name—IVtpService		
Version		
OperatingMode		
DomainName		
ConfigurationRevision		
isPruningEnabled		
isAuthenticationEnabled		
IMO Name—IREPService		
version		
administrativeVlan		
notificationEnabled		
IMO Name—IREPSegmentInfo		
segmentId		
segmentComplete		
IMO Name—IREPPortInfo		
portName		
portKey		
segmentId		
portType		
portRole		
operStatus		
blockedVlans		
preemptTimer		
lslAgeoutTimer		
remoteDeviceName		
remoteDeviceMac		
remotePortName		
configuredLoadBalancingBlockedVlans		
IMO Name—IBridgeILan		
Id		
IMO Name—IIBBridgeEntry		
IS Id		

Table 3-10 Ethernet Attribute Support on Cisco Security Appliances—Cisco Prime Network 3.9

Attribute	ASA5550	ASA5580
IBridge		
BBridge		

Hardware

Table 3-11 Hardware Attribute Support on Cisco Security Appliances—Cisco Prime Network 3.9

Attribute	ASA5550	ASA5580
IMO Name—IChassis		
Description		Y
Equipment Holder Type	Y	Y
Contained Equipment Holders		
Contained Equipments		
Serial Number		Y
IMO Name—IShelf		
Description		
Status		
Equipment Holder Type		
Contained Equipment Holders		
Contained Equipments		
Serial Number		
IMO Name—IModule		
Module Name	Y	Y
Module Description	Y	Y
Software Version	Y	Y
Operational Status	Y	
Hardware Type + Version	Y	Y
Managed IP Address		
Redundant Equipment		
Configured Redundancy		
Redundancy Status		
Operational Status Last Changed		
Supported Physical Termination Points		
Serial Number (soft property)	Y	Y
Slots Number		

Table 3-11 Hardware Attribute Support on Cisco Security Appliances—Cisco Prime Network 3.9

Attribute	ASA5550	ASA5580
IMO Name—IPowerSupply		
Same as IModule		
IMO Name—IFanTray		
Same as IModule		
IMO Name—IPluggableTransceiver		
ConnectorDescription		
PID		
ConnectorSerialNumber		
ConnectorType		
PluggablePortState		
PluggableType		
IMO Name—IManagedElement		
IP Address	Y	Y
Communication State	Y	Y
Investigation State	Y	Y
Element Category	Y	Y
Element Type and Key	Y	Y
Device Name	Y	Y
System Name	Y	Y
System Description	Y	Y
Up Time	Y	Y
Software Version	Y	Y
Vendor Identity	Y	Y
Memory and CPU Usage	Y	Y
DRAM Free		
DRAM Used		
Flash Device Size	Y	
NVRAM Size	Y	
Processor DRAM		
Sys Contact	Y	Y
Sys Location	Y	Y
Serial Number	Y	Y
File Systems		
IMO Name—IContext		
Name		
Bounded Connections		

Table 3-11 Hardware Attribute Support on Cisco Security Appliances—Cisco Prime Network 3.9

Attribute	ASA5550	ASA5580
IP Address Pools		
Forwarding Components List		
Traffic Descriptors List		
Tunnel Containers List		
Data Link Aggregation Containers List		
IMO Name—ISystemService		
Type		
Status		
Up Time	Y	Y
IMO Name—IBridge		
Bridge Table		
Type		
MAC Address		
IP Interface		
Name		
Logical Sons		
Vlan Type		
IMO Name—IBridgeEntry		
Destination MAC		
Outgoing Interface		

Serial

Table 3-12 Serial Attribute Support on Cisco Security Appliances—Cisco Prime Network 3.9

Attribute	ASA5550	ASA5580
IMO Name—IPhysicalLayer		
Media Type	Y	Y
Clocking Source		
Maximum Speed	Y	Y
Is Internal Port	Y	Y
Discarded Bandwidth		
Dropped Bandwidth		
Input Bandwidth		

Table 3-12 Serial Attribute Support on Cisco Security Appliances—Cisco Prime Network 3.9

Attribute	ASA5550	ASA5580
Output Bandwidth		
Discarded and Received Input Data Counters		
Dropped and Forward Output Data Counters		
Administrative Status	Y	Y
Operational Status	Y	Y
Last Changed		
IANA Type	Y	Y
Containing CTPs		
Contained CTPs		
Port Alias	Y	Y
Location	Y	Y
Sending Alarms	Y	Y
Connector Description	Y	
Part ID	Y	
Connector Serial Num	Y	
Product	Y	Y
Status	Y	Y
Managed	Y	Y



CHAPTER 4

Support Information for Cisco Access Servers

This chapter contains support information for Virtual Network Elements (VNEs) that manage Cisco access servers in Cisco Prime Network 3.9.

- Cisco Access Server 5800 Series, page 4-1
- Supported Technologies on Cisco Access Servers, page 4-3

Note For more information about the technologies described in this chapter , see Part 2 Technology Support.

Cisco Access Server 5800 Series

This section includes the following information about Cisco AS 5800 Series access servers (for information on the NE types supported in Cisco Prime Network 3.9, see Cisco Access Server 5800 Series):

- Cisco AS 5800 Series—Supported Software Versions, page 4-1
- Cisco AS 5800 Series—Supported Topologies, page 4-2
- Cisco AS 5800 Series—Supported Modules, page 4-2
- Cisco AS 5800 Series—Supported Technologies, page 4-2
- Cisco AS 5800 Series—Supported Service Events, page 4-3

Cisco AS 5800 Series—Supported Software Versions

Table 4-1 Supported Software Versions for Cisco AS 5800 Series—Cisco Prime Network 3.9

Software Version	Product_Version
IOS 12.1(11b)	3.7.1

Cisco AS 5800 Series—Supported Topologies

Table 4-2 Supported Topologies for Cisco AS 5800 Series—Cisco Prime Network 3.9

Topology Type	Link Type	Product_Version
Business	Business	3.7.1
Ethernet	Ethernet	3.7.1
Physical Layer	Physical Layer	3.7.1

Cisco AS 5800 Series—Supported Modules

Table 4-3 Supported Modules for Cisco AS 5800 Series—Cisco Prime Network 3.9

Module Name	Product_Version	Module Description
1.3.6.1.4.1.9.12.3.1.9.12	3.7.1	
AS5800-DSC	3.7.1	Dial Shelf Controller
1.3.6.1.4.1.9.12.3.1.9.12.10	3.7.1	
1.3.6.1.4.1.9.12.3.1.9.12.2	3.7.1	12 Port CE1
.1.3.6.1.4.1.9.12.3.1.9.12.3	3.7.1	
.1.3.6.1.4.1.9.12.3.1.9.12.4	3.7.1	
.1.3.6.1.4.1.9.12.3.1.9.12.5	3.7.1	
.1.3.6.1.4.1.9.12.3.1.9.12.6	3.7.1	
.1.3.6.1.4.1.9.12.3.1.9.12.7	3.7.1	144 Port MICA Modem
.1.3.6.1.4.1.9.12.3.1.9.12.8	3.7.1	
.1.3.6.1.4.1.9.12.3.1.9.12.9	3.7.1	
AS5800-1FE-DSI	3.7.1	1FE Dial Shelf Interconnect

Cisco AS 5800 Series—Supported Technologies

The following technologies are supported by the Cisco AS 5800 Series in Cisco Prime Network 3.9:

- IP, page 4-4
- Routing Protocols, page 4-7
- Ethernet, page 4-9
- TDM/DSx, page 4-14
- Security, page 4-17
- Hardware, page 4-18
- Serial, page 4-20

Cisco AS 5800 Series—Supported Service Events

Table 4-4 Supported Service Events for Cisco AS 5800 Series—Cisco Prime Network 3.9

Event Name	Product_Version	Expedited
Active IP Interfaces Found	3.7.1	Y
All IP Interfaces Down	3.7.1	Y
BGP process up	3.7.1	N
Card Down	3.7.1	Y
Card In	3.7.1	Y
Card Out	3.7.1	Y
Card Up	3.7.1	Y
CPU utilization exceeded upper threshold	3.7.1	N
Device Unsupported	3.7.1	N
Layer 2 Tunnel Down	3.7.1	N
Link up	3.7.1	N
Memory utilization exceeded upper threshold	3.7.1	N
Module Unsupported	3.7.1	N
MPLS Black Hole found	3.7.1	N

Supported Technologies on Cisco Access Servers

The following sections list the objects and attributes that are supported on Cisco access servers in Cisco Prime Network 3.9 per technology:

- IP, page 4-4
- Routing Protocols, page 4-7
- Ethernet, page 4-9
- TDM/DSx, page 4-14
- Security, page 4-17
- Hardware, page 4-18
- Serial, page 4-20

IP

Table 4-5 IP Attribute Support on Cisco Access Servers—Cisco Prime Network 3.9

Attribute	AS 5800
IMO Name—IIPInterface	
IP Address	Y
Subnetwork Mask	Y
IP Interface Addresses Array	Y
Interface Name	Y
Interface Description	Y
IP Interface State	Y
OSPF Interface Cost	
Broadcast Address	
MTU	
Lookup Method	
Address Resolution Type	
ARP Timeout	
Secured ARP	
ICMP Mask Reply	
IGMP Proxy	
HSRP Groups	
IP Multiplexing Table	
IANA Type	
Containing CTPs	
Contained CTPs	
IMO Name—IIPMuxEntry	
Termination Point	
Destination IP Subnet	
IMO Name—IRoutingEntity	
Routing Table	Y
ARP Entity	Y
Routing Table Changes	
Name	
Logical Sons	Y
IMO Name—IRoutingEntry	
Destination IP Subnet	Y
Next Hop IP Address	Y

Table 4-5 IP Attribute Support on Cisco Access Servers—Cisco Prime Network 3.9 (continued)

Attribute	AS 5800
Type	Y
Routing Protocol Type	Y
Outgoing Interface Name	Y
IMO Name—IARPEntity	
ARP Table	Y
IMO Name—IARPEntry	
IP Address	Y
MAC Address	Y
Port	Y
Entry Type	Y
IMO Name—IIPPool	
IP Address Pool Entries	
Name	
Index	
IMO Name—IIPRangeBasedIPPoolEntry	
Start IP Address	
End IP Address	
Unused Addresses	
Used Addresses	
Reserved Addresses	
IMO Name—IIPSubnetBasedIPPoolEntry	
IP Subnet	
Unused Addresses	
Used Addresses	
Reserved Addresses	
IMO Name—HSRPGroupEntry	
Group Number	
Port Description	
Priority	
Coupled Router	
State	
Tracking Interfaces	
Virtual IP Address	
Virtual MAC Address	

Table 4-5 IP Attribute Support on Cisco Access Servers—Cisco Prime Network 3.9 (continued)

Attribute	AS 5800
IMO Name—ITunnelGRE	
Name	
Tunnel Destination and Source	
IP Address	
IP Interface State	
IANA Type	
Containing CTPs	
Contained CTPs	
Keep Alive Time	
Keep Alive Retry	
IMO Name—IVrrpGroupEntry	
Group Number	
State	
Port Description	
Master IP Address	
Primary IP Address	
Priority	
Virtual Mac Address	
Preempt Mode	
Admin State	
Advertisement Interval	
Tracking Interfaces	
IMO Name—IIPSLAResponderService	
responderStatus	
TWAMPResponderStatus	
tcpConnect	
udpEcho	
IMO Name—IIPAddressPortPair	
type	
ipAddress	
port	

Routing Protocols

Table 4-6 Routing Protocols Attribute Support on Cisco Access Servers—Cisco Prime Network 3.9

Attribute	AS 5800
IMO Name—IBgpNeighborEntry	
Remote Identifier	
Neighbor Type	
Distributing Interfaces	
Remote Address	
Remote Autonomous System	
Peer State	
Peer AdminState	
Hold Time	
Keep Alive Time	
VrfName	
Address family	
IMO Name—IOspfEntry	
Area Identifier	Y
IP Address	Y
Type	Y
Administrative Status	Y
Ospf Entry State	Y
IMO Name—IOspfProcess	
Process Id	
OSPF Version	
Router Id	
IMO Name—IOspfNeighbor	
Neighbor Id	
Outgoing Interface	
State	
Neighbor Interface Address	
Area Id	
IMO Name—IOspfInterface	
Area Id	
Network Type	
Cost	

Table 4-6 Routing Protocols Attribute Support on Cisco Access Servers—Cisco Prime Network 3.9 (continued)

Attribute	AS 5800
State	
Interface Address	
Type	
IF Proirity	
DR Id	
BDR Id	
IMO Name—ISpfTimers	
Schedule Delay	
Min Hold Time	
Max Wait Time	
IMO Name—IISISProcess	
ISIS Version	
Manual Area Address	
IS Type	
System Id	
Process Id	
IMO Name—IISISMetric	
IS Type	
Metric Style	
Metric Value	
Address Family	
IMO Name—IISISInterface	
Interface Name	
IMO Name—IISISNeighbor	
IS Type	
System Id	
Admin State	
Hold Time	
SNPA	
Interface Name	
IP Address	
Adress Family	

Ethernet

Table 4-7 Ethernet Attribute Support on Cisco Access Servers—Cisco Prime Network 3.9

Attribute	AS5800
IMO Name—ILinkAggregationGroup802dot3ad	
dot3adAggMACAddress	
dot3adAggActorSystemPriority	
dot3adAggActorSystemID	
dot3adAggActorAdminKey	
dot3adAggActorOperKey	
dot3adAggPartnerSystemID	
dot3adAggPartnerSystemPriority	
dot3adAggPartnerOperKey	
dot3adAggCollectorMaxDelay	
GroupNumber	
AggregationProtocolType	
MacAddress	
ChannelAdminStatus	
ChannelOperStatus	
IMO Name—IEthernet	
MAC Address	Y
Duplex Mode	
Output Flow Control	Y
Input Flow Control	Y
IANA Type	
Containing CTPs	
Contained CTPs	
Port Type	
isElmiEnabled	
isLOAMEnabled	
IMO Name—IVlanInterface	
Mode	
Native VLAN Identification	
Virtual LAN Table	
IANA Type	
Containing CTPs	
Contained CTPs	

Table 4-7 Ethernet Attribute Support on Cisco Access Servers—Cisco Prime Network 3.9

Attribute	AS5800
vlanAdminType	
vlanencapType	
getAccess	
Allowed Vlans	
IMO Name—IVlanEncapMux	
IANA Type	
Containing CTPs	
Contained CTPs	
IMO Name—IVlanMapping	
direction	
vlanMatchCriteria	
vlanRewriteDefinition	
Drop	
Vlan	
innerVlan	
translatedVlan	
translatedInnerVlan	
IMO Name—IIEEE802	
VLAN Identification	
Binding Information	
Binding Status	
IANA Type	
Containing CTPs	
Contained CTPs	
IMO Name—IStpService	
StpProtocol	
StpMaxAge	
StpHelloTime	
StpBridgeForwardDelay	
StpInstanceInfoTable	
Same as ISystemService	
StpUplinkFastState	
StpBackboneFastState	
StpForwardDelay	
StpBridgeMaxAge	
StpBridgeHelloTime	

Table 4-7 Ethernet Attribute Support on Cisco Access Servers—Cisco Prime Network 3.9

Attribute	AS5800
IMO Name—IMstService	
MstProperties	
Same as IStpService	
IMO Name—IPvstpService	
UpLinkFast	
BackboneFast	
IMO Name—IMstProperties	
MstForceVersion	
MstCfgIdFmtSel	
MstExternalRootCost	
MstMaxInstances	
MstCfgIdName	
MstCfgIdRevLevel	
IMO Name—IStpInstanceInfo	
Object Identification	
StpBridgeId	
BridgePriority	
Designated Parent and Root Bridges	
StpRootCost	
IsRoot	
StpRootPort	
StpPortInfoTable	
STP Instance Id	
Vlan Id	
StpDesignatedBridge	
StpDesignatedRoot	
IMO Name—IMstInstanceInfo	
MstVlanIds	
Same as IStpInstanceInfo	
IMO Name—IPvstpInstanceInfo	
Protocol Type	
StpBridgeMaxAge	
StpBridgeHelloTime	
StpBridgeForwardDelay	
StpProtocolSpecification	
StpVlanId	

Table 4-7 Ethernet Attribute Support on Cisco Access Servers—Cisco Prime Network 3.9

Attribute	AS5800
StpForwardDelay	
StpMaxAge	
IMO Name—IRstpInstanceInfo	
StpForceVersion	
Same as IStpInstanceInfo	
IMO Name—IStpPortInfo	
StpPort	
StpPortPriority	
StpPortState	
StpPortPathCost	
StpPortEdgePort	
StpPortPointToPoint	
StpPortRole	
StpDesignatedPortIdentifier	
StpDesignatedBridge	
StpPortIdentifier	
StpPortBpduGuardState	
StpPortBpduFilterState	
IMO Name—IMstPortInfo	
MstPortHelloTime	
Same as IStpPortInfo	
IMO Name—IPvstpPortInfo	
PvstpPortFastState	
IMO Name—IEthernetChannel	
Group Number	
Bandwidth	
Aggregation Protocol	
IANA Type	
Containing CTPs	
Contained CTPs	
Mac Address	
Admin Status	
Oper Status	
IMO Name—ITokenRingLayer2	
MAC Address	
IANA Type	

Table 4-7 Ethernet Attribute Support on Cisco Access Servers—Cisco Prime Network 3.9

Attribute	AS5800
Containing CTPs	
Contained CTPs	
IMO Name—ITokenRingLayer1	
Same as IPhysicalLayer	
IMO Name—IVtpService	
Version	
OperatingMode	
DomainName	
ConfigurationRevision	
isPruningEnabled	
isAuthenticationEnabled	
IMO Name—IREPService	
version	
administrativeVlan	
notificationEnabled	
IMO Name—IREPSegmentInfo	
segmentId	
segmentComplete	
IMO Name—IREPPortInfo	
portName	
portKey	
segmentId	
portType	
portRole	
operStatus	
blockedVlans	
preemptTimer	
lslAgeoutTimer	
remoteDeviceName	
remoteDeviceMac	
remotePortName	
configuredLoadBalancingBlockedVlans	
IMO Name—IBridgeILan	
Id	
IMO Name—IIBBridgeEntry	
IS Id	

Table 4-7 Ethernet Attribute Support on Cisco Access Servers—Cisco Prime Network 3.9

Attribute	AS5800
IBridge	
BBridge	

TDM/DSx

Table 4-8 TDM/DSx Attribute Support on Cisco Access Servers—Cisco Prime Network 3.9

Attribute	AS5800
IMO Name—IDS0Bundle	
Bundled Time Slots	
Bundle Location	
IANA Type	
Containing CTPs	
Contained CTPs	
AdminStatus	
OperStatus	
IMO Name—IDS1Pdh / IDS3Pdh	
Framing Type	
Cell Mapping Type	
Loopback Type	
Scrambling Mode	
Same as IPhysicalLayer	
portDescription	Y
internationalBit	
nationalBits	
framing	
lineCode	
cableLength	
recoveredClockingId	
clocking	
loopback	
alarmState	Y
IMO Name—IClockService	
ActiveClockSource	
NcsMode	
HoldTimeout	

Table 4-8 TDM/DSx Attribute Support on Cisco Access Servers—Cisco Prime Network 3.9

Attribute	AS5800
UseStratum4	
Mode	
NcsPriorityList	
PtpService	
ClockSourceTable	
PseudowireClockRecovery	
SynchronousEthernet	
IMO Name—IClockSource	
Priority	
Source	
Status	
Type	
IMO Name—IPtpService	
Mode	
ClockId	
Domain	
Priority1	
Priority2	
PtpEnabled	
PtpInterfaceList	
ptpState	
IMO Name—IPtpInterface	
Version	
AnnounceInterval	
AnnounceTimeout	
DestinationAddress	
SourceAddress	
DelayReq	
MasterMode	
SlaveMode	
SyncInterval	
SyncLimit	
InterfaceXid	
Role	
Transport	
State	

Table 4-8 TDM/DSx Attribute Support on Cisco Access Servers—Cisco Prime Network 3.9

Attribute	AS5800
IMO Name—IACRService	
RecoveredClockSource	
RecoveredClockMode	
CemInterface	
RecoveredClockList	
IMO Name—IRecoveredClock	
ClockId	
RecoveredClockMode	
Port	
Cem	
Status	
FrequencyOffset	
CEMGroupId	
CEMInterfaceName	
TransferType	
IMO Name—ICEMEncap	
cemIfName	
IMO Name—ICEMGroup	
IdlePattern	
IdleCAS	
DeJitter	
PayloadSize	
RTP	
RTPHeader	
TimeSlots	
AdminStatus	
OperStatus	
IMO Name—ISyncE	
synchronousMode	
equipmentClock	
clockMode	
ssmOption	
esmcMode	
holdOffTimer	
waitToRestore	
Revertive	

Table 4-8 TDM/DSx Attribute Support on Cisco Access Servers—Cisco Prime Network 3.9

Attribute	AS5800
IMO Name—ISyncEInterface	
InterfaceName	
selectionInput	
ingressESMCMode	
egressESMCMode	
ingressQLMode	
ingressQuality	
egressQLMode	
egressQuality	
waitToRestore	
holdOffTimer	
ingressConfQuality	
egressConfQuality	
Priority	
ingressSSM	
egressSSM	
clockModeStr	

Security

Table 4-9 Security Attribute Support on Cisco Access Servers—Cisco Prime Network 3.9

Attribute	AS5800
IMO Name—IAccessList	
Type	Y
Access List Entries	Y
Name or Id	Y
Index	Y
IMO Name—IAccessListEntry	
Entry Identification	
Action Logic	
Source and Destination Address	
Source and Destination Wildcard	
Protocol Type	
Source and Destination Port Ranges	

Table 4-9 Security Attribute Support on Cisco Access Servers—Cisco Prime Network 3.9

Attribute	AS5800
Source and Destination Port Action	
Protocol Specific Info	
Differential Services Code Points	
Type of Service	
Precedence	
Matches	

Hardware

Table 4-10 Hardware Attribute Support on Cisco Access Servers—Cisco Prime Network 3.9

Attribute	AS5800
IMO Name—IChassis	
Description	
Equipment Holder Type	
Contained Equipment Holders	
Contained Equipments	
Serial Number	Y
IMO Name—IShelf	
Description	
Status	
Equipment Holder Type	
Contained Equipment Holders	
Contained Equipments	
Serial Number	
IMO Name—IModule	
Module Name	Y
Module Description	Y
Software Version	
Operational Status	Y
Hardware Type + Version	Y
Managed IP Address	
Redundant Equipment	
Configured Redundancy	
Redundancy Status	

Table 4-10 Hardware Attribute Support on Cisco Access Servers—Cisco Prime Network 3.9

Attribute	AS5800
Operational Status Last Changed	
Supported Physical Termination Points	
Serial Number (soft property)	
Slots Number	
IMO Name—IPowerSupply	
Same as IModule	
IMO Name—IFanTray	
Same as IModule	
IMO Name—IPluggableTransceiver	
ConnectorDescription	
PID	
ConnectorSerialNumber	
ConnectorType	
PluggablePortState	
PluggableType	
IMO Name—IManagedElement	
IP Address	Y
Communication State	Y
Investigation State	Y
Element Category	Y
Element Type and Key	Y
Device Name	Y
System Name	Y
System Description	Y
Up Time	Y
Software Version	Y
Vendor Identity	Y
Memory and CPU Usage	Y
DRAM Free	
DRAM Used	
Flash Device Size	Y
NVRAM Size	Y
Processor DRAM	
Sys Contact	Y
Sys Location	Y
Serial Number	Y

Table 4-10 Hardware Attribute Support on Cisco Access Servers—Cisco Prime Network 3.9

Attribute	AS5800
File Systems	
IMO Name—IContext	
Name	
Bounded Connections	
IP Address Pools	
Forwarding Components List	
Traffic Descriptors List	
Tunnel Containers List	
Data Link Aggregation Containers List	
IMO Name—ISystemService	
Type	
Status	
Up Time	
IMO Name—IBridge	
Bridge Table	
Type	
MAC Address	
IP Interface	
Name	
Logical Sons	
Vlan Type	
IMO Name—IBridgeEntry	
Destination MAC	
Outgoing Interface	

Serial

Table 4-11 Serial Attribute Support on Cisco Access Servers—Cisco Prime Network 3.9

Attribute	AS5800
IMO Name—IPhysicalLayer	
Media Type	
Clocking Source	
Maximum Speed	Y
Is Internal Port	
Discarded Bandwidth	

Table 4-11 Serial Attribute Support on Cisco Access Servers—Cisco Prime Network 3.9

Attribute	AS5800
Dropped Bandwidth	
Input Bandwidth	
Output Bandwidth	
Discarded and Received Input Data Counters	Y
Dropped and Forward Output Data Counters	Y
Administrative Status	Y
Operational Status	Y
Last Changed	Y
IANA Type	
Containing CTPs	
Contained CTPs	
Port Alias	Y
Location	Y
Sending Alarms	Y
Connector Description	
Part ID	
Connector Serial Num	
Product	Y
Status	Y
Managed	Y



CHAPTER 5

Support Information for Cisco Gateways

This chapter contains support information for Virtual Network Elements (VNEs) that manage Cisco gateways in Cisco Prime Network 3.9.

- Cisco AS5300 Series Universal Gateways, page 5-1
- Supported Technologies on Cisco Gateways, page 5-3

Note For more information about the technologies described in this chapter , see Part 2 Technology Support.

Cisco AS5300 Series Universal Gateways

This section includes the following information about Cisco AS5300 Series gateways (for information on the NE types supported in Cisco Prime Network 3.9, see Cisco AS5300 Series Universal Gateways):

- Cisco AS5300 Series—Supported Software Versions, page 5-1
- Cisco AS5300 Series—Supported Topologies, page 5-2
- Cisco AS5300 Series—Supported Modules, page 5-2
- Cisco AS5300 Series—Supported Technologies, page 5-2
- Cisco AS5300 Series—Supported Service Events, page 5-3

Cisco AS5300 Series—Supported Software Versions

Table 5-1 Supported Software Versions for Cisco AS5300 Series—Cisco Prime Network 3.9

Software Version	Product_Version
12.0(3)T1	3.6.0
12.1(10a)	3.6.0
12.1(11b)	3.6.0
12.1(22b)	3.6.0
12.19(22b)	3.6.0
12.3(10c)	3.6.0

Table 5-1 Supported Software Versions for Cisco AS5300 Series—Cisco Prime Network 3.9

Software Version	Product_Version
12.3(3)	3.6.0

Cisco AS5300 Series—Supported Topologies

Table 5-2 Supported Topologies for Cisco AS5300 Series—Cisco Prime Network 3.9

Topology Type	Link Type	Product_Version
Ethernet	Ethernet	3.6.0
Physical Layer	Physical Layer	3.6.0

Cisco AS5300 Series—Supported Modules

Table 5-3 Supported Modules for Cisco AS5300 Series—Cisco Prime Network 3.9

Module Name	Product_Version	Module Description
AS5300-8CE1-4T	3.6.0	Octal Port Channelized E1/PRI and 4T Card
AS5300-AMAZON2-CARRIER	3.6.0	Access Server MICA Modem Carrier Card
PM-DTD-12M	3.6.0	MICA 12-Modem Module Card
CPU-AS5300	3.6.0	AS5300
AS5300-4CE1	3.6.0	Quad Port Channelized E1/PRI Card
AS5300-DTD-CARRIER	3.6.0	Access Server MICA Modem Carrier Card
PM-DTD-6M	3.6.0	MICA 6-Modem Module Card

Cisco AS5300 Series—Supported Technologies

The following technologies are supported by the Cisco AS5300 Series in Cisco Prime Network 3.9:

- IP, page 5-4
- Ethernet, page 5-7
- Security, page 5-12
- Hardware, page 5-12
- Serial, page 5-15
- CDP, page 5-16
- Discovery Protocol, page 5-16

Cisco AS5300 Series—Supported Service Events

Table 5-4 Supported Service Events for Cisco AS5300 Series—Cisco Prime Network 3.9

Event Name	Product_Version	Expedited
Active IP Interfaces Found	3.6.0	Y
All IP Interfaces Down	3.6.0	Y
BGP process up	3.6.0	N
Card Down	3.6.0	Y
Card In	3.6.0	Y
Card Out	3.6.0	Y
Card Up	3.6.0	Y
CPU utilization exceeded upper threshold	3.6.0	N
Device Unsupported	3.6.0	N
Keepalive configured	3.6.0	N
Keepalive not configured	3.6.0	N
Layer 2 Tunnel Down	3.6.0	N
Link up	3.6.0	N
Memory utilization exceeded upper threshold	3.6.0	N
Module Unsupported	3.6.0	N
Rx utilization exceeded upper threshold	3.6.0	N
Tx utilization exceeded upper threshold	3.6.0	N

Supported Technologies on Cisco Gateways

The following sections list the objects and attributes that are supported on Cisco gateways in Cisco Prime Network 3.9 per technology:

- IP, page 5-4
- Ethernet, page 5-7
- Security, page 5-12
- Hardware, page 5-12
- Serial, page 5-15
- CDP, page 5-16
- Discovery Protocol, page 5-16

IP

Table 5-5 IP Attribute Support on Cisco Gateways—Cisco Prime Network 3.9

Attribute	AS5300
IMO Name—IIPInterface	
IP Address	Y
Subnetwork Mask	Y
IP Interface Addresses Array	Y
Interface Name	Y
Interface Description	Y
IP Interface State	Y
OSPF Interface Cost	
Broadcast Address	
MTU	
Lookup Method	
Address Resolution Type	
ARP Timeout	
Secured ARP	
ICMP Mask Reply	
IGMP Proxy	
HSRP Groups	
IP Multiplexing Table	
IANA Type	
Containing CTPs	
Contained CTPs	
IMO Name—IIPMuxEntry	
Termination Point	
Destination IP Subnet	
IMO Name—IRoutingEntity	
Routing Table	Y
ARP Entity	Y
Routing Table Changes	
Name	
Logical Sons	
IMO Name—IRoutingEntry	
Destination IP Subnet	Y
Next Hop IP Address	Y

Table 5-5 IP Attribute Support on Cisco Gateways—Cisco Prime Network 3.9 (continued)

Attribute	AS5300
Type	Y
Routing Protocol Type	Y
Outgoing Interface Name	Y
IMO Name—IARPEntity	
ARP Table	Y
IMO Name—IARPEntry	
IP Address	Y
MAC Address	Y
Port	Y
Entry Type	Y
IMO Name—IIPPool	
IP Address Pool Entries	
Name	
Index	
IMO Name—IIPRangeBasedIPPoolEntry	
Start IP Address	
End IP Address	
Unused Addresses	
Used Addresses	
Reserved Addresses	
IMO Name—IIPSubnetBasedIPPoolEntry	
IP Subnet	
Unused Addresses	
Used Addresses	
Reserved Addresses	
IMO Name—HSRPGroupEntry	
Group Number	
Port Description	
Priority	
Coupled Router	
State	
Tracking Interfaces	
Virtual IP Address	
Virtual MAC Address	

Table 5-5 IP Attribute Support on Cisco Gateways—Cisco Prime Network 3.9 (continued)

Attribute	AS5300
IMO Name—ITunnelGRE	
Name	
Tunnel Destination and Source	
IP Address	
IP Interface State	
IANA Type	
Containing CTPs	
Contained CTPs	
Keep Alive Time	
Keep Alive Retry	
IMO Name—IVrrpGroupEntry	
Group Number	
State	
Port Description	
Master IP Address	
Primary IP Address	
Priority	
Virtual Mac Address	
Preempt Mode	
Admin State	
Advertisement Interval	
Tracking Interfaces	
IMO Name—IIPSLAResponderService	
responderStatus	
TWAMPResponderStatus	
tcpConnect	
udpEcho	
IMO Name—IIPAddressPortPair	
type	
ipAddress	
port	

Ethernet

Table 5-6 Ethernet Attribute Support on Cisco Gateways—Cisco Prime Network 3.9

Attribute	AS5300
IMO Name—ILinkAggregationGroup802dot3ad	
dot3adAggMACAddress	
dot3adAggActorSystemPriority	
dot3adAggActorSystemID	
dot3adAggActorAdminKey	
dot3adAggActorOperKey	
dot3adAggPartnerSystemID	
dot3adAggPartnerSystemPriority	
dot3adAggPartnerOperKey	
dot3adAggCollectorMaxDelay	
GroupNumber	
AggregationProtocolType	
MacAddress	
ChannelAdminStatus	
ChannelOperStatus	
IMO Name—IEthernet	
MAC Address	Y
Duplex Mode	
Output Flow Control	
Input Flow Control	
IANA Type	
Containing CTPs	
Contained CTPs	
Port Type	
isElmiEnabled	
isLOAMEnabled	
IMO Name—IVlanInterface	
Mode	
Native VLAN Identification	
Virtual LAN Table	
IANA Type	
Containing CTPs	
Contained CTPs	

Table 5-6 Ethernet Attribute Support on Cisco Gateways—Cisco Prime Network 3.9 (continued)

Attribute	AS5300
vlanAdminType	
vlanencapType	
getAccess	
Allowed Vlans	
IMO Name—IVlanEncapMux	
IANA Type	
Containing CTPs	
Contained CTPs	
IMO Name—IVlanMapping	
direction	
vlanMatchCriteria	
vlanRewriteDefinition	
Drop	
Vlan	
innerVlan	
translatedVlan	
translatedInnerVlan	
IMO Name—IIEEE802	
VLAN Identification	
Binding Information	
Binding Status	
IANA Type	
Containing CTPs	
Contained CTPs	
IMO Name—IStpService	
StpProtocol	
StpMaxAge	
StpHelloTime	
StpBridgeForwardDelay	
StpInstanceInfoTable	
Same as ISystemService	
StpUplinkFastState	
StpBackboneFastState	
StpForwardDelay	
StpBridgeMaxAge	
StpBridgeHelloTime	

Table 5-6 Ethernet Attribute Support on Cisco Gateways—Cisco Prime Network 3.9 (continued)

Attribute	AS5300
IMO Name—IMstService	
MstProperties	
Same as IStpService	
IMO Name—IPvstpService	
UpLinkFast	
BackboneFast	
IMO Name—IMstProperties	
MstForceVersion	
MstCfgIdFmtSel	
MstExternalRootCost	
MstMaxInstances	
MstCfgIdName	
MstCfgIdRevLevel	
IMO Name—IStpInstanceInfo	
Object Identification	
StpBridgeId	
BridgePriority	
Designated Parent and Root Bridges	
StpRootCost	
IsRoot	
StpRootPort	
StpPortInfoTable	
STP Instance Id	
Vlan Id	
StpDesignatedBridge	
StpDesignatedRoot	
IMO Name—IMstInstanceInfo	
MstVlanIds	
Same as IStpInstanceInfo	
IMO Name—IPvstpInstanceInfo	
Protocol Type	
StpBridgeMaxAge	
StpBridgeHelloTime	
StpBridgeForwardDelay	
StpProtocolSpecification	
StpVlanId	

Table 5-6 Ethernet Attribute Support on Cisco Gateways—Cisco Prime Network 3.9 (continued)

Attribute	AS5300
StpForwardDelay	
StpMaxAge	
IMO Name—IRstpInstanceInfo	
StpForceVersion	
Same as IStpInstanceInfo	
IMO Name—IStpPortInfo	
StpPort	
StpPortPriority	
StpPortState	
StpPortPathCost	
StpPortEdgePort	
StpPortPointToPoint	
StpPortRole	
StpDesignatedPortIdentifier	
StpDesignatedBridge	
StpPortIdentifier	
StpPortBpduGuardState	
StpPortBpduFilterState	
IMO Name—IMstPortInfo	
MstPortHelloTime	
Same as IStpPortInfo	
IMO Name—IPvstpPortInfo	
PvstpPortFastState	
IMO Name—IEthernetChannel	
Group Number	
Bandwidth	
Aggregation Protocol	
IANA Type	
Containing CTPs	
Contained CTPs	
Mac Address	
Admin Status	
Oper Status	
IMO Name—ITokenRingLayer2	
MAC Address	
IANA Type	

Table 5-6 Ethernet Attribute Support on Cisco Gateways—Cisco Prime Network 3.9 (continued)

Attribute	AS5300
Containing CTPs	
Contained CTPs	
IMO Name—ITokenRingLayer1	
Same as IPhysicalLayer	
IMO Name—IVtpService	
Version	
OperatingMode	
DomainName	
ConfigurationRevision	
isPruningEnabled	
isAuthenticationEnabled	
IMO Name—IREPService	
version	
administrativeVlan	
notificationEnabled	
IMO Name—IREPSegmentInfo	
segmentId	
segmentComplete	
IMO Name—IREPPortInfo	
portName	
portKey	
segmentId	
portType	
portRole	
operStatus	
blockedVlans	
preemptTimer	
lslAgeoutTimer	
remoteDeviceName	
remoteDeviceMac	
remotePortName	
configuredLoadBalancingBlockedVlans	
IMO Name—IBridgeILan	
Id	
IMO Name—IIBBridgeEntry	
IS Id	

Table 5-6 Ethernet Attribute Support on Cisco Gateways—Cisco Prime Network 3.9 (continued)

Attribute	AS5300
IBridge	
BBridge	

Security

Table 5-7 Security Attribute Support on Cisco Gateways—Cisco Prime Network 3.9

Attribute	AS5300
IMO Name—IAccessList	
Type	
Access List Entries	
Name or Id	
Index	
IMO Name—IAccessListEntry	
Entry Identification	Y
Action Logic	Y
Source and Destination Address	Y
Source and Destination Wildcard	Y
Protocol Type	Y
Source and Destination Port Ranges	Y
Source and Destination Port Action	Y
Protocol Specific Info	Y
Differential Services Code Points	Y
Type of Service	Y
Precedence	Y
Matches	Y

Hardware

Table 5-8 Hardware Attribute Support on Cisco Gateways—Cisco Prime Network 3.9

Attribute	AS5300
IMO Name—IChassis	
Description	
Equipment Holder Type	

Table 5-8 Hardware Attribute Support on Cisco Gateways—Cisco Prime Network 3.9 (continued)

Attribute	AS5300
Contained Equipment Holders	
Contained Equipments	
Serial Number	Y
IMO Name—IShelf	
Description	
Status	
Equipment Holder Type	
Contained Equipment Holders	
Contained Equipments	
Serial Number	
IMO Name—IModule	
Module Name	Y
Module Description	Y
Software Version	Y
Operational Status	Y
Hardware Type + Version	Y
Managed IP Address	
Redundant Equipment	
Configured Redundancy	
Redundancy Status	
Operational Status Last Changed	
Supported Physical Termination Points	
Serial Number (soft property)	Y
Slots Number	
IMO Name—IPowerSupply	
Same as IModule	
IMO Name—IFanTray	
Same as IModule	
IMO Name—IPluggableTransceiver	
ConnectorDescription	
PID	
ConnectorSerialNumber	
ConnectorType	
PluggablePortState	
PluggableType	

Table 5-8 Hardware Attribute Support on Cisco Gateways—Cisco Prime Network 3.9 (continued)

Attribute	AS5300
IMO Name—IManagedElement	
IP Address	Y
Communication State	Y
Investigation State	Y
Element Category	Y
Element Type and Key	Y
Device Name	Y
System Name	Y
System Description	Y
Up Time	Y
Software Version	Y
Vendor Identity	Y
Memory and CPU Usage	Y
DRAM Free	
DRAM Used	
Flash Device Size	Y
NVRAM Size	Y
Processor DRAM	
Sys Contact	Y
Sys Location	Y
Serial Number	Y
File Systems	
IMO Name—IContext	
Name	
Bounded Connections	
IP Address Pools	
Forwarding Components List	
Traffic Descriptors List	
Tunnel Containers List	
Data Link Aggregation Containers List	
IMO Name—ISystemService	
Type	
Status	
Up Time	
IMO Name—IBridge	
Bridge Table	

Table 5-8 Hardware Attribute Support on Cisco Gateways—Cisco Prime Network 3.9 (continued)

Attribute	AS5300
Type	
MAC Address	
IP Interface	
Name	
Logical Sons	
Vlan Type	
IMO Name—IBridgeEntry	
Destination MAC	
Outgoing Interface	

Serial

Table 5-9 Serial Attribute Support on Cisco Gateways—Cisco Prime Network 3.9

Attribute	AS5300
IMO Name—IPhysicalLayer	
Media Type	Y
Clocking Source	
Maximum Speed	Y
Is Internal Port	Y
Discarded Bandwidth	
Dropped Bandwidth	
Input Bandwidth	
Output Bandwidth	
Discarded and Received Input Data Counters	Y
Dropped and Forward Output Data Counters	Y
Administrative Status	Y
Operational Status	Y
Last Changed	Y
IANA Type	Y
Containing CTPs	
Contained CTPs	
Port Alias	Y
Location	Y
Sending Alarms	Y

Table 5-9 Serial Attribute Support on Cisco Gateways—Cisco Prime Network 3.9 (continued)

Attribute	AS5300
Connector Description	Y
Part ID	Y
Connector Serial Num	Y
Product	Y
Status	Y
Managed	Y

CDP

Table 5-10 CDP Attribute Support on Cisco Gateways—Cisco Prime Network 3.9

Attribute	AS5300
IMO Name—ICdpService	
cdpHoldtime	Y
cdpMessageInterval	Y
cdpDeviceId	Y
cdpState	Y
cdpVersion	Y
IMO Name—ICdpNeighbor	
remoteDeviceId	Y
remotePortId	Y
remoteIPAddress	Y
localPortId	Y

Discovery Protocol

Table 5-11 Discovery Protocol Attribute Support on Cisco Gateways—Cisco Prime Network 3.9

Attribute	AS5300
IMO Name—IDiscoveryProtocol	
DiscoveryProtocolType	Y
Info	Y



CHAPTER 6

Support Information for Cisco Routers

This chapter contains support information for Virtual Network Elements (VNEs) that manage Cisco routers in Cisco Prime Network 3.9.

- Cisco 800 Series Routers, page 6-2
- Cisco 1000 Series Routers, page 6-3
- Cisco 1600 Series Routers, page 6-6
- Cisco 1700 Series Modular Access Routers, page 6-8
- Cisco 1800 Series Integrated Services Routers, page 6-12
- Cisco 2500 Series Routers, page 6-15
- Cisco 2600 Series Multiservice Platform Routers, page 6-18
- Cisco 2800 Series Integrated Services Routers, page 6-22
- Cisco 3600 Series Multiservice Platform Routers, page 6-27
- Cisco 3700 Series Multiservice Access Routers, page 6-29
- Cisco 3800 Series Integrated Services Routers, page 6-32
- Cisco 7200 Series Routers, page 6-36
- Cisco 7300 Series Routers, page 6-45
- Cisco 7400 Series Routers, page 6-49
- Cisco 7500 Series Routers, page 6-54
- Cisco 7600 Series Routers, page 6-57
- Cisco 10000 Series Routers, page 6-81
- Cisco 12000 Series Routers, page 6-85
- Cisco XR 12000 Series Routers, page 6-95
- Cisco CRS Carrier Routing System, page 6-106
- Cisco ASR 9000 Series Aggregation Services Routers, page 6-121
- Cisco ASR 1000 Series Routers, page 6-134
- Cisco MWR 2900 Series Mobile Wireless Routers, page 6-143
- Cisco 1900 Series Integrated Services Router, page 6-151
- Cisco 2900 Series Integrated Services Router, page 6-154
- Cisco 3900 Series Integrated Service Routers, page 6-158

- Cisco Universal Broadband Router 7200 Series, page 6-161
- Cisco Univeral Broadband Router 10000 Series, page 6-165
- Cisco 4700 Series Routers, page 6-168
- Cisco ASR901 Series Mobile Wireless Routers, page 6-170
- Cisco ASR903 Series Routers, page 6-185
- Cisco ASR 5000 Series Routers, page 6-196
- Supported Technologies on Cisco Routers, page 6-198

Note For more information about the technologies described in this chapter , see Part 2 Technology Support.

Cisco 800 Series Routers

This section includes the following information about Cisco 800 Series routers (for information on the NE types supported in Cisco Prime Network 3.9, see Cisco 800 Series Routers):

- Cisco 800 Series—Supported Software Versions, page 6-2
- Cisco 800 Series—Supported Topologies, page 6-2
- Cisco 800 Series—Supported Technologies, page 6-3
- Cisco 800 Series—Supported Service Events, page 6-3

Cisco 800 Series—Supported Software Versions

Table 6-1 Supported Software Versions for Cisco 800 Series—Cisco Prime Network 3.9

Software Version	Product_Version
12.0(4)XM	3.6.1
12.0(7)T3	3.6.1
12.3(14)T	3.6.2
12.4(11)T	3.6.2

Cisco 800 Series—Supported Topologies

Table 6-2 Supported Topologies for Cisco 800 Series—Cisco Prime Network 3.9

Topology Type	Link Type	Product_Version
ATM	ATM	3.6.0
Ethernet	Ethernet	3.6.0
GRE Tunnel	GRE Tunnel	3.6.0

Table 6-2 Supported Topologies for Cisco 800 Series—Cisco Prime Network 3.9 (continued)

Topology Type	Link Type	Product_Version
Physical Layer	Physical Layer	3.6.0

Cisco 800 Series—Supported Technologies

The following technologies are supported by the Cisco 800 Series in Cisco Prime Network 3.9:

- IP, page 6-199
- Routing Protocols, page 6-202
- Ethernet, page 6-205
- ATM, page 6-213
- TDM/DSx, page 6-222
- VPN (VRF), page 6-233
- Security, page 6-237
- Hardware, page 6-238
- Serial, page 6-242
- Additional Technologies, page 6-243
- LocalSwitching, page 6-245
- CDP, page 6-249
- Discovery Protocol, page 6-249

Cisco 800 Series—Supported Service Events

Table 6-3 Supported Service Events for Cisco 800 Series—Cisco Prime Network 3.9

Event Name	Product_Version	Expedited
Active IP Interfaces Found	3.6.1	Y
All IP Interfaces Down	3.6.1	Y
Device Unsupported	3.6.1	N
Link up	3.6.1	N
Module Unsupported	3.6.1	N

Cisco 1000 Series Routers

This section includes the following information about Cisco 1000 Series routers (for information on the NE types supported in Cisco Prime Network 3.9, see Cisco 1000 Series Routers):

- Cisco 1000 Series—Supported Software Versions, page 6-4

- Cisco 1000 Series—Supported Topologies, page 6-4
- Cisco 1000 Series—Supported Technologies, page 6-4
- Cisco 1000 Series—Supported Service Events, page 6-5

Cisco 1000 Series—Supported Software Versions

Table 6-4 Supported Software Versions for Cisco 1000 Series—Cisco Prime Network 3.9

Software Version	Product_Version
IOS 12.1(27)	3.6.1
IOS 12.1(22)	3.6.1

Cisco 1000 Series—Supported Topologies

Table 6-5 Supported Topologies for Cisco 1000 Series—Cisco Prime Network 3.9

Topology Type	Link Type	Product_Version
Ethernet	Ethernet	3.6.1
Framerelay	Framerelay	3.6.1
PPP/HDLC	PPP or HDLC	3.6.1
GRE Tunnel	GRE Tunnel	3.6.1
Physical Layer	Physical Layer	3.6.1

Cisco 1000 Series—Supported Technologies

The following technologies are supported by the Cisco 1000 Series in Cisco Prime Network 3.9:

- IP, page 6-199
- Routing Protocols, page 6-202
- Ethernet, page 6-205
- ATM, page 6-213
- Frame Relay, page 6-217
- PPP, page 6-219
- HDLC, page 6-220
- SONET/SDH, page 6-220
- TDM/DSx, page 6-222
- Security, page 6-237
- Hardware, page 6-238
- Serial, page 6-242

- Additional Technologies, page 6-243
- LocalSwitching, page 6-245
- CDP, page 6-249
- Discovery Protocol, page 6-249

Cisco 1000 Series—Supported Service Events

Table 6-6 Supported Service Events for Cisco 1000 Series—Cisco Prime Network 3.9

Event Name	Product_Version	Expedited
Active IP Interfaces Found	3.6.1	Y
All IP Interfaces Down	3.6.1	Y
BGP process up	3.6.1	N
Card Down	3.6.1	Y
Card In	3.6.1	Y
Card Out	3.6.1	Y
Card Up	3.6.1	Y
CPU utilization exceeded upper threshold	3.6.1	N
Device Unsupported	3.6.1	N
Fan-tray down	Prime Network 3.8	N
Fan-tray out	Prime Network 3.8	N
Keepalive configured	3.6.1	N
Keepalive not configured	3.6.1	N
Layer 2 Tunnel Down	3.6.1	N
Link up	3.6.0	N
Memory utilization exceeded upper threshold	3.6.1	N
Module Unsupported	3.6.1	N
MPLS Black Hole found	3.6.1	N
Pluggable transceiver out	Prime Network 3.8	N
Power-supply down	Prime Network 3.8	N

Table 6-6 Supported Service Events for Cisco 1000 Series—Cisco Prime Network 3.9

Event Name	Product_Version	Expedited
Power-supply out	Prime Network 3.8	N
Rx utilization exceeded upper threshold	3.6.1	N
Tx utilization exceeded upper threshold	3.6.1	N

Cisco 1600 Series Routers

This section includes the following information about Cisco 1600 Series routers (for information on the NE types supported in Cisco Prime Network 3.9, see Cisco 1600 Series Routers):

- Cisco 1600 Series—Supported Software Versions, page 6-6
- Cisco 1600 Series—Supported Topologies, page 6-6
- Cisco 1600 Series—Supported Technologies, page 6-7
- Cisco 1600 Series—Supported Service Events, page 6-7

Cisco 1600 Series—Supported Software Versions

Table 6-7 Supported Software Versions for Cisco 1600 Series—Cisco Prime Network 3.9

Software Version	Product_Version
12.0(12)	3.6.1

Cisco 1600 Series—Supported Topologies

Table 6-8 Supported Topologies for Cisco 1600 Series—Cisco Prime Network 3.9

Topology Type	Link Type	Product_Version
Ethernet	Ethernet	3.6.1
Framerelay	Framerelay	3.6.1
PPP/HDLC	PPP or HDLC	3.6.1
GRE Tunnel	GRE Tunnel	3.6.1
Physical Layer	Physical Layer	3.6.1

Cisco 1600 Series—Supported Technologies

The following technologies are supported by the Cisco 1600 Series in Cisco Prime Network 3.9:

- IP, page 6-199
- Routing Protocols, page 6-202
- Ethernet, page 6-205
- ATM, page 6-213
- Frame Relay, page 6-217
- PPP, page 6-219
- HDLC, page 6-220
- SONET/SDH, page 6-220
- TDM/DSx, page 6-222
- Security, page 6-237
- Hardware, page 6-238
- Serial, page 6-242
- LocalSwitching, page 6-245
- CDP, page 6-249
- Discovery Protocol, page 6-249

Cisco 1600 Series—Supported Service Events

Table 6-9 Supported Service Events for Cisco 1600 Series—Cisco Prime Network 3.9

Event Name	Product_Version	Expedited
Active IP Interfaces Found	3.6.1	Y
All IP Interfaces Down	3.6.1	Y
BGP process up	3.6.1	N
Card Down	3.6.1	Y
Card In	3.6.1	Y
Card Out	3.6.1	Y
Card Up	3.6.1	Y
CPU utilization exceeded upper threshold	3.6.1	N
Device Unsupported	3.6.1	N
Fan-tray down	Prime Network 3.8	N

Table 6-9 Supported Service Events for Cisco 1600 Series—Cisco Prime Network 3.9

Event Name	Product_Version	Expedited
Fan-tray out	Prime Network 3.8	N
Keepalive configured	3.6.1	N
Keepalive not configured	3.6.1	N
Layer 2 Tunnel Down	3.6.1	N
Link up	3.6.0	N
Memory utilization exceeded upper threshold	3.6.1	N
Module Unsupported	3.6.1	N
MPLS Black Hole found	3.6.1	N
Pluggable transceiver out	Prime Network 3.8	N
Power-supply down	Prime Network 3.8	N
Power-supply out	Prime Network 3.8	N
Rx utilization exceeded upper threshold	3.6.1	N
Tx utilization exceeded upper threshold	3.6.1	N
BFD neighbor found	3.7.1	N

Cisco 1700 Series Modular Access Routers

This section includes the following information about Cisco 1700 Series routers (for information on the NE types supported in Cisco Prime Network 3.9, see Cisco 1700 Series Modular Access Routers):

- Cisco 1700 Series—Supported Software Versions, page 6-9
- Cisco 1700 Series—Supported Topologies, page 6-9
- Cisco 1700 Series—Supported Modules, page 6-9
- Cisco 1700 Series—Supported Technologies, page 6-10
- Cisco 1700 Series—Supported Service Events, page 6-11

Cisco 1700 Series—Supported Software Versions

Table 6-10 Supported Software Versions for Cisco 1700 Series—Cisco Prime Network 3.9

Software Version	Product_Version
12.1(3)XP3	3.6.1
12.4(11)T	3.6.2
12.3(14)T	3.6.2
12.3(14)T7	3.6.4

Cisco 1700 Series—Supported Topologies

Table 6-11 Supported Topologies for Cisco 1700 Series—Cisco Prime Network 3.9

Topology Type	Link Type	Product_Version
ATM	ATM	3.6.0
BGP	BGP	3.6.0
Ethernet	Ethernet	3.6.0
GRE Tunnel	GRE Tunnel	3.6.1
Physical Layer	Physical Layer	3.6.1

Cisco 1700 Series—Supported Modules

Table 6-12 Supported Modules for Cisco 1700 Series—Cisco Prime Network 3.9

Module Name	Product_Version	Module Description
WIC-1SHDSL-V3	3.6.0	1-port G.shdsl WIC with Four Wire Support (spare + system)
VWIC-2MFT-T1	3.6.0	2-Port RJ-48 Multiflex Trunk - T1
VWIC-2MFT-E1	3.6.0	2-port RJ-48 Multifled Trunk - E1
VWIC-2MFT-T1-DI	3.6.0	2-Port RJ-48 Multiflex Trunk - T1 With Drop and Insert
VWIC-2MFT-E1-DI	3.6.0	2-Port RJ-48 Multiflex Trunk - E1 With Drop and Insert
WIC-1ENET	3.6.0	1-port ethernet WAN Interface card
MPC860	3.6.0	Power PC processor, such as in the Cisco 1700 Series
WIC-1DSU-T1	3.6.0	1-port T1/Fractional T1 DSU/CSU WAN Interface card

Table 6-12 Supported Modules for Cisco 1700 Series—Cisco Prime Network 3.9 (continued)

Module Name	Product_Version	Module Description
AIM-VPN/BP	3.6.0	DES/3DES VPN Encryption AIM-Base Performance
AIM-VPN/BPII	3.6.0	DES/3DES/AES and Layer 3 (IPPCP) Compression VPN Encryption AIM-Base Performance
AIM-VPN/EPII	3.6.0	DES/3DES/AES and Layer 3 (IPPCP) Compression VPN Encryption AIM-Enhanced Performance
WIC-1DSU-T1-V2	3.6.0	Updated one-port T1/fractional T1 DSU/CSU WIC
VWIC-1MFT-E1	3.6.0	1-Port RJ-48 Multiflex Trunk-E1
WIC-1ADSL	3.6.0	1-port ADSLoPOTS HWIC
WIC-1T	3.6.0	1-Port Serial WAN Interface Card
WIC-2A/S	3.6.0	2-Port Async/Sync Serial WAN Interface Card
WIC-2T	3.6.0	2-Port Serial WAN Interface Card
WIC-1ADSL-DG	3.6.2	1-port ADSLoPOTS WIC with Dying Gasp
WIC-1ADSL-I-DG	3.6.2	1-port ADSLoISDN Wan Interface Card
WIC-1B-U-V2	3.6.2	1-Port ISDN BRI NT-1 WIC
WIC-1SHDSL	3.6.2	One port G.shdsl WIC with 4-wire support

Cisco 1700 Series—Supported Technologies

The following technologies are supported by the Cisco 1700 Series in Cisco Prime Network 3.9:

- IP, page 6-199
- Routing Protocols, page 6-202
- Ethernet, page 6-205
- ATM, page 6-213
- Frame Relay, page 6-217
- PPP, page 6-219
- HDLC, page 6-220
- SONET/SDH, page 6-220
- TDM/DSx, page 6-222
- Security, page 6-237
- Hardware, page 6-238
- Serial, page 6-242
- Additional Technologies, page 6-243
- LocalSwitching, page 6-245
- BFD, page 6-246
- CDP, page 6-249
- Discovery Protocol, page 6-249

Cisco 1700 Series—Supported Service Events

Table 6-13 Supported Service Events for Cisco 1700 Series—Cisco Prime Network 3.9

Event Name	Product_Version	Expedited
Active IP Interfaces Found	3.6.1	Y
All IP Interfaces Down	3.6.1	Y
BGP process up	3.6.1	N
Card Down	3.6.1	Y
Card In	3.6.1	Y
Card Out	3.6.1	Y
Card Up	3.6.1	Y
CPU utilization exceeded upper threshold	3.6.1	N
Device Unsupported	3.6.1	N
Fan-tray down	Prime Network 3.8	N
Fan-tray out	Prime Network 3.8	N
Keepalive configured	3.6.1	N
Keepalive not configured	3.6.1	N
Layer 2 Tunnel Down	3.6.1	N
Link up	3.6.1	N
Memory utilization exceeded upper threshold	3.6.1	N
Module Unsupported	3.6.1	N
MPLS Black Hole found	3.6.1	N
Rx utilization exceeded upper threshold	3.6.1	N
Tx utilization exceeded upper threshold	3.6.1	N
Pluggable transceiver out	Prime Network 3.8	N
Power-supply down	Prime Network 3.8	N
Power-supply out	Prime Network 3.8	N

Cisco 1800 Series Integrated Services Routers

This section includes the following information about Cisco 1800 Series routers (for information on the NE types supported in Cisco Prime Network 3.9, see Cisco 1800 Series Integrated Services Routers):

- Cisco 1800 Series—Supported Software Versions, page 6-12
- Cisco 1800 Series—Supported Topologies, page 6-12
- Cisco 1800 Series—Supported Modules, page 6-13
- Cisco 1800 Series—Supported Technologies, page 6-14
- Cisco 1800 Series—Supported Service Events, page 6-14

Cisco 1800 Series—Supported Software Versions

Table 6-14 Supported Software Versions for Cisco 1800 Series—Cisco Prime Network 3.9

Software Version	Product_Version
12.3(14)T	3.6.2
12.3(8)T11	3.6.4
12.4(11)T	3.6.2
12.4(12)	3.6.4
12.4(12b)	3.6.4
12.4(17)	3.6.4
12.4(22)T	3.6.7[1]
12.4(24)T	3.7[2]
12.4(3)	3.6.3
12.4(3b)	3.6.2
12.4(5a)	3.6.4
12.4(5b)	3.6.4
12.4(8)	3.6.4

[1, 2]ANA recognizes all maintenance builds in this IOS release train.

Cisco 1800 Series—Supported Topologies

Table 6-15 Supported Topologies for Cisco 1800 Series—Cisco Prime Network 3.9

Topology Type	Link Type	Product_Version
ATM	ATM	3.6.0
BGP	BGP	3.6.0

Table 6-15 Supported Topologies for Cisco 1800 Series—Cisco Prime Network 3.9 (continued)

Topology Type	Link Type	Product_Version
Ethernet	Ethernet	3.6.0
GRE Tunnel	GRE Tunnel	3.6.0
Physical Layer	Physical Layer	3.6.0

Cisco 1800 Series—Supported Modules

Table 6-16 Supported Modules for Cisco 1800 Series—Cisco Prime Network 3.9

Module Name	Product_Version	Module Description
AIM-VPN-EPII-PLUS	3.6.0	Virtual Private Network (VPN) Module
C1841 MOTHERBOARD WITH 2 FAST ETHERNET	3.6.0	C1841 Motherboard with 2 Fast Ethernet
HWIC-16A	3.6.0	16-Port Async HWIC
HWIC-4A/S	3.6.0	4-Port Async/Sync Serial HWIC
HWIC-4T	3.6.0	4-Port Serial HWIC
HWIC-8A	3.6.0	8-Port Async HWIC
HWIC-8A/S-232	3.6.0	8-Port Async/Sync Serial HWIC, EIA-232
VWIC-2MFT-E1-DI	3.6.0	2-port RJ-48 multiflex trunk-E1 with drop and insertñ data only
VWIC-2MFT-G703	3.6.0	2-port RJ-48 multiflex trunk-G.703ñ data only
VWIC-2MFT-T1-DI	3.6.0	2-port RJ-48 multiflex trunk-T1 with drop and insertñ data only
WIC-1ADSL	3.6.0	1-port asymmetric DSL (ADSL) over basic telephone service WIC
WIC-1ADSL-DG	3.6.0	1-port ADSLoPOTS WIC with Dying Gasp
WIC-1B-U-V2	3.6.2	1-Port ISDN BRI NT-1 WIC
WIC-1DSU-T1-V2	3.6.0	1-port T1/Fractional-T1 CSU/DSU WIC
WIC-1SHDSL-V3	3.6.0	One port G.shdsl WIC with 4-wire support
WIC-1T	3.6.0	1-Port Serial WAN Interface Card
WIC-2A/S	3.6.0	2-Port Async/Sync Serial WAN Interface Card
WIC-2AM	3.6.0	2-port analog modem WIC
WIC-2T	3.6.0	2-Port Serial WAN Interface Card

Cisco 1800 Series—Supported Technologies

The following technologies are supported by the Cisco 1800 Series in Cisco Prime Network 3.9:

- IP, page 6-199
- Routing Protocols, page 6-202
- Ethernet, page 6-205
- ATM, page 6-213
- Frame Relay, page 6-217
- PPP, page 6-219
- HDLC, page 6-220
- SONET/SDH, page 6-220
- TDM/DSx, page 6-222
- VPN (VRF), page 6-233
- Security, page 6-237
- Hardware, page 6-238
- Serial, page 6-242
- Additional Technologies, page 6-243
- LocalSwitching, page 6-245
- CDP, page 6-249
- Discovery Protocol, page 6-249

Cisco 1800 Series—Supported Service Events

Table 6-17 Supported Service Events for Cisco 1800 Series—Cisco Prime Network 3.9

Event Name	Product_Version	Expedited
Device Unsupported	3.6.0	Y
Fan-tray down	Prime Network 3.8	N
Fan-tray out	Prime Network 3.8	N
Link up	3.6.0	Y
Module Unsupported	3.6.0	N
Pluggable transceiver out	Prime Network 3.8	N

Table 6-17 Supported Service Events for Cisco 1800 Series—Cisco Prime Network 3.9

Event Name	Product_Version	Expedited
Power-supply down	Prime Network 3.8	N
Power-supply out	Prime Network 3.8	N

Cisco 2500 Series Routers

This section includes the following information about Cisco 2500 Series routers (for information on the NE types supported in Cisco Prime Network 3.9, see Cisco 2500 Series Routers):

- Cisco 2500 Series—Supported Software Versions, page 6-15
- Cisco 2500 Series—Supported Topologies, page 6-15
- Cisco 2500 Series—Supported Modules, page 6-16
- Cisco 2500 Series—Supported Technologies, page 6-16
- Cisco 2500 Series—Supported Service Events, page 6-16

Cisco 2500 Series—Supported Software Versions

Table 6-18 Supported Software Versions for Cisco 2500 Series—Cisco Prime Network 3.9

Software Version	Product_Version
11.2(18)	3.6.0
12.0(17a)	3.6.0

Cisco 2500 Series—Supported Topologies

Table 6-19 Supported Topologies for Cisco 2500 Series—Cisco Prime Network 3.9

Topology Type	Link Type	Product_Version
ATM	ATM	3.6.0
BGP	BGP	3.6.0
Ethernet	Ethernet	3.6.0
Framerelay	Framerelay	3.6.0
Physical Layer	Physical Layer	3.6.0

Cisco 2500 Series—Supported Modules

Table 6-20 Supported Modules for Cisco 2500 Series—Cisco Prime Network 3.9

Module Name	Product_Version	Module Description
CPU-2500	3.6.0	Cisco 2500 CPU card

Cisco 2500 Series—Supported Technologies

The following technologies are supported by the Cisco 2500 Series in Cisco Prime Network 3.9:

- IP, page 6-199
- Routing Protocols, page 6-202
- Ethernet, page 6-205
- ATM, page 6-213
- Frame Relay, page 6-217
- SONET/SDH, page 6-220
- TDM/DSx, page 6-222
- MPLS, page 6-226
- VPN (VRF), page 6-233
- Security, page 6-237
- Hardware, page 6-238
- Serial, page 6-242
- Additional Technologies, page 6-243
- LocalSwitching, page 6-245
- CDP, page 6-249
- Discovery Protocol, page 6-249

Cisco 2500 Series—Supported Service Events

Table 6-21 Supported Service Events for Cisco 2500 Series—Cisco Prime Network 3.9

Event Name	Product_Version	Expedited
Active IP Interfaces Found	3.6.0	Y
All IP Interfaces Down	3.6.0	Y
BGP process up	3.6.0	N
Card Down	3.6.0	Y
Card In	3.6.0	Y

Table 6-21 Supported Service Events for Cisco 2500 Series—Cisco Prime Network 3.9

Event Name	Product_Version	Expedited
Card Out	3.6.0	Y
Card Up	3.6.0	Y
CPU utilization exceeded upper threshold	3.6.0	N
Device Unsupported	3.6.0	N
Fan-tray down	Prime Network 3.8	N
Fan-tray out	Prime Network 3.8	N
Keepalive configured	3.6.0	N
Keepalive not configured	3.6.0	N
Layer 2 Tunnel Down	3.6.0	N
Link up	3.6.0	N
Memory utilization exceeded upper threshold	3.6.0	N
Module Unsupported	3.6.0	N
MPLS Black Hole found	3.6.0	N
Rx utilization exceeded upper threshold	3.6.0	N
Tx utilization exceeded upper threshold	3.6.0	N
BFD neighbor found	3.7.1	N
BFD neighbor loss	3.7.1	N
CGN statistics dropsPortLimitIn2Out higher threshold exceeded	3.7.1	N
CGN statistics dropsSystemLimitIn2Out higher threshold exceeded	3.7.1	N
CGN statistics fwdIn2Out higher threshold exceeded	3.7.1	N
CGN statistics fwdOut2In higher threshold exceeded	3.7.1	N
Pluggable transceiver out	Prime Network 3.8	N
Power-supply down	Prime Network 3.8	N

Table 6-21 Supported Service Events for Cisco 2500 Series—Cisco Prime Network 3.9

Event Name	Product_Version	Expedited
Power-supply out	Prime Network 3.8	N

Cisco 2600 Series Multiservice Platform Routers

This section includes the following information about Cisco 2600 Series routers (for information on the NE types supported in Cisco Prime Network 3.9, see Cisco 2600 Series Multiservice Platform Routers):

- Cisco 2600 Series—Supported Software Versions, page 6-18
- Cisco 2600 Series—Supported Topologies, page 6-19
- Cisco 2600 Series—Supported Modules, page 6-19
- Cisco 2600 Series—Supported Technologies, page 6-20
- Cisco 2600 Series—Supported Service Events, page 6-21

Cisco 2600 Series—Supported Software Versions

Table 6-22 Supported Software Versions for Cisco 2600 Series—Cisco Prime Network 3.9

Software Version	Product_Version
11.3(10)T	3.6.1
12.0(3)T3	3.6.1
12.2(15)T	3.6.1
12.2(17a)	3.6.1
12.2(8)T5	3.6.1
12.3(15a)	3.6.2
12.3(17a)	3.6.1
12.3(3i)	3.6.4
12.3(4)	3.6.1
12.4(10)	3.6.1

Cisco 2600 Series—Supported Topologies

Table 6-23 Supported Topologies for Cisco 2600 Series—Cisco Prime Network 3.9

Topology Type	Link Type	Product_Version
ATM	ATM	3.6.0
BGP	BGP	3.6.0
Ethernet	Ethernet	3.6.0
Framerelay	Framerelay	3.6.0
Physical Layer	Physical Layer	3.6.0

Cisco 2600 Series—Supported Modules

Table 6-24 Supported Modules for Cisco 2600 Series—Cisco Prime Network 3.9

Module Name	Product_Version	Module Description
AIM-VOICE-30	3.6.0	AIM supporting voice/fax DSP features
ATM-AIM	3.6.0	AIM(Advanced Integration Module) supporting ATM features for Cisco 2600, 2600XM, 2691, 3660, and 3700
NM-16AM-V2	3.6.0	16-port analog modem network module with V.92
NM-1A-T3 AND NM-1A-E3	3.6.0	DS3/E3 ATM Network Modules for the Cisco 2600, 2800, 3600, 3700 and 3800 Series Routers
NM-1CE1T1-PRI	3.6.0	1-port Channelized E1/T1/ISDN PRI network module
NM-1FE1R2W	3.6.0	1 10/100 Ethernet 14/16 Token Ring 2 WAN card slot network module
NM-1FE2W	3.6.0	1 10/100 Ethernet 2 WAN card slot network module
NM-1T3/E3	3.6.0	One-port clear-channel T3/E3 network module
NM-1T3/E3(12)	3.6.0	1-port Clear Channel
NM-2CE1T1-PRI	3.6.0	2-port Channelized E1/T1/ISDN PRI network module
NM-2FE2W	3.6.0	2 10/100 Ethernet 2 WAN card slot network module
NM-2W	3.6.0	2 WIC slot network module, (WAN I/F cards offered separately)
NM-8AM-V2	3.6.0	8-port analog modem network module with V.92
NM-AIC-64(6)	3.6.0	Alarm monitoring and control network module; 64 contact points and 16 control points
NM-CUE-EC	3.6.0	Cisco Unity Express Network Module Enhanced Capacity
NM-HDV2	3.6.0	IP Communications high-density digital voice network module

Table 6-24 Supported Modules for Cisco 2600 Series—Cisco Prime Network 3.9 (continued)

Module Name	Product_Version	Module Description
NM-NAM	3.6.0	Network analysis module
VIC2-2E/M	3.6.0	2-port E+M voice/fax interface card
VIC2-2FXS	3.6.0	2-port FXS voice/fax interface card
VIC-2FXO	3.6.0	Two-port FXO voice/fax interface card [also see VIC-2FXO-M1]
VIC-4FXS/DID	3.6.0	4-port FXS voice/fax interface card (Note
VWIC-1MFT-E1	3.6.0	1-Port RJ-48 Multiflex Trunk-E1
VWIC-1MFT-T1	3.6.0	1-Port RJ-48 Multiflex Trunk-T1
VWIC-2MFT-E1	3.6.0	2-Port RJ-48 Multiflex Trunk-E1
VWIC-2MFT-E1-DI	3.6.0	2-Port RJ-48 Multiflex Trunk-E1 With Drop and Insert
VWIC-2MFT-T1	3.6.0	2-Port RJ-48 Multiflex Trunk-T1
VWIC-2MFT-T1-DIR	3.6.0	2-Port RJ-48 Multiflex Trunk-T1 With Drop and Insert
WIC-1ADSL	3.6.0	1-port ADSLoPOTS WAN Interface Card (System)

Cisco 2600 Series—Supported Technologies

The following technologies are supported by the Cisco 2600 Series in Cisco Prime Network 3.9:

- IP, page 6-199
- Routing Protocols, page 6-202
- Ethernet, page 6-205
- ATM, page 6-213
- Frame Relay, page 6-217
- PPP, page 6-219
- HDLC, page 6-220
- SONET/SDH, page 6-220
- TDM/DSx, page 6-222
- VPN (VRF), page 6-233
- Security, page 6-237
- Hardware, page 6-238
- Serial, page 6-242
- Additional Technologies, page 6-243
- LocalSwitching, page 6-245
- CDP, page 6-249
- Discovery Protocol, page 6-249

Cisco 2600 Series—Supported Service Events

Table 6-25 Supported Service Events for Cisco 2600 Series—Cisco Prime Network 3.9

Event Name	Product_Version	Expedited
Active IP Interfaces Found	3.6.1	Y
All IP Interfaces Down	3.6.1	Y
BGP process up	3.6.1	N
Card Down	3.6.1	Y
Card In	3.6.1	Y
Card Out	3.6.1	Y
Card Up	3.6.1	Y
CPU utilization exceeded upper threshold	3.6.1	N
Device Unsupported	3.6.1	N
Fan-tray down	Prime Network 3.8	N
Fan-tray out	Prime Network 3.8	N
Keepalive configured	3.6.1	N
Keepalive not configured	3.6.1	N
Layer 2 Tunnel Down	3.6.1	N
Link up	3.6.1	N
Memory utilization exceeded upper threshold	3.6.1	N
Module Unsupported	3.6.1	N
MPLS Black Hole found	3.6.1	N
Rx utilization exceeded upper threshold	3.6.1	N
Tx utilization exceeded upper threshold	3.6.1	N
Pluggable transceiver out	Prime Network 3.8	N
Power-supply down	Prime Network 3.8	N
Power-supply out	Prime Network 3.8	N

Cisco 2800 Series Integrated Services Routers

This section includes the following information about Cisco 2800 Series routers (for information on the NE types supported in Cisco Prime Network 3.9, see Cisco 2800 Series Integrated Services Routers):

- Cisco 2800 Series—Supported Software Versions, page 6-22
- Cisco 2800 Series—Supported Topologies, page 6-23
- Cisco 2800 Series—Supported Modules, page 6-23
- Cisco 2800 Series—Supported Technologies, page 6-25
- Cisco 2800 Series—Supported Service Events, page 6-26

Cisco 2800 Series—Supported Software Versions

Table 6-26 Supported Software Versions for Cisco 2800 Series—Cisco Prime Network 3.9

Software Version	Product_Version
12.3(11)T5	3.6.2
12.3(11)T6	3.6.2
12.3(14)T	3.6.2
12.3(14)T7	3.6.2
12.3(8)T11	3.6.4
12.3(8)T5	3.6.4
12.3(8)T6	3.6.4
12.3(8)T8	3.6.4
12.3(8)T9	3.6.4
12.4(1)	3.6.1
12.4(10)	3.6.1
12.4(11)T	3.6.2
12.4(12)	3.6.1
12.4(13c)	3.6.4
12.4(13d)	3.6.4
12.4(15)T	3.6.7
12.4(17)	3.6.3
12.4(1a)	3.6.4
12.4(2)T2	3.6.4
12.4(22)T	3.6.7[1]
12.4(24)T	3.7
12.4(24)T1	3.7[2]
12.4(3)	3.6.1

Table 6-26 Supported Software Versions for Cisco 2800 Series—Cisco Prime Network 3.9

Software Version	Product_Version
12.4(3a)	3.7[3]
12.4(5)	3.6.1
12.4(7)	3.6.1
12.4(8)	3.6.1

[1, 2]ANA recognizes all maintenance builds in this IOS release train.

[3]Support tested and validated using AdvanceEnterprise image of 12.4(3a)

Cisco 2800 Series—Supported Topologies

Table 6-27 Supported Topologies for Cisco 2800 Series—Cisco Prime Network 3.9

Topology Type	Link Type	Product_Version
ATM	ATM	3.6.0
BGP	BGP	3.6.0
Ethernet	Ethernet	3.6.0
Framerelay	Framerelay	3.6.0
GRE Tunnel	GRE Tunnel	3.6.0
Physical Layer	Physical Layer	3.6.0

Cisco 2800 Series—Supported Modules

Table 6-28 Supported Modules for Cisco 2800 Series—Cisco Prime Network 3.9

Module Name	Product_Version	Module Description
AIM-VPN/EPII-PLUS	3.7	Enhanced-performance DES, 3DES, AES, and compression VPN encryption AIM
EM-4BRI-NTTE	3.6.0	4-port BRI voice and fax expansion module
HWIC-16A	3.6.0	16-Port Async HWIC
HWIC-1ADSLI	3.6.0	1-port ADSL over ISDN HWIC
HWIC-1FE	3.6.0	1-port Fast Ethernet HWIC
HWIC-1GE-SFP	3.6.0	Cisco Gigabit Ethernet High-Speed Interface Card
HWIC-2SHDSL	3.6.0	2-port G.SHDSL HWIC with 2-wire and 4-wire support
HWIC-4AS	3.6.0	4-Port Async/Sync Serial HWIC

Table 6-28 Supported Modules for Cisco 2800 Series—Cisco Prime Network 3.9 (continued)

Module Name	Product_Version	Module Description
HWIC-4ESW	3.6.0	4-port Cisco EtherSwitch 10BASE-T/100BASE-TX autosensing HWIC
HWIC-4SHDSL	3.6.0	4-port G.SHDSL HWIC with 2-wire, 4-wire, and 8-wire support
HWIC-4T	3.6.0	4-Port serial HWIC
HWIC-8A	3.6.0	8-Port Async HWIC
HWIC-8A/S-232	3.6.0	8-Port Async/Sync Serial HWIC, EIA-232
HWIC-ADSL-BST	3.6.0	2-port HWIC with 1-port ADSLoPOTS and 1-port ISDN BRI-S/T
HWIC-D-9ESW	3.6.7	9 Port FE Switch
NM-16A	3.6.0	16-Port Async HWIC
NM-16AM-V2	3.6.0	16-port analog modem network module with v.92
NM-16AS	3.6.2	16-Port Async/Sync Serial Network Module
NM-1A-E3	3.6.2	1-Port E3 ATM Network Module
NM-1A-T3	3.6.0	1-Port DS3 ATM Network Module
NM-1CE1T1-PRI	3.6.0	1-port Channelized E1/T1/ISDN PRI network module
NM-1HSSI	3.6.2	Single port HSSI network module
NM-1T3E3	3.6.0	1-port clear-channel T3/E3 network module
NM-2CE1T1-PRI	3.6.0	2-port Channelized E1/T1/ISDN PRI network module
NM-32A	3.6.0	32 port Asynchronous Module
NM-4A/S	3.6.0	4-Port Async/Sync Serial Network Module
NM-4B-ST	3.6.2	4-Port ISDN-BRI Network Module
NM-4B-U	3.6.0	4-Port ISDN-BRI with NT-1 Network Module
NM-4T	3.6.0	4-Port Serial Network Module
NM-8AM-V2	3.6.0	8-port analog modem network module with v.92
NM-8B-ST	3.6.2	8-Port ISDN-BRI Network Module
NM-8B-U	3.6.0	8-Port ISDN-BRI with NT-1 Network Module
NM-CUE-EC	3.6.0	Cisco Unity Express Voice-Mail Network Module extended capacity
NM-HD-2V	3.6.0	2-slot IP Communications voice and fax network module
NM-HDV2	3.6.0	IP Communications high-density voice and fax network module
NM-NAM	3.6.0	network analysis module
VIC2-2BRI-NTTE	3.6.0	2-port VIC card-BRI (NT and TE)
VIC2-2FXS	3.6.0	2-port VIC-FXS

Table 6-28 Supported Modules for Cisco 2800 Series—Cisco Prime Network 3.9 (continued)

Module Name	Product_Version	Module Description
VWIC-1MFT-G703	3.6.7	1-Port RJ-48 Multiflex Trunk - E1 for unstructured G.703
VWIC2-1MFT-G703	3.6.7	1-Port T1/E1 Voice/WAN with D+I + unstructured E1 (G703)
VWIC2-1MFT-T1E1	3.6.0	1-Port T1/E1 Voice/WAN with Drop + Insert
VWIC-2MFT-E1-DI	3.6.0	2-port RJ-48 multiflex trunk-E1 with drop and insert
VWIC-2MFT-G703	3.6.0	2-port RJ-48 multiflex trunk-G.703
VWIC-2MFT-T1-DI	3.6.0	2-port RJ-48 multiflex trunk-T1 with drop and insert
WIC-1ADSL	3.6.0	1-port asymmetric DSL (ADSL) over POTS service WIC
WIC-1ADSL-DG	3.6.2	1-port ADSLoPOTS WIC with Dying Gasp
WIC-1ADSL-I-DG	3.6.2	1-port ADSLoISDN Wan Interface Card
WIC-1AM-V2	3.6.0	1-port analog modem WIC (updated version)
WIC-1B-U-V2	3.6.2	1-Port ISDN BRI NT-1 WIC
WIC-1DSU-T1-V2	3.6.2	Updated 1-Port T1/Fractional T1 DSU/CSU WAN Interface Card
WIC-1SHDSL	3.6.2	One port G.shdsl WIC with 4-wire support
WIC-1SHDSL-V3	3.6.0	1-port G.SHDSL WIC with 4-wire support
WIC-1T	3.6.0	1-Port Serial WAN Interface Card
WIC-2AM-V2	3.6.0	2-port analog modem WIC (updated version)
WIC-2AS	3.6.0	2-Port Async/Sync Serial WAN Interface Card
WIC-2T	3.6.0	2-Port Serial WAN Interface Card

Cisco 2800 Series—Supported Technologies

The following technologies are supported by the Cisco 2800 Series in Cisco Prime Network 3.9:

- IP, page 6-199
- Routing Protocols, page 6-202
- Ethernet, page 6-205
- ATM, page 6-213
- Frame Relay, page 6-217
- PPP, page 6-219
- HDLC, page 6-220
- SONET/SDH, page 6-220
- TDM/DSx, page 6-222
- VPN (VRF), page 6-233

- Security, page 6-237
- Hardware, page 6-238
- Serial, page 6-242
- Additional Technologies, page 6-243
- LocalSwitching, page 6-245

Cisco 2800 Series—Supported Service Events

Table 6-29 Supported Service Events for Cisco 2800 Series—Cisco Prime Network 3.9

Event Name	Product_Version	Expedited
Active IP Interfaces Found	3.6.1	Y
All IP Interfaces Down	3.6.1	Y
BGP process up	3.6.1	N
Card Down	3.6.1	Y
Card In	3.6.1	Y
Card Out	3.6.1	Y
Card Up	3.6.1	Y
CPU utilization exceeded upper threshold	3.6.1	N
Device Unsupported	3.6.1	N
Fan-tray down	Prime Network 3.8	N
Fan-tray out	Prime Network 3.8	N
Keepalive configured	3.6.1	N
Keepalive not configured	3.6.1	N
Layer 2 Tunnel Down	3.6.1	N
Link up	3.6.1	N
Memory utilization exceeded upper threshold	3.6.1	N
Module Unsupported	3.6.1	N
MPLS Black Hole found	3.6.1	N
Rx utilization exceeded upper threshold	3.6.1	N
Tx utilization exceeded upper threshold	3.6.1	N

Table 6-29 Supported Service Events for Cisco 2800 Series—Cisco Prime Network 3.9

Event Name	Product_Version	Expedited
Pluggable transceiver out	Prime Network 3.8	N
Power-supply down	Prime Network 3.8	N
Power-supply out	Prime Network 3.8	N

Cisco 3600 Series Multiservice Platform Routers

This section includes the following information about Cisco 3600 Series routers (for information on the NE types supported in Cisco Prime Network 3.9, see Cisco 3600 Series Multiservice Platform Routers):

- Cisco 3600 Series—Supported Software Versions, page 6-27
- Cisco 3600 Series—Supported Topologies, page 6-28
- Cisco 3600 Series—Supported Modules, page 6-28
- Cisco 3600 Series—Supported Technologies, page 6-28
- Cisco 3600 Series—Supported Service Events, page 6-29

Cisco 3600 Series—Supported Software Versions

Table 6-30 Supported Software Versions for Cisco 3600 Series—Cisco Prime Network 3.9

Software Version	Product_Version
IOS 12.0(0.20)T	3.6.0
IOS 12.0(3)T3	3.6.0
IOS 12.0(4)T	3.6.0
IOS 12.0(5)	3.6.0
IOS 12.0(5)T1	3.6.0
IOS 12.0(6.5)T3	3.6.0
IOS 12.0(7)XK1	3.6.0
IOS 12.1(20)	3.6.0
IOS 12.2(12)	3.6.0
IOS 12.2(4)T1	3.6.0
IOS 12.2(8)T5	3.6.0
IOS 12.2(27)	3.6.2

Cisco 3600 Series—Supported Topologies

Table 6-31 Supported Topologies for Cisco 3600 Series—Cisco Prime Network 3.9

Topology Type	Link Type	Product_Version
Ethernet	Ethernet	3.6.0
Physical Layer	Physical Layer	3.6.0

Cisco 3600 Series—Supported Modules

Table 6-32 Supported Modules for Cisco 3600 Series—Cisco Prime Network 3.9

Module Name	Product_Version	Module Description
CPU-3600	3.6.0	Cisco 3600 CPU
NM-2FE-2W	3.6.0	FastEthernet/WAN
PM-1E	3.6.0	One Port Ethernet
PM-2CE1-UNBALANCED	3.6.0	Two Port Channelized E1/PRI (75 ohm, unbalanced)
PM-4E	3.6.0	Four Port Ethernet
PM-C3600-1FE-TX	3.6.0	One port Fastethernet TX
WIC-SERIAL-1T	3.6.0	WAN Interface Card - Serial (1T)

Cisco 3600 Series—Supported Technologies

The following technologies are supported by the Cisco 3600 Series in Cisco Prime Network 3.9:

- IP, page 6-199
- Routing Protocols, page 6-202
- Ethernet, page 6-205
- ATM, page 6-213
- Frame Relay, page 6-217
- PPP, page 6-219
- SONET/SDH, page 6-220
- TDM/DSx, page 6-222
- MPLS, page 6-226
- MPLS-TE, page 6-228
- VPN (VRF), page 6-233
- PWE3, page 6-235
- Security, page 6-237
- Hardware, page 6-238

- Serial, page 6-242
- Additional Technologies, page 6-243
- LocalSwitching, page 6-245
- CDP, page 6-249
- Discovery Protocol, page 6-249

Cisco 3600 Series—Supported Service Events

Table 6-33 Supported Service Events for Cisco 3600 Series—Cisco Prime Network 3.9

Event Name	Product_Version	Expedited
Active ip interfaces found	3.7.1	N
All ip interfaces down	3.7.1	N
Device Unsupported	3.6.0	N
Layer 2 Tunnel Down	3.6.0	N
Module Unsupported	3.6.0	N

Cisco 3700 Series Multiservice Access Routers

This section includes the following information about Cisco 3700 Series routers (for information on the NE types supported in Cisco Prime Network 3.9, see Cisco 3700 Series Multiservice Access Routers):

- Cisco 3700 Series—Supported Software Versions, page 6-29
- Cisco 3700 Series—Supported Topologies, page 6-30
- Cisco 3700 Series—Supported Modules, page 6-30
- Cisco 3700 Series—Supported Technologies, page 6-31
- Cisco 3700 Series—Supported Service Events, page 6-31

Cisco 3700 Series—Supported Software Versions

Table 6-34 Supported Software Versions for Cisco 3700 Series—Cisco Prime Network 3.9

Software Version	Product_Version
12.3(15b)	3.6.2
12.4(9)T	3.6.0

Cisco 3700 Series—Supported Topologies

Table 6-35 Supported Topologies for Cisco 3700 Series—Cisco Prime Network 3.9

Topology Type	Link Type	Product_Version
Ethernet	Ethernet	3.6.0
MPLS	MPLS	3.6.0
Physical Layer	Physical Layer	3.6.0
LAG	LAG	3.6.0

Cisco 3700 Series—Supported Modules

Table 6-36 Supported Modules for Cisco 3700 Series—Cisco Prime Network 3.9

Module Name	Product_Version	Module Description
NM-16ESW	3.6.0	16 port 10/100 EtherSwitch NM
NM-1FE2W	3.6.0	1 10/100 Ethernet 2 WAN Card Slot Network Module
NM-2FE2W	3.6.0	2 10/100 Ethernet 2 WAN Card Slot Network Module
NM-2W	3.6.0	2 WAN Card Slot Network Module(no LAN)
NM-1T3/E3	3.6.0	1-Port Clear-channel T3/E3 Network Module
NM-1HSSI	3.6.0	Single port HSSI network module
NM-1CE1T1-PRI	3.6.0	1-Port Channelized T1 / E1 Modules with PRI Network Modules
NM-2CE1T1-PRI	3.6.0	2-Port Channelized T1 / E1 Modules with PRI Network Modules
VIC-2E/M	3.6.0	Two-port Voice Interface Card - EandM
VIC-2FXO	3.6.0	Two-port Voice Interface Card - FXO
VIC-2FXS	3.6.0	Two-port Voice Interface Card - FXS
VWIC-2MFT-G703	3.6.0	2-Port RJ-48 Multiflex Trunk - G.703
VWIC-2MFT-T1	3.6.0	2-Port RJ-48 Multiflex Trunk - T1
VWIC-2MFT-E1	3.6.0	2-Port RJ-48 Multiflex Trunk - E1
WIC-2AM	3.6.0	Two-port Analog Modem WAN Interface Card
WIC-1ADSL-I-DG	3.6.0	1-Port ADSLoISDN WAN Interface Card
NM-2FE2W-V2	3.7	2-port 10/100 Ethernet 2 WAN Card Slot Network Module

Cisco 3700 Series—Supported Technologies

The following technologies are supported by the Cisco 3700 Series in Cisco Prime Network 3.9:

- IP, page 6-199
- Routing Protocols, page 6-202
- Ethernet, page 6-205
- ATM, page 6-213
- Frame Relay, page 6-217
- PPP, page 6-219
- SONET/SDH, page 6-220
- TDM/DSx, page 6-222
- MPLS, page 6-226
- MPLS-TE, page 6-228
- VPN (VRF), page 6-233
- PWE3, page 6-235
- Security, page 6-237
- Hardware, page 6-238
- Serial, page 6-242
- Additional Technologies, page 6-243
- LocalSwitching, page 6-245
- CDP, page 6-249
- Discovery Protocol, page 6-249

Cisco 3700 Series—Supported Service Events

Table 6-37 Supported Service Events for Cisco 3700 Series—Cisco Prime Network 3.9

Event Name	Product_Version	Expedited
Active IP Interfaces Found	3.6.0	Y
All IP Interfaces Down	3.6.0	Y
BGP process up	3.6.0	N
Card Down	3.6.0	Y
Card In	3.6.0	Y
Card Out	3.6.0	Y
Card Up	3.6.0	Y
CPU utilization exceeded upper threshold	3.6.0	N
Device Unsupported	3.6.0	N

Table 6-37 Supported Service Events for Cisco 3700 Series—Cisco Prime Network 3.9

Event Name	Product_Version	Expedited
Fan-tray down	Prime Network 3.8	N
Fan-tray out	Prime Network 3.8	N
Keepalive configured	3.6.0	N
Keepalive not configured	3.6.0	N
Layer 2 Tunnel Down	3.6.0	N
Link up	3.6.0	N
Memory utilization exceeded upper threshold	3.6.0	N
Module Unsupported	3.6.0	N
MPLS Black Hole found	3.6.0	N
Rx utilization exceeded upper threshold	3.6.0	N
Tx utilization exceeded upper threshold	3.6.0	N
Pluggable transceiver out	Prime Network 3.8	N
Power-supply down	Prime Network 3.8	N
Power-supply out	Prime Network 3.8	N

Cisco 3800 Series Integrated Services Routers

This section includes the following information about Cisco 3800 Series routers (for information on the NE types supported in Cisco Prime Network 3.9, see Cisco 3800 Series Integrated Services Routers):

- Cisco 3800 Series—Supported Software Versions, page 6-33
- Cisco 3800 Series—Supported Topologies, page 6-33
- Cisco 3800 Series—Supported Modules, page 6-34
- Cisco 3800 Series—Supported Technologies, page 6-35
- Cisco 3800 Series—Supported Service Events, page 6-36

Cisco 3800 Series—Supported Software Versions

Table 6-38 Supported Software Versions for Cisco 3800 Series—Cisco Prime Network 3.9

Software Version	Product_Version
IOS 12.3(14)T	3.6.2
IOS 12.3(14)T7	3.6.2
IOS 12.4(11)T	3.6.2[1]
IOS 12.4(22)T	3.6.7[2]
IOS 12.4(24)T	3.7[3]
15.1(1)T	Cisco-ANA3.7.X-DP13 , PrimeNetwork-3.8.X-DP4
15.1(2)T	Cisco-ANA3.7.X-DP13 , PrimeNetwork-3.8.X-DP4
15.1(3)T	Cisco-ANA3.7.X-DP13 , PrimeNetwork-3.8.X-DP4

[1]ANA models pluggable ports for this IOS version.

[2, 3]ANA recognizes all maintenance builds in this IOS release train.ANA models pluggable ports for this IOS version.

Cisco 3800 Series—Supported Topologies

Table 6-39 Supported Topologies for Cisco 3800 Series—Cisco Prime Network 3.9

Topology Type	Link Type	Product_Version
ATM	ATM	3.6.0
BGP	BGP	3.6.0
Ethernet	Ethernet	3.6.0
PPP/HDLC	PPP or HDLC	3.6.0
PWE3 (Martini)	Tunnel	3.6.0
GRE Tunnel	GRE Tunnel	3.6.0
VPN (VRF)	VPN	3.6.0
Physical Layer	Physical Layer	3.6.0

Cisco 3800 Series—Supported Modules

Table 6-40 Supported Modules for Cisco 3800 Series—Cisco Prime Network 3.9

Module Name	Product_Version	Module Description
AIM-VPN/EPII-PLUS	3.6.1	DES/3DES/AES VPN Encryption/Compression
HWIC-16A	3.6.1	16-Port Async HWIC
HWIC-1GE-SFP	3.6.1	GigE High Speed WIC With One SFP Slot
HWIC-4A/S	3.6.1	4-Port Async/Sync Serial HWIC
HWIC-4T	3.6.1	4-Port Serial HWIC
HWIC-8A	3.6.1	8-Port Async HWIC
HWIC-8A/S-232	3.6.1	8-Port Async/Sync Serial HWIC, EIA-232
NM-16A	3.6.1	16 port Asynchronous Module
NM-16A/S	3.6.2	16-Port Async/Sync Serial Network Module
NM-1A-E3	3.6.2	1-Port E3 ATM Network Module
NM-1A-T3	3.6.1	1-Port DS3 ATM Network Module
NM-1CE1T1-PRI	3.6.1	1-Port Channelized E1/T1/ISDN-PRI Network Module
NM-1FE1R2W	3.6.1	1 10/100 Ethernet 1 4/16 Token-Ring 2 WAN Card Slot NM
NM-1FE2W	3.6.1	Network Module with One-Fast Ethernet and Two-WIC slots
NM-1GE	3.6.2	1 Port GE Network Module
NM-1HSSI	3.6.1	Single port HSSI network module
NM-1T3/E3	3.6.1	One port T3/E3 network module
NM-2CE1T1-PRI	3.6.1	2-Port Channelized E1/T1/ISDN-PRI Network Module
NM-2FE2W-V2=	3.6.7	2-port 10/100 Ethernet 2 WAN Card Slot Network Module
NM-2W	3.6.1	2 WAN Card Slot Network Module(no LAN)
NM-32A	3.6.1	32 port Asynchronous Module
NM-4A/S	3.6.1	4-Port Async/Sync Serial Network Module
NM-4B-S/T	3.6.2	4-Port ISDN-BRI Network Module
NM-4B-U	3.6.1	4-Port ISDN-BRI with NT-1 Network Module
NM-4T	3.6.1	4-Port Serial Network Module
NM-8B-S/T	3.6.2	8-Port ISDN-BRI Network Module
NM-8B-U	3.6.1	8-Port ISDN-BRI with NT-1 Network Module
WIC-1ADSL	3.6.1	1-port ADSL WAN Interface Card
WIC-1ADSL-DG	3.6.2	1-port ADSLoPOTS WIC with Dying Gasp
WIC-1ADSL-I-DG	3.6.2	1-port ADSLoISDN Wan Interface Card

Table 6-40 Supported Modules for Cisco 3800 Series—Cisco Prime Network 3.9 (continued)

Module Name	Product_Version	Module Description
WIC-1B-U-V2	3.6.2	1-Port ISDN BRI NT-1 WIC
WIC-1DSU-T1-V2	3.6.2	Updated 1-Port T1/Fractional T1 DSU/CSU WAN Interface Card
WIC-1SHDSL	3.6.2	1-port G.shdsl WIC (two wire only)
WIC-1SHDSL-V2	3.6.1	1-Port G.SHDSL WIC with Four Wire Suppor
WIC-1T	3.6.1	1-Port Serial WAN Interface Card
WIC-2A/S	3.6.1	2-Port Async/Sync Serial WAN Interface Card
WIC-2T	3.6.1	2-Port Serial WAN Interface Card

Cisco 3800 Series—Supported Technologies

The following technologies are supported by the Cisco 3800 Series in Cisco Prime Network 3.9:

- IP, page 6-199
- Routing Protocols, page 6-202
- Ethernet, page 6-205
- ATM, page 6-213
- Frame Relay, page 6-217
- PPP, page 6-219
- HDLC, page 6-220
- TDM/DSx, page 6-222
- MPLS, page 6-226
- MPLS-TE, page 6-228
- VPN (VRF), page 6-233
- PWE3, page 6-235
- Security, page 6-237
- Hardware, page 6-238
- Serial, page 6-242
- CDP, page 6-249
- Discovery Protocol, page 6-249

Cisco 3800 Series—Supported Service Events

Table 6-41 Supported Service Events for Cisco 3800 Series—Cisco Prime Network 3.9

Event Name	Product_Version	Expedited
Active IP Interfaces Found	3.6.0	Y
All IP Interfaces Down	3.6.0	Y
BGP process up	3.6.0	N
Card Down	3.6.0	Y
Card In	3.6.0	Y
Card Out	3.6.0	Y
Card Up	3.6.0	Y
CPU utilization exceeded upper threshold	3.6.0	N
Device Unsupported	3.6.0	N
Fan-tray down	Prime Network 3.8	N
Fan-tray out	Prime Network 3.8	N
Layer 2 Tunnel Down	3.6.0	N
Link up	3.6.0	N
Memory utilization exceeded upper threshold	3.6.0	N
Module Unsupported	3.6.0	N
MPLS Black Hole found	3.6.0	N
Pluggable transceiver out	Prime Network 3.8	N
Power-supply down	Prime Network 3.8	N
Power-supply out	Prime Network 3.8	N

Cisco 7200 Series Routers

This section includes the following information about Cisco 7200 Series routers (for information on the NE types supported in Cisco Prime Network 3.9, see Cisco 7200 Series Routers):

- Cisco 7200 Series—Supported Software Versions, page 6-37

- Cisco 7200 Series—Supported Topologies, page 6-40
- Cisco 7200 Series—Supported Modules, page 6-40
- Cisco 7200 Series—Supported Technologies, page 6-43
- Cisco 7200 Series—Supported Service Events, page 6-44

Cisco 7200 Series—Supported Software Versions

Table 6-42 Supported Software Versions for Cisco 7200 Series—Cisco Prime Network 3.9

Software Version	Product_Version
12.2(31)SB3x	3.6.1
IOS 11.3(7)T	3.6.1
IOS 12.0(21)s7	3.6.2
IOS 12.0(22)S5	3.6.1
IOS 12.0(23)S3.0619	3.6.1
IOS 12.0(23)S4	3.6.1
IOS 12.0(23)S6	3.6.1
IOS 12.0(23)S6.0412	3.6.1
IOS 12.0(24)S3	3.6.1
IOS 12.0(25)S2	3.6.1
IOS 12.0(26)S4	3.6.1
IOS 12.0(26)S5	3.6.1
IOS 12.0(26)S6	3.6.1
IOS 12.0(27)S1	3.6.1
IOS 12.0(32)S6	3.6.0
IOS 12.0(33)S	3.6.2
IOS 12.0(33)S1	3.6.2[1]
IOS 12.1(10)E	3.6.0
IOS 12.1(19)E6	3.6.0
IOS 12.1(1a)	3.6.0
IOS 12.2(12)	3.6.0
IOS 12.2(15)B	3.6.0
IOS 12.2(15)T5	3.6.0
IOS 12.2(18)S12	3.6.2
IOS 12.2(18)s3	3.6.2
IOS 12.2(18.2)	3.6.0
IOS 12.2(25)s2	3.6.2

Table 6-42 Supported Software Versions for Cisco 7200 Series—Cisco Prime Network 3.9 (continued)

Software Version	Product_Version
IOS 12.2(25)s6	3.6.2
IOS 12.2(25)s9	3.6.2
IOS 12.2(27)SBC2	3.6.2
IOS 12.2(28)SB8	3.7.1
IOS 12.2(31)SB	3.6.4
IOS 12.2(31)SB10	3.6.3[2]
IOS 12.2(31)SB12	3.6.4
IOS 12.2(33)SRA	3.6.0
IOS 12.2(33)SRC	3.6.2[3]
IOS 12.2(33)SRC1	3.7.1[4]
IOS 12.2(33)SRC2	3.7.1[5]
IOS 12.2(33)SRC3	3.6.7[6]
IOS 12.2(33)SRC4	3.7.1
IOS 12.2(33)SRC5	3.7.1
IOS 12.2(33)SRC6	3.7.1
IOS 12.2(33)SRD	3.7.1[7]
IOS 12.2(33)SRD1	3.6.6[8]
IOS 12.2(33)SRD2	3.7.1
IOS 12.2(33)SRD3	3.7.1
IOS 12.2(33)SRD4	3.7.1
IOS 12.2(34)	3.6.0[9]
IOS 12.2(37)	3.6.0[10]
IOS 12.2(40)	3.6.0[11]
IOS 12.2.(31)SB11	3.7[12]
IOS 12.3(10)	3.6.0[13]
IOS 12.3(10b)	3.6.2
IOS 12.3(10c)	3.6.2
IOS 12.3(10d)	3.6.2
IOS 12.3(12.10)	3.6.0
IOS 12.3(15a)	3.6.0
IOS 12.3(17)	3.6.2
IOS 12.3(17a)	3.6.2
IOS 12.3(20)	3.6.2
IOS 12.3(21)	3.6.2
IOS 12.3(26)	3.6.4[14]

Table 6-42 Supported Software Versions for Cisco 7200 Series—Cisco Prime Network 3.9 (continued)

Software Version	Product_Version
IOS 12.3(3)B1	3.6.0
IOS 12.3(6e)	3.6.2
IOS 12.3(6f)	3.6.2
IOS 12.3(7)XI7a	3.6.0
IOS 12.4(11)T1	3.6.1
IOS 12.4(20)T	3.7[15]
IOS 12.4(24)T	3.7.1
IOS 12.2(33)SRD5	3.7.1.0.4
IOS 12.2(33)SRE2	3.7.1.0.4
IOS 12.2(33)SRE1	3.7.1.0.4
IOS 12.2(33)SRE	3.7.1.0.4
IOS 12.2(31)SB18	3.7.1.1.0
IOS 12.4(15)T1	3.7.1.1.0
IOS 12.2(33)SRD6	3.7.2-DP-1.0
IOS 12.2(33)SRE3	3.7.2-DP-1.0
IOS 12.2(33)SRE4	3.7.X-DP-4.0
IOS 15.1(3)S	3.7.X-DP-7.0
IOS 12.2(33)SRD7	3.7.X-DP-9.0
IOS 15.1(3)S1	3.7.X-DP-9.0

[1, 2, 12, 13, 14]ANA models pluggable ports for this IOS version.

[3]ANA recognizes all maintenance builds in this IOS release train.Physical Inventory for SP Services images of this IOS version will not be modeled since inventory data is not available using CLI and SNMP.Images other than SP services like IP services/Advanced Enter Services do not have this issue.

[4, 5, 6]Physical Inventory for this IOS(SP Services) version will not be modeled since inventory data is not available using CLI and SNMP.Support tested + validated using AdvancedEnterprises image.ANA models pluggable ports for this IOS version.

[7]Physical Inventory for this IOS (SP Services) version will not be modeled since inventory data is not available using CLI and SNMP.

[8]ANA recognizes all maintenance builds in this IOS release train.Physical Inventory for this IOS(SP Services) version will not be modeled since inventory data is not available using CLI and SNMP.ANA models pluggable ports for this IOS version.

[9, 15]ANA recognizes all maintenance builds in this IOS release train.ANA models pluggable ports for this IOS version.

[10, 11]ANA recognizes all maintenance builds in this IOS release train.

Cisco 7200 Series—Supported Topologies

Table 6-43 Supported Topologies for Cisco 7200 Series—Cisco Prime Network 3.9

Topology Type	Link Type	Product_Version
ATM	ATM	3.6.0
BGP	BGP	3.6.0
Ethernet	Ethernet	3.6.5
Framerelay	Framerelay	3.6.0
MPLS	MPLS	3.6.0
PPP/HDLC	PPP or HDLC	3.6.0
Physical Layer	Physical Layer	3.6.5
MLPPP	MLPPP	3.7.1
BFD	BFD	3.7.1
VPN (IPv6)	VPN	3.7.1

Cisco 7200 Series—Supported Modules

Table 6-44 Supported Modules for Cisco 7200 Series—Cisco Prime Network 3.9

Module Name	Product_Version	Module Description
7201	3.6.4	Cisco 7201 (c7201) processor
ATM WAN OC3+ (MM) /PA-A1	3.6.0	ATM WAN OC3+ (MM) Port adapter, 1 port. Port adapter
C7200-I/O-2FE/E	3.6.0	Cisco 7200 Series 2-Port 10/100 Auto-Sensing Fast Ethernet Input/Output Controller
C7200-I/O-FE	3.6.1	7200 I/O FE Controller.
C7200-I/O-GE+E	3.6.0	Cisco 7200 Series 1-Port Gigabit Ethernet and 1-Port Ethernet Input/Output Controller
C7200-IO	3.6.0	I/O controller with no Ethernet port
C7200-JC-PA	3.6.7	Cisco 7200VXR Series Port Adapter Jacket Card.
CX-FEIP-1FX	3.6.0	1-port fast ethernet interface processor (100TX)
NPE-100	3.6.0	Cisco 7200 Series Network Processing Engine 100
NPE-150	3.6.0	Cisco 7200 Series Network Processing Engine 150
NPE-200	3.6.0	Network Processing Engine NPE-200
NPE-225	3.6.0	Cisco 7200 Network Processing Engine NPE-225
NPE-300	3.6.0	Network Processing Engine NPE-300
NPE-400	3.6.0	Cisco 7200VXR Network Processing Engine NPE-400, including 256 MB SDRAM

Table 6-44 Supported Modules for Cisco 7200 Series—Cisco Prime Network 3.9 (continued)

Module Name	Product_Version	Module Description
NPE-G1	3.6.0	Cisco 7200 Series NPE-G1 including 256 MB default DRAM and 64 MB default flash memory
NPE-G2	3.6.0	Cisco 7200VXR NPE-G2 Network Processing Engine
NPE-G2	3.7	Cisco 7201 Series NPE-G2 Network Processing Engine
NSE-1	3.6.0	Cisco 7200 Series Network Services Engine, NSE-1
PA-2E3	3.7.1.1.1	2 Port E3 Serial Port Adapter with E3 DSUs
PA-2FE-FX	3.7.1.1.1	2-Port Fast Ethernet 100Base FX Port Adapter
PA-2FE-TX	3.6.0	2-Port Fast Ethernet 100Base TX Port Adapter
PA-2H	3.7.1.1.1	2-Port HSSI Port Adapter
PA-2T3/E3-EC	3.6.7	Cisco 2-Port Clear Channel Enhanced Capability Port Adapter
PA-2T3+	3.6.0	Two-port clear-channel DS3 port adap
PA-4E	3.6.0	4-Port 10BaseT Ethernet Port Adapter
PA-4R-DTR	3.6.0	4-port dedicated Token Ring, 4/16 Mbps, half duplex(HDX) or full duplex (FDX)
PA-4T	3.7.1.1.1	4 Port Serial Port Adapter, Enhanced
PA-8E	3.6.0	8-Port 10BaseT Ethernet Port Adapter
PA-8T1	3.6.1	8-port channelized T1
PA-8T-232	3.7.1.1.1	8-Port Serial, 232 Port Adapter
PA-A3-E3	3.6.1	1-Port ATM Enhanced E3 Port Adapter
PA-A3-OC3MM	3.6.0	Single port ATM OC3c/STM1 Multi Mode Port Adapter
PA-A3-OC3SMI	3.6.0	Single port ATM OC3c/STM1 Single Mode (IR) Port Adapter
PA-A3-OC3SML	3.6.0	Single port ATM OC3c/STM1 Single Mode (LR) Port Adapter
PA-A3-T3	3.6.1	1-Port ATM Enhanced DS3 Port Adapter
PA-A6-OC3MM	3.6.1	1 Port Enh ATM OC3c/STM1 Multimode Port Adapter
PA-A6-OC3SMI	3.6.0	1-Port Enhanced ATM OC3c/STM1 Singlemode (IR) Port Adapter
PA-A6-T3	3.6.2	1Port Enh ATM DS3 Port Adapter
PA-CHSTM1	3.6.1	4 port channelized STM-1 card
PA-E3	3.7.1.1.1	1 Port E3 Serial Port Adapter with E3 DSU
PA-FE-FX	3.6.0	1-Port Fast Ethernet 100BaseFx Port Adapter
PA-FE-TX	3.6.0	1-Port Fast Ethernet 100BaseTx Port Adapter
PA-GE	3.6.0	Gigabit Ethernet Port Adapter

Table 6-44 Supported Modules for Cisco 7200 Series—Cisco Prime Network 3.9 (continued)

Module Name	Product_Version	Module Description
PA-H	3.6.1	1-Port HSSI Port Adapter, Spare
PA-ISA	3.7	PA-ISA port adapter card for Cisco 7200 series
PA-MC-2E1/120	3.6.0	2-Port Multichannel E1/PRI Port Adapter
PA-MC-2T	3.6.0	2-port multichannel T1 with integrated channel service units (CSUs)/DSUs
PA-MC-2T	3.6.0	Two-port enhanced multichannel T3 port adapter
PA-MC-2T3-EC	3.6.1	2 port multichannel T3 port adapter
PA-MC-8E1	3.6.0	8-port MultiChannel E1 Port Adapter
PA-MC-8TE1	3.6.0	8 port multichannel T1/E1 8PRI port adapter
PA-MC-8TE1+	3.6.7	8-port multichannel T1/E1 8PRI port adapter
PA-MC-E3	3.6.0	1-port MultiChannel E3 Port Adapter
PA-MC-STM1-SMI	3.6.1	1 port multichannel STM-1 single mode port adapter Spare
PA-MC-T3	3.6.0	Single port enhanced multichannel T3 port adapter
PA-MC-T3-EC	3.6.1	Enhanced 1 port multichannel PA
PA-MCX-4TE1	3.6.0	4 port MIX-enabled multichannel T1/E1 with CSU/DSU
PA-MCX-8TE1	3.6.0	8 port multichannel T1/E1 8PRI port adapter
PA-POS-1OC3	3.6.1	2 Port Packet/SONET OC3c/STM1 Port Adapter
PA-POS-OC3	3.6.4	1-Port Packet/SONET OC3c/STM1 Port Adapter
PA-POS-OC3MM	3.6.0	MultiMode PoS, OC3 Port Adapter
PA-POS-OC3SMI	3.6.0	Single-Mode Intermediate Reach PoS, OC3 Port Adapter
PA-POS-OC3SML	3.6.0	Single-Mode Long Reach PoS, OC3 Port Adapter
PA-T3	3.6.0	One-port clear-channel DS3 port adapter
PA-T3+	3.6.7	1-port T3 Serial Port Adapter Enhanced
PWR-7200-AC	3.6.6	Cisco 7200 AC power supply
PWR-7200-DC	3.6.4	Cisco 7200 DC power supply
SA-VAM	3.6.1	VPN Acceleration Module
SA-VAM2	3.6.2	AES wide key crypto card
SA-VAM2+	3.7	The VPN Acceleration Module 2+ (VAM2+) is a port adapter that installs in any single port-adapter slot on the Cisco 7204VXR or Cisco 7206VXR router with the NPE-225, NPE-400, or NPE-G1 processor, or the Cisco 7301 router.
SFP-GE-L	3.6.7	1000BASE-LX/LH short wavelength; with digital optical monitoring

Table 6-44 Supported Modules for Cisco 7200 Series—Cisco Prime Network 3.9 (continued)

Module Name	Product_Version	Module Description
SFP-GE-S	3.6.7	1000BASE-SX short wavelength; with digital optical monitoring
SFP-OC3-IR1	3.7	OC3 Single Mode Intermediate Reach SFP
VAM2	3.6.2	VPN Acceleration Module 2
VSA	3.6.1	VPN Serivce Adapter
WS-G5484	3.6.1	1000Base-ZX extended reach GBIC(singlemode)
WS-G5486	3.6.1	1000Base-ZX extended reach GBIC(singlemode)
WS-G5487	3.6.1	1000Base-ZX extended reach GBIC(singlemode)
WS-X6582-2PA	3.6.0	Enhanced FlexWAN Module, Fabric-enabled

Cisco 7200 Series—Supported Technologies

The following technologies are supported by the Cisco 7200 Series in Cisco Prime Network 3.9:

- IP, page 6-199
- Routing Protocols, page 6-202
- Ethernet, page 6-205
- ATM, page 6-213
- Frame Relay, page 6-217
- PPP, page 6-219
- HDLC, page 6-220
- SONET/SDH, page 6-220
- TDM/DSx, page 6-222
- MPLS, page 6-226
- MPLS-TE, page 6-228
- VPN (VRF), page 6-233
- PWE3, page 6-235
- Security, page 6-237
- Hardware, page 6-238
- Serial, page 6-242
- Additional Technologies, page 6-243
- LocalSwitching, page 6-245
- BFD, page 6-246
- Carrier Ethernet, page 6-247
- CDP, page 6-249
- Discovery Protocol, page 6-249

- 6PE, page 6-264

Cisco 7200 Series—Supported Service Events

Table 6-45 Supported Service Events for Cisco 7200 Series—Cisco Prime Network 3.9

Event Name	Product_Version	Expedited
Active IP Interfaces Found	3.6.0	Y
All IP Interfaces Down	3.6.0	Y
BGP link down due to admin	3.6.0	Y
BGP link down due to oper	3.6.0	Y
Card Down	3.6.0	Y
Card In	3.6.0	Y
Card Out	3.6.0	Y
Card Up	3.6.0	Y
CPU utilization exceeded upper threshold	3.6.0	N
Device Unsupported	3.6.0	Y
Dropped packet rate exceeded upper threshold	3.6.0	N
DS0 Bundle Admin down	3.7	N
DS0 Bundle Oper down	3.7	N
DS0 Bundle Up	3.7	N
DS1 Path link down due to Admin down	3.7	N
DS1 Path link down due to Oper down	3.7	N
DS1 Path link Up	3.7	N
DS1 Path up	3.7	N
EFP down due to error disabled	3.6.7	N
IMA Administratively down	3.7	N
IMA Operationally down	3.7	N
IMA Operationally up	3.7	N
Keepalive configured	3.7	N
Keepalive not configured	3.7	N
Layer 2 Tunnel Down	3.6.0	N
LDP neighbor down	3.6.0	Y
Link up	3.6.0	N
Memory utilization exceeded upper threshold	3.6.0	N

Table 6-45 Supported Service Events for Cisco 7200 Series—Cisco Prime Network 3.9

Event Name	Product_Version	Expedited
MLPPP Administratively down	3.7	N
MLPPP Operationaly down	3.7	N
MLPPP Up	3.7	N
Module Unsupported		Y
MPLS Black Hole found	3.6.0	N
MPLS interface removed	3.6.0	Y
Pluggable transceiver out	Prime Network 3.8	N
Primary HSRP Interface Active	3.6.0	N
Primary HSRP Interface not Active	3.6.0	N
Rx utilization exceeded upper threshold	3.6.0	N
Secondary HSRP Interface Active	3.6.0	N
Secondary HSRP Interface not Active	3.6.0	N
Sonet Path link down due to Admin down	3.7	N
Sonet Path link down due to Oper down	3.7	N
Sonet Path link Up	3.7	N
SONET Path up	3.7	N
Tx utilization exceeded upper threshold	3.6.0	N
VSI Down	3.6.7	N

Cisco 7300 Series Routers

This section includes the following information about Cisco 7300 Series routers (for information on the NE types supported in Cisco Prime Network 3.9, see Cisco 7300 Series Routers):

- Cisco 7300 Series—Supported Software Versions, page 6-46
- Cisco 7300 Series—Supported Topologies, page 6-48
- Cisco 7300 Series—Supported Modules, page 6-48
- Cisco 7300 Series—Supported Technologies, page 6-48
- Cisco 7300 Series—Supported Service Events, page 6-49

Cisco 7300 Series—Supported Software Versions

Table 6-46 Supported Software Versions for Cisco 7300 Series—Cisco Prime Network 3.9

Software Version	Product_Version
11.3(7)T	3.7
12.0(21)s7	3.7
12.0(22)S5	3.7
12.0(23)S3.0619	3.7
12.0(23)S4	3.7
12.0(23)S6	3.7
12.0(25)S2	3.7
12.0(26)S4	3.7
12.0(26)S5	3.7
12.0(26)S6	3.7
12.0(27)S1	3.7
12.0(32.S7.051907A)	3.7
12.0(33)S1	3.7[1]
12.1(10)E	3.7
12.1(19)E6	3.7
12.1(1a)	3.7
12.2(12)	3.7
12.2(15)B	3.7
12.2(15)T5	3.7
12.2(18)s3	3.7
12.2(18.2)	3.7
12.2(25)s2	3.7
12.2(25)s6	3.7
12.2(25)s9	3.7
12.2(27)SBC2	3.7
12.2(31)SB	3.7
12.2(31)SB11	3.7[2]
12.2(31)SB12	3.7
12.2(31)SB3	3.7
12.2(31)SB3x	3.7
12.2(33)SRA	3.7
12.2(33)SRC	3.7[3]
12.2(33)SRC3	3.7[4]

Table 6-46 Supported Software Versions for Cisco 7300 Series—Cisco Prime Network 3.9

Software Version	Product_Version
12.2(33)SRD1	3.7[5]
12.3(10)	3.7[6]
12.3(10b)	3.7
12.3(10c)	3.7
12.3(10d)	3.7
12.3(12.10)	3.7
12.3(17)	3.7
12.3(17a)	3.7
12.3(20)	3.7
12.3(21)	3.7
12.3(26)	3.7[7]
12.3(6b)	3.7[8]
12.3(6e)	3.7
12.3(6f)	3.7
12.4(20)T	3.7[9]
12.0(32)S	3.7[10]
12.2(34)	3.7[11]
12.3	3.7[12]
12.3(14)	3.7[13]
12.3(15)	3.7[14]
12.4	3.7[15]
12.4(11)T	3.7[16]
12.4(12)	3.7[17]
12.4(20)T1	3.7[18]
15.1(3)S	3.7.X-DP-7.0
15.0(1)M	3.7.X-DP-7.0
15.0(1)M6	3.7.X-DP-7.0
15.0(1)M1	3.7.X-DP-8.0
15.0(1)M2	3.7.X-DP-8.0
15.0(1)M3	3.7.X-DP-8.0
15.0(1)M4	3.7.X-DP-8.0
15.0(1)M5	3.7.X-DP-8.0

[1, 2, 3, 4, 5, 6, 7, 8, 9, 11] ANA models pluggable ports for this IOS version.

[10, 12, 13, 14, 15, 16, 18] ANA supports all maintenance builds in this IOS release train.ANA models pluggable ports for this IOS version.

[17]ANA supports all maintenance builds in this IOS release train.

Cisco 7300 Series—Supported Topologies

Table 6-47 Supported Topologies for Cisco 7300 Series—Cisco Prime Network 3.9

Topology Type	Link Type	Product_Version
Business	Business	3.7
Ethernet	Ethernet	3.6.5
Physical Layer	Physical Layer	3.6.5
VPN (IPv6)	VPN	3.7

Cisco 7300 Series—Supported Modules

Table 6-48 Supported Modules for Cisco 7300 Series—Cisco Prime Network 3.9

Module Name	Product_Version	Module Description
7300-PA-CC	3.7	Carrier card for Cisco 7200 Series port adapters
C7304-MSC100-SPA	3.7	Cisco 7304 SPA Modular Services Carrier Card
CISCO 7301 NETWORK PROCESSOR ENGINE	3.7.2	Cisco 7301 Network Processor Engine
NSE-100	3.7	Cisco 7304 NSE-100 w/512MB SDRAM, 256MB Flsh, (2)GE
NSE-150	3.7	Cisco 7304 NSE-150 with 2 GB SDRAM, 256MB Flash, (4)GE (offered through system bundle only)
SFP-OC3-IR1	3.7	SFP OC-3/STM-1 Intermediate-Reach
SFP-OC3-LR1	3.7	SFP OC-3/STM-1 Long-Reach (40 km)
SFP-OC3-MM	3.7	SFP OC-3/STM-1 Multimode

Cisco 7300 Series—Supported Technologies

The following technologies are supported by the Cisco 7300 Series in Cisco Prime Network 3.9:

- IP, page 6-199
- Routing Protocols, page 6-202
- Ethernet, page 6-205
- ATM, page 6-213
- HDLC, page 6-220
- SONET/SDH, page 6-220
- MPLS, page 6-226

- VPN (VRF), page 6-233
- Security, page 6-237
- Hardware, page 6-238
- Serial, page 6-242
- Carrier Ethernet, page 6-247
- CDP, page 6-249
- Discovery Protocol, page 6-249

Cisco 7300 Series—Supported Service Events

Table 6-49 Supported Service Events for Cisco 7300 Series—Cisco Prime Network 3.9

Event Name	Product_Version	Expedited
Active IP Interfaces Found	3.7	Y
All IP Interfaces Down	3.7	Y
Card Down	3.7	Y
Card In	3.7	Y
Card Out	3.7	Y
Card Up	3.7	Y
Device Unsupported	3.7	Y
Link up	3.7	N
Pluggable transceiver out	Prime Network 3.8	N
Rep port role change	Prime Network 3.8	Y

Cisco 7400 Series Routers

This section includes the following information about Cisco 7400 Series routers (for information on the NE types supported in Cisco Prime Network 3.9, see Cisco 7400 Series Routers):

- Cisco 7400 Series—Supported Software Versions, page 6-50
- Cisco 7400 Series—Supported Topologies, page 6-51
- Cisco 7400 Series—Supported Modules, page 6-51
- Cisco 7400 Series—Supported Technologies, page 6-52
- Cisco 7400 Series—Supported Service Events, page 6-53

Cisco 7400 Series—Supported Software Versions

Table 6-50 Supported Software Versions for Cisco 7400 Series—Cisco Prime Network 3.9

Software Version	Product_Version
IOS 11.3(7)T	3.6.1
IOS 12.0(22)S5	3.6.1
IOS 12.0(23)S3.0619	3.6.1
IOS 12.0(23)S4	3.6.1
IOS 12.0(23)S6	3.6.1
IOS 12.0(23)S6.0412	3.6.1
IOS 12.0(24)S3	3.6.1
IOS 12.0(25)S2	3.6.1
IOS 12.0(26)S4	3.6.1
IOS 12.0(26)S5	3.6.1
IOS 12.0(26)S6	3.6.1
IOS 12.0(27)S1	3.6.1
IOS 12.0(32)S6	3.6.0[1]
IOS 12.0(33)S	3.6.2
IOS 12.0(33)S1	3.6.2[2]
IOS 12.1(10)E	3.6.0
IOS 12.1(19)E6	3.6.0
IOS 12.1(1a)	3.6.0
IOS 12.2(12)	3.6.0
IOS 12.2(15)B	3.6.0
IOS 12.2(15)T5	3.6.0
IOS 12.2(18.2)	3.6.0
IOS 12.2(28)SB	3.6.2
IOS 12.2(31)SB3x	3.6.1
IOS 12.2(33)SRA	3.6.2
IOS 12.2(34)	3.6.0[3]
IOS 12.3(10)	3.6.0[4]
IOS 12.3(12.10)	3.6.0
IOS 12.3(14)	3.6.2[5]
IOS 12.3(15a)	3.6.0
IOS 12.3(3)B1	3.6.0
IOS 12.3(7)XI7a	3.6.0[6]
IOS 12.4(11)T1	3.6.1[7]

[1, 2, 3, 4, 5, 6, 7]ANA models pluggable ports for this IOS version.

Cisco 7400 Series—Supported Topologies

Table 6-51 Supported Topologies for Cisco 7400 Series—Cisco Prime Network 3.9

Topology Type	Link Type	Product_Version
BGP	BGP	3.6.0
Ethernet	Ethernet	3.6.0
Framerelay	Framerelay	3.6.0
MPLS	MPLS	3.6.0
PPP/HDLC	PPP or HDLC	3.6.0
Physical Layer	Physical Layer	3.6.0
LAG	LAG	3.6.0

Cisco 7400 Series—Supported Modules

Table 6-52 Supported Modules for Cisco 7400 Series—Cisco Prime Network 3.9

Module Name	Product_Version	Module Description
PA-2FE-TX	3.6.0	2-Port Fast Ethernet 100Base TX Port Adapter
PA-2T3	3.6.0	Two-port clear-channel DS3 port adap
PA-4E	3.6.0	4-Port 10BaseT Ethernet Port Adapter
PA-4R-DTR	3.6.0	4-port dedicated Token Ring, 4/16 Mbps, half duplex(HDX) or full duplex (FDX)
PA-8E	3.6.0	8-Port 10BaseT Ethernet Port Adapter
PA-A3-OC3MM	3.6.0	Single port ATM OC3c/STM1 Multi Mode Port Adapter
PA-A3-OC3SMI	3.6.0	Single port ATM OC3c/STM1 Single Mode (IR) Port Adapter
PA-A3-OC3SML	3.6.0	Single port ATM OC3c/STM1 Single Mode (LR) Port Adapter
PA-FE-FX	3.6.0	1-Port Fast Ethernet 100BaseFx Port Adapter
PA-FE-TX	3.6.0	1-Port Fast Ethernet 100BaseTx Port Adapter
PA-GE	3.6.0	Gigabit Ethernet Port Adapter
PA-MC-2E1/120	3.6.0	2-Port Multichannel E1/PRI Port Adapter
PA-MC-2T	3.6.0	2-port multichannel T1 with integrated channel service units (CSUs)/DSUs
PA-MC-8E1	3.6.0	8-port MultiChannel E1 Port Adapter

Table 6-52 Supported Modules for Cisco 7400 Series—Cisco Prime Network 3.9 (continued)

Module Name	Product_Version	Module Description
PA-MC-8TE1	3.6.0	8 port multichannel T1/E1 8PRI port adapter
PA-MC-E3	3.6.0	1-port MultiChannel E3 Port Adapter
PA-MC-T3	3.6.0	Single port enhanced multichannel T3 port adapter
PA-POS-OC3MM	3.6.0	MultiMode PoS, OC3 Port Adapter
PA-POS-OC3SMI	3.6.0	Single-Mode Intermediate Reach PoS, OC3 Port Adapter
PA-POS-OC3SML	3.6.0	Single-Mode Long Reach PoS, OC3 Port Adapter
PA-T3	3.6.0	One-port clear-channel DS3 port adapter

Cisco 7400 Series—Supported Technologies

The following technologies are supported by the Cisco 7400 Series in Cisco Prime Network 3.9:

- IP, page 6-199
- Routing Protocols, page 6-202
- Ethernet, page 6-205
- ATM, page 6-213
- Frame Relay, page 6-217
- PPP, page 6-219
- HDLC, page 6-220
- SONET/SDH, page 6-220
- TDM/DSx, page 6-222
- MPLS, page 6-226
- MPLS-TE, page 6-228
- VPN (VRF), page 6-233
- PWE3, page 6-235
- Security, page 6-237
- Hardware, page 6-238
- Serial, page 6-242
- Additional Technologies, page 6-243
- LocalSwitching, page 6-245
- CDP, page 6-249
- Discovery Protocol, page 6-249

Cisco 7400 Series—Supported Service Events

Table 6-53 Supported Service Events for Cisco 7400 Series—Cisco Prime Network 3.9

Event Name	Product_Version	Expedited
Active IP Interfaces Found	3.6.0	Y
All IP Interfaces Down	3.6.0	Y
BGP process up	3.6.0	N
Card Down	3.6.0	Y
Card In	3.6.0	Y
Card Out	3.6.0	Y
Card Up	3.6.0	Y
CPU utilization exceeded upper threshold	3.6.0	N
Device Unsupported	3.6.0	N
Fan-tray down	Prime Network 3.8	N
Fan-tray out	Prime Network 3.8	N
Keepalive configured	3.6.0	N
Keepalive not configured	3.6.0	N
Layer 2 Tunnel Down	3.6.0	N
Link up	3.6.0	N
Memory utilization exceeded upper threshold	3.6.0	N
Module Unsupported	3.6.0	N
Rx utilization exceeded upper threshold	3.6.0	N
Tx utilization exceeded upper threshold	3.6.0	N
Pluggable transceiver out	Prime Network 3.8	N
Power-supply down	Prime Network 3.8	N
Power-supply out	Prime Network 3.8	N

Cisco 7500 Series Routers

This section includes the following information about Cisco 7500 Series routers (for information on the NE types supported in Cisco Prime Network 3.9, see Cisco 7500 Series Routers):

- Cisco 7500 Series—Supported Software Versions, page 6-54
- Cisco 7500 Series—Supported Topologies, page 6-56
- Cisco 7500 Series—Supported Modules, page 6-56
- Cisco 7500 Series—Supported Technologies, page 6-56
- Cisco 7500 Series—Supported Service Events, page 6-57

Cisco 7500 Series—Supported Software Versions

Table 6-54 Supported Software Versions for Cisco 7500 Series—Cisco Prime Network 3.9

Software Version	Product_Version
11.3(7)T	3.7
12.0(20060619:094154)	3.7
12.0(21)s7	3.7
12.0(23)S3.0619	3.7
12.0(23)S4	3.7
12.0(23)S6	3.7
12.0(25)S2	3.7
12.0(26)S4	3.7
12.0(26)S5	3.7
12.0(26)S6	3.7
12.0(27)S1	3.7
12.0(32.S7.051907A)	3.7
12.0(33)S1	3.7[1]
12.1(10)E	3.7
12.1(19)E6	3.7
12.1(1a)	3.7
12.2(12)	3.7
12.2(15)B	3.7
12.2(15)T5	3.7
12.2(18)s3	3.7
12.2(18.2)	3.7
12.2(25)s2	3.7
12.2(25)s6	3.7

Table 6-54 Supported Software Versions for Cisco 7500 Series—Cisco Prime Network 3.9

Software Version	Product_Version
12.2(25)s9	3.7
12.2(27)SBC2	3.7
12.2(31)SB	3.7
12.2(31)SB11	3.7[2]
12.2(31)SB12	3.7
12.2(31)SB3	3.7
12.2(31)SB3x	3.7
12.2(33)SRA	3.7
12.2(33)SRC	3.7[3]
12.2(33)SRC3	3.7[4]
12.2(33)SRD1	3.7[5]
12.3(10)	3.7[6]
12.3(10b)	3.7
12.3(10c)	3.7
12.3(10d)	3.7
12.3(12.10)	3.7
12.3(17)	3.7
12.3(17a)	3.7
12.3(20)	3.7
12.3(21)	3.7
12.3(26)	3.7[7]
12.3(6b)	3.7[8]
12.3(6e)	3.7
12.3(6f)	3.7
12.4(20)T	3.7[9]
12.0(32)S	3.7[10]
12.2(128)SB	3.7
12.2(34)	3.7[11]
12.3	3.7[12]
12.3(14)	3.7[13]
12.3(15)	3.7[14]
12.4	3.7[15]
12.4(11)T	3.7[16]
12.4(12)	3.7

[1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16] ANA models pluggable ports for this IOS version.

Cisco 7500 Series—Supported Topologies

Table 6-55 Supported Topologies for Cisco 7500 Series—Cisco Prime Network 3.9

Topology Type	Link Type	Product_Version
Business	Business	3.7
Ethernet	Ethernet	3.7
Physical Layer	Physical Layer	3.7

Cisco 7500 Series—Supported Modules

Table 6-56 Supported Modules for Cisco 7500 Series—Cisco Prime Network 3.9

Module Name	Product_Version	Module Description
NSE-150	3.7	Cisco 7304 NSE-150 Network Services Engine
NSE-100	3.7	Cisco 7304 NSE-100 Network Services Engine

Cisco 7500 Series—Supported Technologies

The following technologies are supported by the Cisco 7500 Series in Cisco Prime Network 3.9:

- IP, page 6-199
- Routing Protocols, page 6-202
- Ethernet, page 6-205
- ATM, page 6-213
- HDLC, page 6-220
- SONET/SDH, page 6-220
- MPLS, page 6-226
- VPN (VRF), page 6-233
- Security, page 6-237
- Hardware, page 6-238
- Serial, page 6-242
- CDP, page 6-249
- Discovery Protocol, page 6-249

Cisco 7500 Series—Supported Service Events

Table 6-57 Supported Service Events for Cisco 7500 Series—Cisco Prime Network 3.9

Event Name	Product_Version	Expedited
Active IP Interfaces Found	3.7	Y
All IP Interfaces Down	3.7	Y
Card Down	3.7	Y
Card In	3.7	Y
Card Out	3.7	Y
Card Up	3.7	Y
Device Unsupported	3.7	N
Fan-tray down	Prime Network 3.8	N
Fan-tray out	Prime Network 3.8	N
Link up	3.7	N
Pluggable transceiver out	Prime Network 3.8	N
Power-supply down	Prime Network 3.8	N
Power-supply out	Prime Network 3.8	N

Cisco 7600 Series Routers

This section includes the following information about Cisco 7600 Series routers (for information on the NE types supported in Cisco Prime Network 3.9, see Cisco 7600 Series Routers):

- Cisco 7600 Series—Supported Software Versions, page 6-58
- Cisco 7600 Series—Supported Topologies, page 6-60
- Cisco 7600 Series—Supported Modules, page 6-61
- Cisco 7600 Series—Supported Technologies, page 6-77
- Cisco 7600 Series—Supported Service Events, page 6-78

Cisco 7600 Series—Supported Software Versions

Table 6-58 Supported Software Versions for Cisco 7600 Series—Cisco Prime Network 3.9

Software Version	Product_Version
IOS 12.1(13)E6	3.6.1
IOS 12.1(20)E3	3.6.1
IOS 12.2(18)SXD	3.6.0
IOS 12.2(18)SXD2	3.6.1
IOS 12.2(18)SXD5	3.6.0
IOS 12.2(18)SXE	3.6.0[1]
IOS 12.2(18)SXE6b	3.6.0
IOS 12.2(18)SXF	3.6.0
IOS 12.2(18)SXF7	3.6.2[2]
IOS 12.2(33)SRA	3.6.0[3]
IOS 12.2(33)SRA2	3.6.0
IOS 12.2(33)SRA6	3.6.3[4]
IOS 12.2(33)SRB	3.6.0[5]
IOS 12.2(33)SRB1	3.6.1[6]
IOS 12.2(33)SRB2	3.6.2
IOS 12.2(33)SRB3	3.6.3[7]
IOS 12.2(33)SRB4	3.6.4[8]
IOS 12.2(33)SRB5	3.7.0.1
IOS 12.2(33)SRB6	3.7.0.1
IOS 12.2(33)SRC	3.6.2[9]
IOS 12.2(33)SRC1	3.6.3[10]
IOS 12.2(33)SRC2	3.6.4[11]
IOS 12.2(33)SRC3	3.6.7[12]
IOS 12.2(33)SRC4	3.7[13]
IOS 12.2(33)SRC5	3.7.0.1
IOS 12.2(33)SRC6	3.7.1
IOS 12.2(33)SRD1	3.6.4[14]
IOS 12.2(33)SRD2	3.6.6[15]
IOS 12.2(33)SRD2a	3.7.0.1
IOS 12.2(33)SRD3	3.7[16]
IOS 12.2(33)SRD4	3.7.0.1
IOS 12.2(33)SRE	3.7[17]
IOS 12.2(33)SRE0a	3.7.0.1

Table 6-58 Supported Software Versions for Cisco 7600 Series—Cisco Prime Network 3.9

Software Version	Product_Version
IOS 12.2(33)SRE1	3.7.0.1
IOS 12.2(33)SXH2a	3.6.5[18]
IOS 15.0(1)S	3.7.1
IOS 15.1(1)S	3.7.2
IOS 12.2(33)SRD5	3.7.1.1.0
IOS 12.2(33)SRE2	3.7.1.1.0
IOS 15.0(1)S1	3.7.2
IOS 15.0(1)S2	3.7.2
IOS 12.2(33)SRE3	3.7.2
IOS 12.2(33)SRD6	ANA-3.7.2-DP1
IOS 15.1(1)S1	ANA-3.7.2-DP1
IOS 12.2(18)SXF11	ANA-3.7.2-DP1
IOS 15.1(2)S	ANA-3.7.2-DP2
IOS 15.0(1)S3	ANA-3.7.2-DP2
IOS 15.1(1)S2	ANA-3.7.2-DP3
IOS 12.2(33)SRE4	ANA-3.7.2-DP4
IOS 15.1(2)S1	ANA-3.7.3-DP5
IOS 15.1(3)S	ANA-3.7.3-DP6
IOS 15.0(1)S4	ANA-3.7.3-DP6
IOS 15.1(2)S2	ANA-3.7.3-DP7
IOS 12.2(33)SRD7	ANA-3.7.3-DP9
IOS 15.1(3)S1	ANA-3.7.3-DP9
IOS 15.2(1)S	Cisco-ANA-3.7.x-DP10, Cisco-ANA-3.8-DP1

Table 6-58 Supported Software Versions for Cisco 7600 Series—Cisco Prime Network 3.9

Software Version	Product_Version
IOS 12.2(33)SRE5	Cisco-ANA-3.7.x-DP10, Cisco-ANA-3.8-DP1
IOS 15.1(3)S2	Cisco-ANA-3.7.x-DP10, Cisco-ANA-3.8-DP1
IOS 15.0(1)S5	Cisco-ANA-3.7.x-DP11, Cisco-ANA-3.8-DP2
IOS 12.2(33)SRE6	Cisco-ANA-3.7.x-DP13, Cisco-ANA-3.8-DP4
IOS 12.2(33)SRD8	Cisco-ANA-3.7.x-DP14, Cisco-ANA-3.8-DP5
IOS 15.1(3)S3	Cisco-ANA-3.7.x-DP14, Cisco-ANA-3.8-DP5
IOS 15.2(1)S1	Cisco-ANA-3.7.x-DP14, Cisco-ANA-3.8-DP5

[1, 2, 3, 4, 7, 8, 10, 11, 12, 13, 15, 16, 18]ANA models pluggable ports for this IOS version.

[5]12.2(33)SRB is not supported on Cisco 7603-S and Cisco 7609-S, as both devices provide incorrect sysoids.ANA models pluggable ports for this IOS version.

[6]12.2(33)SRB1 is not supported on Cisco 7603-S and Cisco 7609-S, as both devices provide incorrect sysoids.

[9, 14, 17]ANA recognizes all maintenance builds in this IOS release train.ANA models pluggable ports for this IOS version.

Cisco 7600 Series—Supported Topologies

Table 6-59 Supported Topologies for Cisco 7600 Series—Cisco Prime Network 3.9

Topology Type	Link Type	Product_Version
ATM	ATM	3.6.0

Table 6-59 Supported Topologies for Cisco 7600 Series—Cisco Prime Network 3.9 (continued)

Topology Type	Link Type	Product_Version
BGP	BGP	3.6.0
Ethernet	Ethernet	3.6.0
Framerelay	Framerelay	3.6.0
MPLS	MPLS	3.6.0
PPP/HDLC	PPP or HDLC	3.6.0
Physical Layer	Physical Layer	3.6.0
LAG	LAG	3.6.0
MLPPP	MLPPP	3.7.1
BFD	BFD	3.7.1
VPN (IPv6)	VPN	3.7.1
MPLS-TP	Tunnel	Prime Network 3.8

Cisco 7600 Series—Supported Modules

Table 6-60 Supported Modules for Cisco 7600 Series—Cisco Prime Network 3.9

Module Name	Product_Version	Module Description
4000W-DC	3.6.2	4000W DC PS for 7609/7613Chassis
6000W-DC	3.6.2	6000W DC PS
7600-ES+20C3C	3.7	20G Combo Link Daughter Card (not a FRU)
7600-ES+20G	3.6.6	7600 ES+ 20x1G Link DC
7600-ES+20G3C	3.6.6	7600 ES+ Line Card, 20xGE SFP with DFC 3C
7600-ES+20G3CXL	3.6.6	7600 ES+ Line Card, 20xGE SFP with DFC 3CXL
7600-ES+2TG	3.6.6	7600 ES+ 2x10G Link DC
7600-ES+2TG3C	3.6.6	7600 ES+ Line Card, 2x10GE XFP with DFC 3C
7600-ES+2TG3CXL	3.6.6	7600 ES+ Line Card, 2x10GE XFP with DFC 3CXL
7600-ES+3C	3.6.6	7600 ES+ Policy Forwarding 3C DC
7600-ES+3CXL	3.6.6	7600 ES+ Policy Forwarding 3CXL DC
7600-ES+40C3C	3.7	40G Combo Link Daughter Card (not a FRU)
7600-ES+40G	3.6.6	7600 ES+ 40x1G Link DC
7600-ES+40G3C	3.6.6	7600 ES+ Line Card, 40xGE SFP with DFC 3C
7600-ES+40G3CXL	3.6.4	7600 ES+ Line Card, 40xGE SFP with DFC 3CXL
7600-ES+4TG	3.6.6	7600 ES+ 4x10G Link DC
7600-ES+4TG3C	3.6.6	7600 ES+ Line Card, 4x10GE XFP with DFC 3C

Table 6-60 Supported Modules for Cisco 7600 Series—Cisco Prime Network 3.9 (continued)

Module Name	Product_Version	Module Description
7600-ES+4TG3CXL	3.6.6	7600 ES+ Line Card, 4x10GE XFP with DFC 3CXL
7600-ES20	3.6.1	Cisco 7600 Series Ethernet Services Card
7600-ES20-10G3C	3.6.1	Cisco 7600 ES20 line card, 2x10GE XFP with DFC 3C
7600-ES20-10G3CXL	3.6.1	Cisco 7600 ES20 line card, 2x10GE XFP with DFC 3CXL
7600-ES20-GE3C	3.6.1	Cisco 7600 ES20 line card, 20xGE SFP with DFC 3C
7600-ES20-GE3CXL	3.6.1	Cisco 7600 ES20 line card, 20xGE SFP with DFC 3CXL
7600-ES20-PROC	3.6.1	7600 ES20 PROC FRU
7600-MSFC4	3.6.1	c7600 MSFC4 Daughterboard
7600-PFC3C	3.6.5	RSP720 Policy Feature Card 3C
7600-SIP-200	3.6.0	SPA Interface Processor-200
7600-SIP-400	3.6.0	SPA Interface Processor-400
7600-SIP-600	3.6.0	SPA Interface Processor-600
7600-SSC-400	3.6.3	Cisco 7600 / Catalyst 6500 Services SPA Carrier Card-400 Rev. 2.0
76-ES+T-20G	3.7.1	7600 ES+T Fixed 20x1G Low Queue Transport 3CXL
76-ES+T-20GQ	3.7.1	7600 ES+T 20x1G Low Queue Transport Link Daughter Card
76-ES+T-2TG	3.7.1	7600 ES+T Fixed OTN/DWDM+FEC 2x10GE 3C XL Low Queue Transport 3CXL
76-ES+T-2TGQ	3.7.1	7600 ES+T OTN/DWDM+FEC 2x10GE 3C XL Low Queue Transport Link Daughter card
76-ES+T-40G	3.7.1	7600 ES+T Fixed 40x1G Low Queue Transport 3CXL
76-ES+T-40GQ	3.7.1	7600 ES+T 40x1G Low Queue Transport Link Daughter Card
76-ES+T-4TG	3.7.1	7600 ES+T Fixed OTN/DWDM+FEC 4x10GE 3C XL Low Queue Transport 3CXL
76-ES+T-4TGQ	3.7.1	7600 ES+T OTN/DWDM+FEC 4x10GE 3C XL Low Queue Transport Link Daughter card
76-ES+XC-20G3C	3.7	7600 ES+XC Combo 10x1GE/ 1x10GE, DFC3CXL
76-ES+XC-20G3CXL	3.7	7600 ES+XC Combo 10x1GE/ 1x10GE, DFC3CXL
76-ES+XC-40G3C	3.7	Combo 20x1GE/2x10GE - 3C
76-ES+XC-40G3CXL	3.7	Combo 20x1GE/2x10GE - 3CXL
76-ES+XT-2TG3C	3.7	7600 ES+XT, LAN/WAN PHY, OTN/G.709, 2x10GE, XFP, DFC3C
76-ES+XT-2TG3CXL	3.7	7600 ES+XT, LAN/WAN PHY, OTN/G.709, 2x10GE, XFP, DFC3CXL

Table 6-60 Supported Modules for Cisco 7600 Series—Cisco Prime Network 3.9 (continued)

Module Name	Product_Version	Module Description
76-ES+XT-4TG3C	3.7	7600 ES+XT, LAN/WAN PHY, OTN/G.709, 4x10GE, XFP, DFC3C
76-ES+XT-4TG3CXL	3.7	7600 ES+XT, LAN/WAN PHY, OTN/G.709, 4x10GE, XFP, DFC3CXL
ACE10-6500-K9	3.7	Cisco Application Control Engine Service Module
CEVFAN	3.6.1	Fan
CLK-7600	3.7	Cisco 7600 Clock Module
CWDM-SFP-1470	3.7	CWDM SFP 1470 nm, Gigabit Ethernet and 1G/2G FC
CWDM-SFP-1490	3.7	CWDM SFP 1490 nm, Gigabit Ethernet and 1G/2G FC
CWDM-SFP-1510	3.7	CWDM SFP 1510 nm, Gigabit Ethernet and 1G/2G FC
CWDM-SFP-1530	3.7	CWDM SFP 1530 nm, Gigabit Ethernet and 1G/2G FC
CWDM-SFP-1550	3.7	CWDM SFP 1550 nm, Gigabit Ethernet and 1G/2G FC
CWDM-SFP-1570	3.7	CWDM SFP 1570 nm, Gigabit Ethernet and 1G/2G FC
CWDM-SFP-1590	3.7	CWDM SFP 1590 nm, Gigabit Ethernet and 1G/2G FC
CWDM-SFP-1610	3.7	CWDM SFP 1610 nm, Gigabit Ethernet and 1G/2G FC
DFC-3C	3.6.1	Distributed Forwarding Card 3C
DWDM-SFP-3033	3.6.7	Cisco 1000BASE-DWDM SFP 1530.33 nm
DWDM-SFP-3112	3.6.7	Cisco 1000BASE-DWDM SFP 1531.12 nm
DWDM-SFP-3190	3.6.7	Cisco 1000BASE-DWDM SFP 1531.90 nm
DWDM-SFP-3268	3.6.7	Cisco 1000BASE-DWDM SFP 1532.68 nm
DWDM-SFP-3346	3.7.2	Cisco 1000BASE-DWDM SFP 1533.46 nm
DWDM-SFP-3425	3.6.7	Cisco 1000BASE-DWDM SFP 1534.25 nm
DWDM-SFP-3504	3.6.7	Cisco 1000BASE-DWDM SFP 1535.04 nm
DWDM-SFP-3582	3.6.7	Cisco 1000BASE-DWDM SFP 1535.82 nm
DWDM-SFP-3661	3.6.7	Cisco 1000BASE-DWDM SFP 1536.61 nm
DWDM-SFP-3739	3.7.2	Cisco 1000BASE-DWDM SFP 1537.39 nm
DWDM-SFP-3819	3.6.7	Cisco 1000BASE-DWDM SFP 1538.19 nm
DWDM-SFP-3898	3.6.7	Cisco 1000BASE-DWDM SFP 1539.98 nm
DWDM-SFP-3977	3.6.7	Cisco 1000BASE-DWDM SFP 1539.77 nm
DWDM-SFP-4056	3.6.7	Cisco 1000BASE-DWDM SFP 1540.56 nm

Table 6-60 Supported Modules for Cisco 7600 Series—Cisco Prime Network 3.9 (continued)

Module Name	Product_Version	Module Description
DWDM-SFP-4134	3.7.2	Cisco 1000BASE-DWDM SFP 1541.34 nm
DWDM-SFP-4214	3.6.7	Cisco 1000BASE-DWDM SFP 1542.14 nm
DWDM-SFP-4294	3.6.7	Cisco 1000BASE-DWDM SFP 1542.94 nm
DWDM-SFP-4373	3.6.7	Cisco 1000BASE-DWDM SFP 1543.73 nm
DWDM-SFP-4453	3.6.7	Cisco 1000BASE-DWDM SFP 1544.53 nm
DWDM-SFP-4532	3.7.2	Cisco 1000BASE-DWDM SFP 1545.32 nm
DWDM-SFP-4612	3.6.7	Cisco 1000BASE-DWDM SFP 1546.12 nm
DWDM-SFP-4692	3.6.7	Cisco 1000BASE-DWDM SFP 1546.92 nm
DWDM-SFP-4772	3.6.7	Cisco 1000BASE-DWDM SFP 1547.72 nm
DWDM-SFP-4851	3.6.7	Cisco 1000BASE-DWDM SFP 1548.51 nm
DWDM-SFP-4931	3.7.2	Cisco 1000BASE-DWDM SFP 1549.31 nm
DWDM-SFP-5012	3.6.7	Cisco 1000BASE-DWDM SFP 1550.12 nm
DWDM-SFP-5092	3.6.7	Cisco 1000BASE-DWDM SFP 1550.92 nm
DWDM-SFP-5172	3.6.7	Cisco 1000BASE-DWDM SFP 1551.72 nm
DWDM-SFP-5252	3.6.7	Cisco 1000BASE-DWDM SFP 1552.52 nm
DWDM-SFP-5332	3.7.2	Cisco 1000BASE-DWDM SFP 1553.32 nm
DWDM-SFP-5413	3.6.7	Cisco 1000BASE-DWDM SFP 1554.13 nm
DWDM-SFP-5494	3.6.7	Cisco 1000BASE-DWDM SFP 1554.94 nm
DWDM-SFP-5575	3.6.7	Cisco 1000BASE-DWDM SFP 1555.75 nm
DWDM-SFP-5655	3.6.7	Cisco 1000BASE-DWDM SFP 1556.55 nm
DWDM-SFP-5736	3.7.2	Cisco 1000BASE-DWDM SFP 1557.36 nm
DWDM-SFP-5817	3.6.7	Cisco 1000BASE-DWDM SFP 1558.17 nm
DWDM-SFP-5898	3.6.7	Cisco 1000BASE-DWDM SFP 1558.98 nm
DWDM-SFP-5979	3.6.7	Cisco 1000BASE-DWDM SFP 1559.79 nm
DWDM-SFP-6061	3.6.7	Cisco 1000BASE-DWDM SFP 1560.61 nm
DWDM-SFP-6141	3.7.2	Cisco 1000BASE-DWDM SFP 1561.41 nm
DWDM-XENPAK-30.33	3.6.7	10GBASE-DWDM 1530.33 nm XENPAK (100-GHz ITU grid)
DWDM-XENPAK-31.12	3.6.7	10GBASE-DWDM 1531.12 nm XENPAK (100-GHz ITU grid)
DWDM-XENPAK-31.90	3.6.7	10GBASE-DWDM 1531.90 nm XENPAK (100-GHz ITU grid)
DWDM-XENPAK-32.68	3.6.7	10GBASE-DWDM 1532.68 nm XENPAK (100-GHz ITU grid)
DWDM-XENPAK-34.25	3.6.7	10GBASE-DWDM 1534.25 nm XENPAK (100-GHz ITU grid)

Table 6-60 Supported Modules for Cisco 7600 Series—Cisco Prime Network 3.9 (continued)

Module Name	Product_Version	Module Description
DWDM-XENPAK-35.04	3.6.7	10GBASE-DWDM 1535.04 nm XENPAK (100-GHz ITU grid)
DWDM-XENPAK-35.82	3.6.7	10GBASE-DWDM 1535.82 nm XENPAK (100-GHz ITU grid)
DWDM-XENPAK-36.61	3.6.7	10GBASE-DWDM 1536.61 nm XENPAK (100-GHz ITU grid)
DWDM-XENPAK-38.19	3.6.7	10GBASE-DWDM 1538.19 nm XENPAK (100-GHz ITU grid)
DWDM-XENPAK-38.98	3.6.7	10GBASE-DWDM 1538.98 nm XENPAK (100-GHz ITU grid)
DWDM-XENPAK-39.77	3.6.7	10GBASE-DWDM 1539.77 nm XENPAK (100-GHz ITU grid)
DWDM-XENPAK-40.56	3.6.7	10GBASE-DWDM 1540.56 nm XENPAK (100-GHz ITU grid)
DWDM-XENPAK-42.14	3.6.7	10GBASE-DWDM 1542.14 nm XENPAK (100-GHz ITU grid)
DWDM-XENPAK-42.94	3.6.7	10GBASE-DWDM 1542.94 nm XENPAK (100-GHz ITU grid)
DWDM-XENPAK-43.73	3.6.7	10GBASE-DWDM 1543.73 nm XENPAK (100-GHz ITU grid)
DWDM-XENPAK-44.53	3.6.7	10GBASE-DWDM 1544.53 nm XENPAK (100-GHz ITU grid)
DWDM-XENPAK-46.12	3.6.7	10GBASE-DWDM 1546.12 nm XENPAK (100-GHz ITU grid)
DWDM-XENPAK-46.92	3.6.7	10GBASE-DWDM 1546.92 nm XENPAK (100-GHz ITU grid)
DWDM-XENPAK-47.72	3.6.7	10GBASE-DWDM 1547.72 nm XENPAK (100-GHz ITU grid)
DWDM-XENPAK-48.51	3.6.7	10GBASE-DWDM 1548.51 nm XENPAK (100-GHz ITU grid)
DWDM-XENPAK-50.12	3.6.7	10GBASE-DWDM 1550.12 nm XENPAK (100-GHz ITU grid)
DWDM-XENPAK-50.92	3.6.7	10GBASE-DWDM 1550.92 nm XENPAK (100-GHz ITU grid)
DWDM-XENPAK-51.72	3.6.7	10GBASE-DWDM 1551.72 nm XENPAK (100-GHz ITU grid)
DWDM-XENPAK-52.52	3.6.7	10GBASE-DWDM 1552.52 nm XENPAK (100-GHz ITU grid)
DWDM-XENPAK-54.13	3.6.7	10GBASE-DWDM 1554.13 nm XENPAK (100-GHz ITU grid)

Table 6-60 Supported Modules for Cisco 7600 Series—Cisco Prime Network 3.9 (continued)

Module Name	Product_Version	Module Description
DWDM-XENPAK-54.94	3.6.7	10GBASE-DWDM 1554.94 nm XENPAK (100-GHz ITU grid)
DWDM-XENPAK-55.75	3.6.7	10GBASE-DWDM 1555.75 nm XENPAK (100-GHz ITU grid)
DWDM-XENPAK-56.55	3.6.7	10GBASE-DWDM 1556.55 nm XENPAK (100-GHz ITU grid)
DWDM-XENPAK-58.17	3.6.7	10GBASE-DWDM 1558.17 nm XENPAK (100-GHz ITU grid)
DWDM-XENPAK-58.98	3.6.7	10GBASE-DWDM 1558.98 nm XENPAK (100-GHz ITU grid)
DWDM-XENPAK-59.79	3.6.7	10GBASE-DWDM 1559.79 nm XENPAK (100-GHz ITU grid)
DWDM-XENPAK-60.61	3.6.7	10GBASE-DWDM 1560.61 nm XENPAK (100-GHz ITU grid)
DWDM-XFP-30.33	3.6.7[1]	10GBASE-DWDM 1530.33 nm XFP (100-GHz ITU grid)
DWDM-XFP-31.12	3.6.7[2]	10GBASE-DWDM 1531.12 nm XFP (100-GHz ITU grid)
DWDM-XFP-31.90	3.6.7[3]	10GBASE-DWDM 1531.90 nm XFP (100-GHz ITU grid)
DWDM-XFP-32.68	3.6.7[4]	10GBASE-DWDM 1532.68 nm XFP (100-GHz ITU grid)
DWDM-XFP-34.25	3.6.7[5]	10GBASE-DWDM 1534.25 nm XFP (100-GHz ITU grid)
DWDM-XFP-35.04	3.6.7[6]	10GBASE-DWDM 1535.04 nm XFP (100-GHz ITU grid)
DWDM-XFP-35.82	3.6.7[7]	10GBASE-DWDM 1535.82 nm XFP (100-GHz ITU grid)
DWDM-XFP-36.61	3.6.7[8]	10GBASE-DWDM 1536.61 nm XFP (100-GHz ITU grid)
DWDM-XFP-38.19	3.6.7[9]	10GBASE-DWDM 1538.19 nm XFP (100-GHz ITU grid)
DWDM-XFP-38.98	3.6.7[10]	10GBASE-DWDM 1538.98 nm XFP (100-GHz ITU grid)
DWDM-XFP-39.77	3.6.7[11]	10GBASE-DWDM 1539.77 nm XFP (100-GHz ITU grid)
DWDM-XFP-40.56	3.6.7[12]	10GBASE-DWDM 1540.56 nm XFP (100-GHz ITU grid)
DWDM-XFP-42.14	3.6.7[13]	10GBASE-DWDM 1542.14 nm XFP (100-GHz ITU grid)

Table 6-60 Supported Modules for Cisco 7600 Series—Cisco Prime Network 3.9 (continued)

Module Name	Product_Version	Module Description
DWDM-XFP-42.94	3.6.7[14]	10GBASE-DWDM 1542.94 nm XFP (100-GHz ITU grid)
DWDM-XFP-43.73	3.6.7[15]	10GBASE-DWDM 1543.73 nm XFP (100-GHz ITU grid)
DWDM-XFP-44.53	3.6.7[16]	10GBASE-DWDM 1544.53 nm XFP (100-GHz ITU grid)
DWDM-XFP-46.12	3.6.7[17]	10GBASE-DWDM 1546.12 nm XFP (100-GHz ITU grid)
DWDM-XFP-46.92	3.6.7[18]	10GBASE-DWDM 1546.92 nm XFP (100-GHz ITU grid)
DWDM-XFP-47.72	3.6.7[19]	10GBASE-DWDM 1547.72 nm XFP (100-GHz ITU grid)
DWDM-XFP-48.51	3.6.7[20]	10GBASE-DWDM 1548.51 nm XFP (100-GHz ITU grid)
DWDM-XFP-50.12	3.6.7[21]	10GBASE-DWDM 1550.12 nm XFP (100-GHz ITU grid)
DWDM-XFP-50.92	3.6.7[22]	10GBASE-DWDM 1550.92 nm XFP (100-GHz ITU grid)
DWDM-XFP-51.72	3.6.7[23]	10GBASE-DWDM 1551.72 nm XFP (100-GHz ITU grid)
DWDM-XFP-52.52	3.6.7[24]	10GBASE-DWDM 1552.52 nm XFP (100-GHz ITU grid)
DWDM-XFP-54.13	3.6.7[25]	10GBASE-DWDM 1554.13 nm XFP (100-GHz ITU grid)
DWDM-XFP-54.94	3.6.7[26]	10GBASE-DWDM 1554.94 nm XFP (100-GHz ITU grid)
DWDM-XFP-55.75	3.6.7[27]	10GBASE-DWDM 1555.75 nm XFP (100-GHz ITU grid)
DWDM-XFP-56.55	3.6.7[28]	10GBASE-DWDM 1556.55 nm XFP (100-GHz ITU grid)
DWDM-XFP-58.17	3.6.7[29]	10GBASE-DWDM 1558.17 nm XFP (100-GHz ITU grid)
DWDM-XFP-58.98	3.6.7[30]	10GBASE-DWDM 1558.98 nm XFP (100-GHz ITU grid)
DWDM-XFP-59.79	3.6.7[31]	10GBASE-DWDM 1559.79 nm XFP (100-GHz ITU grid)
DWDM-XFP-60.61	3.6.7[32]	10GBASE-DWDM 1560.61 nm XFP (100-GHz ITU grid)
DWDM-XFP-C	3.7.2	Tunable DWDM XFP
FAN-MOD-3SHS	3.7	Spare High-speed fan module for Cisco 7603-S Chassis

Table 6-60 Supported Modules for Cisco 7600 Series—Cisco Prime Network 3.9 (continued)

Module Name	Product_Version	Module Description
FAN-MOD-4HS	3.7	High-speed fan module
FAN-MOD-6HS	3.7	High Speed Fan Module for CISCO7606 Chassis
FAN-MOD-6SHS	3.7	High Speed Fan Module for CISCO7606-S Chassis
FAN-MOD-9	3.7	High-speed fan module
FAN-MOD-9SHS	3.6.4	High-speed fan module
GLC-BX-D	3.6.6	1000BASE-BX10 SFP module for single-strand SMF, 1490-nm TX/1310-nm RX wavelength
GLC-BX-U	3.6.6	1000BASE-BX10 SFP module for single-strand SMF, 1310-nm TX/1490-nm RX wavelength
GLC-GE-100FX	3.7.1.1.0	Cisco 100Base-FX SFP Module, LC Connector
GLC-LH-SM	3.6.4	Short Wave fiber Gigabit Ethernet
GLC-SX-MM	3.7	1000BASE-SX SFP transceiver module for MMF, 850-nm wavelength
GLC-T	3.6.7	1000Base-T SFP Transceiver module for Category 5 copper wire
GLC-ZX-SM	3.6.7	1000BASE-ZX SFP transceiver module for SMF, 1550-nm wavelength
MSFC4	3.6.2	Multilayer Switch Feature Card
ONS-SC-155-EL	3.7.2	STM-1E
OSM-12CT3T1	3.6.0	12-port channelized/unchannelized CT3-T1
OSM-1CHOC12T3-SI	3.6.0	1-port channelized OC-12, SM-IR
OSM-1OC48-POS-SI+	3.6.0	Enhanced 1-port OC-48/STM-16 SONET/SDH OSM, SM-IR
OSM-1OC48-POS-SL+	3.6.0	Enhanced 1-port OC-48/STM-16 SONET/SDH OSM, SM-LR
OSM-1OC48-POS-SS+	3.6.0	Enhanced 1-port OC-48/STM-16 SONET/SDH OSM, SM-SR
OSM-2+4GE-WAN+	3.6.0	4-port Gigabit Ethernet WAN (GBIC) with two Layer 2 LAN ports; CEF256
OSM-2OC12-ATM-MM+	3.6.0	Enhanced 2-port OC-12/STM-4 ATM OSM, MM
OSM-2OC12-ATM-SI+	3.6.0	Enhanced 2-port OC-12/STM-4 ATM OSM, SM-IR
OSM-2OC12-POS-SI+	3.6.0	Enhanced 2-port OC-12c/STM-4c POS, SM-IR; CEF256
OSM-4OC12-POS-SI+	3.6.0	Enhanced 4-port OC-12c/STM-4c POS, SM-IR; CEF256
OSM-4OC3-POS-SI+	3.6.0	Enhanced 4-port OC-3c/STM-1c POS, SM-IR;
PA-1FE-TX, -FX	3.6.0	1-port Fast Ethernet port adapter
PA-2CE/PRI	3.6.1	Not Found

Table 6-60 Supported Modules for Cisco 7600 Series—Cisco Prime Network 3.9 (continued)

Module Name	Product_Version	Module Description
PA-2FE-TX, -FX	3.6.0	2-port Fast Ethernet port adapter
PA-4T+	3.6.0	T1/E1 port adapters
PA-A3-E3	3.6.0	ATM with traffic shaping port adapters
PA-A3-T3	3.6.0	ATM with traffic shaping port adapters
PA-MC-2E1/120	3.6.1	2 port multichannel E1 port adapter with G.703 120ohm interf
PA-MC-4T1	3.6.0	T1/E1 port adapters
PA-MC-8T1	3.6.0	T1/E1 port adapters
PA-MC-8TE1	3.6.1	8 port multichannel T1/E1 8PRI port adapter
PA-MC-STM-1	3.6.0	Multichannel STM-1 port adapters
PA-POS-2OC3	3.6.0	2-port POS OC3c/STM1 port adapter
PFC-3C	3.6.2	Policy Feature Card 3C
PFC-3CXL	3.6.1	Policy Feature Card 3Cxl (PFC3CXL)
PWR-1900-DC	3.7	1900W DC power supply for CISCO7606
PWR-2700-AC	3.6.3	2700W DC power supply
PWR-2700-DC	3.6.2	2700W DC power supply for CISCO7606
PWR-2700-DC/4	3.6.2	2700W DC Power Supply for Cisco 7604
PWR-4500-DC	3.7	7606-S 4500W DC power supply
PWR-6000-DC	3.6.4	6000W DC Power Supply
RSP720-3C-10GE	3.7	Cisco 7600 Series RSP 720-10GE with 10 Gigabit Ethernet Uplinks that includes PFC-3C and Multilayer Switch Feature Card (MSFC4)
RSP720-3C-GE	3.6.1	Route Switch Processor 720 with PFC3C
RSP720-3CXL	3.6.4	Catalyst 6500 Supervisor Module 720 base board
RSP720-3CXL-10GE	3.7	Cisco 7600 Series RSP 720-10GE with 10 Gigabit Ethernet Uplinks that includes PFC-3CXL and Multilayer Switch Feature Card (MSFC4)
RSP720-3CXL-GE	3.6.1	Cisco 7600 Route Switch Processor 72Gbps fabric, PFC3CXL, GE
SFP-GE-L	3.6.4	1000BASE-LH/LX pluggable transceiver
SFP-GE-S	3.6.6	1000BASE-Sx Short wavelength gigabit ethernet SFP.
SFP-GE-T	3.6.6	1000BASE-T copper gigabit ethernet SFP.
SFP-GE-Z	3.6.6	1000BASE-Zx Extended reach gigabit ethernet SFP.
SFP-OC12-IR1	3.6.6	OC-12/STM-4 pluggable intermediate-reach (15 km) transceiver module, 1310-nm wavelength

Table 6-60 Supported Modules for Cisco 7600 Series—Cisco Prime Network 3.9 (continued)

Module Name	Product_Version	Module Description
SFP-OC12-LR1	3.6.6	OC-12/STM-4 pluggable long-reach (40 km) transceiver module, 1310-nm wavelength, LC connector
SFP-OC12-LR2	3.6.6	OC-12/STM-4 pluggable long-reach (80 km) transceiver module, 1550-nm wavelength, LC connector
SFP-OC12-MM	3.6.6	OC-12/STM-4 pluggable short-reach (2 km) transceiver module, 1310-nm wavelength, MMF, LC connector
SFP-OC12-SR	3.6.6	OC-12/STM-4 pluggable short-reach (2 km) transceiver module, 1310-nm wavelength, LC connector
SFP-OC3-IR1	3.6.0	Intermediate range, single-mode fiber
SFP-OC3-LR1	3.6.0	Long range, single-mode fiber
SFP-OC3-LR2	3.6.7	OC-3/STM-1 pluggable long-reach (80 km) transceiver module, 1550-nm wavelength, LC connector
SFP-OC3-MM	3.6.0	Short range, multimode fiber
SFP-OC3-SR	3.6.1	OC3/STM1 SFP, Single-mode fiber, Short Reach
SFP-OC48-IR1	3.6.7	OC-48c/STM-16c
SPA-10X1GE	3.6.0	10-port Gigabit Ethernet SPA, SFP Optics
SPA-10X1GE-V2	3.6.0	10-port Gigabit Ethernet SPA, SFP Optics
SPA-1CHOC3-CE-ATM	3.6.2	1-Port Channelized STM-1/OC-3 Shared Port Adapters
SPA-1X10GE-L-V2	3.7.1.1.0	Cisco 1-Port 10GE LAN-PHY Shared Port Adapter
SPA-1XCHOC12/DS0	3.6.6	1-Port Channelized OC-12/STM-4 Shared Port Adapter
SPA-1XCHSTM1/OC3	3.6.0	1-port Channelized STM1/OC3 to DS0 SPA
SPA-1XOC12-ATM	3.6.0	1-Port OC-12c/STM-4c ATM SPA
SPA-1XOC12-ATM-V2	3.7.1.1.0	1-port OC12c SFP Optics ATM Shared Port Adapter
SPA-1XOC12-POS	3.6.0	1-port OC-12c/STM-4c POS SPA
SPA-1XOC3-ATM-V2	3.7.1.1.0	1-port OC3c SFP Optics ATM Shared Port Adapter
SPA-1XOC48-ATM	3.6.0	1 port OC-48c/STM-16 ATM SPA
SPA-1XOC48POS/RPR	3.6.7	1 port OC-48c/STM-16 POS/RPR SPA
SPA-1XTENGE-XFP	3.6.0	1-port 10 Gigabit Ethernet SPA, LANPHY XFP Optics
SPA-24CHT1-CE-ATM	3.6.0	24-Port Channelized T1/E1/J1 ATM CEoP SPA
SPA-2X1GE	3.6.0	2-port Gigabit Ethernet SPA, SFP Optics

Table 6-60 Supported Modules for Cisco 7600 Series—Cisco Prime Network 3.9 (continued)

Module Name	Product_Version	Module Description
SPA-2X1GE-SYNCE	3.7	2-port Synchronous Gigabit Ethernet Shared Port Adapter
SPA-2X1GE-V2	3.6.0	2-port Gigabit Ethernet SPA, SFP Optics
SPA-2XCT3/DS0	3.6.0	2-port Channelized T3 to DS0 SPA
SPA-2XOC3-ATM	3.6.0	2-port OC-3c/STM-1c ATM SPA
SPA-2XOC3-POS	3.6.0	2-port OC-3c/STM-1c POS SPA
SPA-2XOC48POS/RPR	3.6.1	1-port 10 Gigabit Ethernet Shared Port Adapter XFP based
SPA-2XOC48POSRPR	3.6.0	2 port OC-48 POS/RPR SPA with SFP Optics
SPA-2XT3/E3	3.6.0	2-port Clear Channel T3/E3 SPA
SPA-3XOC3-ATM-V2	3.7.1.1.0	3-port OC3c SFP Optics ATM Shared Port Adapter
SPA-4X1FE-TX-V2	3.6.0	4-port 10/100 Ethernet SPA TX
SPA-4XCT3/DS0	3.6.0	4-port Channelized T3 to DS0 SPA
SPA-4XOC3-ATM	3.6.0	4-port OC-3c/STM-1c ATM SPA
SPA-4XOC3-POS	3.6.0	4-port OC-3c/STM-1c POS SPA
SPA-4XOC48POSRPR	3.6.0	4-port OC-48c/STM-16 POS/DPT/RPR SPA
SPA-4XT3/E3	3.6.0	4-port Clear Channel T3/E3 SPA
SPA-5X1GE	3.6.0	5-port Gigabit Ethernet SPA, SFP Optics
SPA-5X1GE-V2	3.6.2	5-Port Gigabit Ethernet Shared Port Adapter
SPA-8X1FE-TX-V2	3.6.0	8-port 10/100 Ethernet SPA TX
SPA-8XCHT1/E1	3.6.0	8-Port Channelized T1/E1 SPA
SPA-IPSEC-2G	3.6.7	IpSec SPA with 2Gbps DES/3DES/AES
SPA-OC192POS-LR	3.6.0	1-port OC-192c/STM-64 POS/RPR SPA, SM-LR
SPA-OC192POS-XFP	3.6.0	1-port OC-192c/STM-64 POS/RPR SPA, XFP Optics
WS-C6509-E-FAN	3.6.0	High-capacity fan tray
WS-C6509-NEB-A	3.6.1	Enhanced 9-slot vertically oriented chassis
WS-C6K-13SLOT-FAN	3.7	Cisco 7613 fan tray, spare
WS-C6K-VTT-E	3.7	Cisco 6500 VTT Module
WS-CAC-3000W	3.6.4	Catalyst 6500 3000W AC power supply
WS-CAC-4000W-INT	3.6.4	4000W AC PowerSupply, International (cable included)
WS-CAC-4000W-US	3.6.4	4000Watt AC Power Supply for US (cable attached)
WS-CAC-6000W	3.6.0	Cat6500 6000W AC Power Supply
WS-CDC-2500W	3.6.4	Catalyst 6000 2500W DC Power Supply
WS-F6700-CFC	3.6.0	Catalyst 6500 Central Fwd Card for WS-X67xx modules

Table 6-60 Supported Modules for Cisco 7600 Series—Cisco Prime Network 3.9 (continued)

Module Name	Product_Version	Module Description
WS-F6700-DFC3A	3.6.1	Distributed Forwarding Card 3
WS-F6700-DFC3B	3.6.1	Catalyst 6500 Distributed forwarding card 3B
WS-F6700-DFC3BXL	3.6.0	Distributed Forwarding Card 3BXL (DFC3BXL) for use on CEF720 modules
WS-F6700-DFC3C	3.6.0	Distributed Forwarding Card 3C (DFC3C) for use on CEF720 modules
WS-F6700-DFC3CXL	3.6.0	Distributed Forwarding Card 3CXL (DFC3CXL) for use on CEF720 modules
WS-F6K-FE48X2-AF	3.6.0	IEEE 802.3af PoE daughtercard
WS-F6K-GE48-AF	3.6.0	IEEE 802.3af PoE daughtercard
WS-F6K-MSFC2	3.6.1	Multilevel Switching Feature Card Version 2 for Catalyst 6000 that is treated as a standalone system by the NMS
WS-F6K-PFC2	3.6.1	Catalyst 6500 L3 switching engine II
WS-F6K-PFC3B	3.7	Policy Feature Card-3B
WS-F6K-PFC3BXL	3.6.0	Policy Feature Card 3BXL (PFC3BXL)
WS-F6K-PFC3CXL	3.6.0	Policy Feature Card 3CXL (PFC3CXL)
WS-F6K-VPWR	3.6.0	PoE Daughtercard
WS-F6K-VPWR-GE	3.6.0	PoE Daughtercard
WS-G6483	3.6.0	10GBASE-ER serial 1550 nm extended-reach OIM
WS-G6488	3.6.0	10GBASE-LR serial 1310 nm long-reach OIM
WS-SUP32-10GE-3B	3.6.0	Supervisor Engine 32
WS-SUP32-GE-3B	3.6.0	Supervisor Engine 32
WS-SUP720-3B	3.6.0	Supervisor Engine 720 with PFC3B
WS-SUP720-3BXL	3.6.0	Supervisor Engine 720 with PFC3BXL
WS-SVC-ADM-1-K9	3.6.3	Catalyst 6500 Cisco Anomaly Detection Module
WS-SVC-AGM-1-K9	3.6.3	Catalyst 6500 Cisco Anomaly Guard Module
WS-SVC-FWM-1-K9	3.6.0	Firewall blade for 6500 and 7600, VFW License Separate
WS-SVC-IDS2-BUN-K9	3.6.1	Cisco Catalyst 6500 Series Intrusion Detection System (IDSM-2) Service Module
WS-SVC-IDSUPG	3.7	IDS 2 accelerator board
WS-SVC-MWAM-1	3.6.0	Multi-Processor WAN Application Module
WS-SVC-NAM-1	3.6.0	Network Analysis module 1
WS-SVC-NAM-2	3.6.0	Network Analysis module 2
WS-X6148A-GE-TX	3.6.0	48 port 10/100/1000 RJ-45 Ethernet Switching Module

Table 6-60 Supported Modules for Cisco 7600 Series—Cisco Prime Network 3.9 (continued)

Module Name	Product_Version	Module Description
WS-X6148A-RJ-45	3.6.0	48 port 10/100TX RJ-45 Ethernet/Fast Ethernet Switching Module
WS-X6148FE-SFP	3.6.1	Catalyst 6500 48 port 100Base-X SFP module
WS-X6148-FE-SFP	3.6.0	48 port 100BASE-FX Fast Ethernet Switching Module
WS-X6148-GE-TX	3.6.0	48 port 10/100/1000 RJ-45 Ethernet Switching Module
WS-X6148-RJ-21	3.6.0	48 port 10/100TX RJ-21 Ethernet/Fast Ethernet Switching Module
WS-X6148-RJ-45	3.6.0	48 port 10/100TX RJ-45 Ethernet/Fast Ethernet Switching Module
WS-X6148X2-RJ-45	3.6.0	96 port 10/100TX RJ-45 Ethernet/Fast Ethernet Switching Module
WS-X6196-RJ-21	3.6.0	96 port 10/100TX RJ-21 Ethernet/Fast Ethernet Switching Module
WS-X6248A-TEL	3.6.0	48 port 10/100TX RJ-21 Enhanced Ethernet/Fast Ethernet Switching Module
WS-X6248-RJ-45	3.6.0	48 port 10/100TX RJ-45 Ethernet/Fast Ethernet Switching Module
WS-X6248-TEL	3.6.0	48 port 10/100TX RJ-21 Ethernet/Fast Ethernet Switching Module
WS-X6316-GE-TX	3.6.0	16-port Gigabit Ethernet RJ-45
WS-X6324-100FX-SM	3.6.0	24 port 100FX SingleMode Fast Ethernet Switching Module
WS-X6348-RJ-21	3.6.0	6500 48 port 10/100BaseTX (RJ-21)
WS-X6348-RJ-45	3.6.0	48 port 10/100TX RJ-45 Ethernet/Fast Ethernet Switching Module
WS-X6408A-GBIC	3.6.0	8-port Gigabit Ethernet GBIC Enhanced QoS Module
WS-X6408-GBIC	3.6.0	8-port Gigabit Ethernet GBIC
WS-X6416-GBIC	3.6.0	16-port Gigabit Ethernet GBIC
WS-X6502-10GE	3.6.0	1-port 10-Gigabit Ethernet
WS-X6516A-GBIC	3.6.0	16-port Gigabit Ethernet GBIC
WS-X6516-GBIC	3.6.0	16-port Gigabit Ethernet GBIC
WS-X6516-GE-TX	3.6.0	16 port 10/100/1000 Base-T Ethernet Switching Module
WS-X6548-GE-TX	3.6.0	48 port 10/100/1000 RJ-45 Ethernet Switching Module
WS-X6548-RJ-21	3.6.0	48 port 10/100TX RJ-21 Ethernet/Fast Ethernet Switching Module

Table 6-60 Supported Modules for Cisco 7600 Series—Cisco Prime Network 3.9 (continued)

Module Name	Product_Version	Module Description
WS-X6548-RJ-45	3.6.0	48 port 10/100TX RJ-45 Ethernet/Fast Ethernet Switching Module
WS-X6582-2PA	3.6.0	Enhanced FlexWAN Module;
WS-X6700-CFC	3.6.0	Centralized Forwarding Card
WS-X6704-10GE	3.6.0	4-port 10-Gigabit Ethernet
WS-X6708-10GE	3.6.7	CEF720 8 port 10GE with DFC Rev. 1.4
WS-X6724-SFP	3.6.0	24-port Gigabit Ethernet SFP
WS-X6748-GE-TX	3.6.0	48 port 10/100/1000 RJ-45 Ethernet Switching Module
WS-X6748-SFP	3.6.0	48-port Gigabit Ethernet SFP
WS-X6816-GBIC	3.6.0	16-port Gigabit Ethernet GBIC
WS-X6K-S1A-MSFC2	3.6.1	Catalyst 6000 Supervisor Engine 1A, 2 Gigabit Ethernet, plus MSFC2 and policy feature card (PFC)
WS-X6K-S2-MSFC2	3.6.1	Catalyst 6500 Supervisor Engine-2, 2GE, plus MSFC-2 / PFC-2
WS-X6K-SUP2-2GE	3.6.1	Supervisor 2 with 2 Gigabit Ethernet ports
X2-10GB-CX4	3.7.1	X2 GE SR transceiver for RSP720-10GE
X2-10GB-ER	3.7.1	X2 GE LR transceiver for RSP720-10GE
X2-10GB-LR	3.7.1	X2 GE LX4 transceiver for RSP720-10GE
X2-10GB-LX4	3.7.1	X2 GE ER transceiver for RSP720-10GE
X2-10GB-SR	3.7.1	X2 GE CX4 transceiver for RSP720-10GE
XENPAK-10GB-CX4	3.7	10GBASE-CX4 XENPAK transceiver module for CX4 cable, copper, InfiniBand 4X connector
XENPAK-10GB-ER	3.6.0	10GBASE-ER Serial 1550-nm extended-reach, single-mode fiber (SMF), dispersion-shifted fiber (DSF)
XENPAK-10GB-ER+	3.6.7	10GBase-ER transceiver module for SMF, 1550-nm wavelength ,duplex connector
XENPAK-10GB-LR	3.6.7	10GBase-LR-XENPAK Module
XENPAK-10GB-LR+	3.6.1	10GBASE-LR XENPAK Module
XENPAK-10GB-LW	3.7	Cisco 10GBASE-LW XENPAK Module for SMF
XENPAK-10GB-SR	3.6.0	10GBASE-SR Serial 850-nm short-reach multimode fiber (MMF)
XFP-10GER-192IR+	3.6.6	Cisco multirate XFP transceiver module for 10GBASE-ER Ethernet and OC-192/STM-64 intermediate-reach (IR-2) Packet-over-SONET/SDH (POS) applications, SMF, dual LC connector
XFP-10GLR-OC192SR	3.6.4	OC192 XFP Single Mode Long Reach 2 (80km)
XFP-10G-MM-SR	3.7.2	10GBASE-SR

Table 6-60 Supported Modules for Cisco 7600 Series—Cisco Prime Network 3.9 (continued)

Module Name	Product_Version	Module Description
XFP-10GZR-OC192LR	3.6.6	Cisco multirate XFP transceiver module for 10GBASE-LR Ethernet and OC-192/STM-64 long-reach Packet-over-SONET/SDH (POS) applications, SMF, dual LC connector
CISCO-SFP-T3-GE	ANA-3.7.2-DP1	Cisco SFP Ethernet to T3 Remote Bridge
ACE30-MOD-K9	ANA-3.7.2-DP1	Cisco Application Control Engine (ACE30) Module
DWDM-GBIC-30.33	ANA-3.7.2-DP2	Cisco Dense Wavelength-Division Multiplexing Gigabit Interface Converters
DWDM-GBIC-31.12	ANA-3.7.2-DP2	Cisco Dense Wavelength-Division Multiplexing Gigabit Interface Converters
DWDM-GBIC-31.90	ANA-3.7.2-DP2	Cisco Dense Wavelength-Division Multiplexing Gigabit Interface Converters
DWDM-GBIC-32.68	ANA-3.7.2-DP2	Cisco Dense Wavelength-Division Multiplexing Gigabit Interface Converters
DWDM-GBIC-34.25	ANA-3.7.2-DP2	Cisco Dense Wavelength-Division Multiplexing Gigabit Interface Converters
DWDM-GBIC-35.04	ANA-3.7.2-DP2	Cisco Dense Wavelength-Division Multiplexing Gigabit Interface Converters
DWDM-GBIC-35.82	ANA-3.7.2-DP2	Cisco Dense Wavelength-Division Multiplexing Gigabit Interface Converters
DWDM-GBIC-36.61	ANA-3.7.2-DP2	Cisco Dense Wavelength-Division Multiplexing Gigabit Interface Converters
DWDM-GBIC-38.19	ANA-3.7.2-DP2	Cisco Dense Wavelength-Division Multiplexing Gigabit Interface Converters
DWDM-GBIC-39.98	ANA-3.7.2-DP2	Cisco Dense Wavelength-Division Multiplexing Gigabit Interface Converters
DWDM-GBIC-39.77	ANA-3.7.2-DP2	Cisco Dense Wavelength-Division Multiplexing Gigabit Interface Converters
DWDM-GBIC-40.56	ANA-3.7.2-DP2	Cisco Dense Wavelength-Division Multiplexing Gigabit Interface Converters
DWDM-GBIC-42.14	ANA-3.7.2-DP2	Cisco Dense Wavelength-Division Multiplexing Gigabit Interface Converters
DWDM-GBIC-42.94	ANA-3.7.2-DP2	Cisco Dense Wavelength-Division Multiplexing Gigabit Interface Converters
DWDM-GBIC-43.73	ANA-3.7.2-DP2	Cisco Dense Wavelength-Division Multiplexing Gigabit Interface Converters
DWDM-GBIC-44.53	ANA-3.7.2-DP2	Cisco Dense Wavelength-Division Multiplexing Gigabit Interface Converters

Table 6-60 Supported Modules for Cisco 7600 Series—Cisco Prime Network 3.9 (continued)

Module Name	Product_Version	Module Description
DWDM-GBIC-46.12	ANA-3.7.2-DP2	Cisco Dense Wavelength-Division Multiplexing Gigabit Interface Converters
DWDM-GBIC-46.92	ANA-3.7.2-DP2	Cisco Dense Wavelength-Division Multiplexing Gigabit Interface Converters
DWDM-GBIC-47.72	ANA-3.7.2-DP2	Cisco Dense Wavelength-Division Multiplexing Gigabit Interface Converters
DWDM-GBIC-48.51	ANA-3.7.2-DP2	Cisco Dense Wavelength-Division Multiplexing Gigabit Interface Converters
DWDM-GBIC-50.12	ANA-3.7.2-DP2	Cisco Dense Wavelength-Division Multiplexing Gigabit Interface Converters
DWDM-GBIC-50.92	ANA-3.7.2-DP2	Cisco Dense Wavelength-Division Multiplexing Gigabit Interface Converters
DWDM-GBIC-51.72	ANA-3.7.2-DP2	Cisco Dense Wavelength-Division Multiplexing Gigabit Interface Converters
DWDM-GBIC-52.52	ANA-3.7.2-DP2	Cisco Dense Wavelength-Division Multiplexing Gigabit Interface Converters
DWDM-GBIC-54.13	ANA-3.7.2-DP2	Cisco Dense Wavelength-Division Multiplexing Gigabit Interface Converters
DWDM-GBIC-54.94	ANA-3.7.2-DP2	Cisco Dense Wavelength-Division Multiplexing Gigabit Interface Converters
DWDM-GBIC-55.75	ANA-3.7.2-DP2	Cisco Dense Wavelength-Division Multiplexing Gigabit Interface Converters
DWDM-GBIC-56.55	ANA-3.7.2-DP2	Cisco Dense Wavelength-Division Multiplexing Gigabit Interface Converters
DWDM-GBIC-58.17	ANA-3.7.2-DP2	Cisco Dense Wavelength-Division Multiplexing Gigabit Interface Converters
DWDM-GBIC-58.98	ANA-3.7.2-DP2	Cisco Dense Wavelength-Division Multiplexing Gigabit Interface Converters
DWDM-GBIC-59.79	ANA-3.7.2-DP2	Cisco Dense Wavelength-Division Multiplexing Gigabit Interface Converters
DWDM-GBIC-60.61	ANA-3.7.2-DP2	Cisco Dense Wavelength-Division Multiplexing Gigabit Interface Converters
GLC-LH-SMD	ANA-3.7.2-DP2	Long wavelength gigabit Ethernet SFP
GLC-SX-MMD	ANA-3.7.2-DP2	Short wavelength gigabit Ethernet SFP
SFP-OC48-LR2	ANA-3.7.3-DP6	OC-48c/STM-16 pluggable long-reach (80 km) transceiver module, 1550-nm wavelength, LC connector

Table 6-60 Supported Modules for Cisco 7600 Series—Cisco Prime Network 3.9 (continued)

Module Name	Product_Version	Module Description
SFP-OC48-SR	ANA-3.7.3-DP6	OC-48c/STM-16 pluggable short-reach (2 km) transceiver module, 1310-nm wavelength, LC connector
GLC-ZX-SMD	ANA-3.7.3-DP8[33]	GE ZX
WS-IPSEC-3	ANA-3.7.3-DP8	IPSec Shared Port Adapter with 5 Gbps DES/3DES/AES
WS-SSC-600	ANA-3.7.3-DP8	Cisco 7600 / Catalyst 6500 Services SPA Carrier Card-600 Rev. 1.0
7600-ES+ITU-2TG-LK	Cisco-ANA-3.7.x-DP12, Cisco-ANA-3.8-DP3	7600-ES+ITU-2TG-LK 7600 ES+ 2x10GE XFP ITU Rev. 1.0
ACE20-MOD-K9	Cisco-ANA-3.7.x-DP12, Cisco-ANA-3.8-DP3	ACE20-MOD-K9 1 ports Application Control Engine Module Rev. 2.5
WS-SVC-NAM-2-250S	Cisco-ANA-3.7.x-DP12, Cisco-ANA-3.8-DP3	WS-SVC-NAM-2-250S 8 ports Network Analysis Module Rev. 1.2
76-ES+XT-2TG3CXL	Cisco-ANA-3.7.x-DP12, Cisco-ANA-3.8-DP3	76-ES+XT-2TG3CXL 2 ports 7600 ES+ Rev. 1.1

1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 31, 32 Support Verified against XC Combo Cards in ANA 3.7

33 Tested using 15.2 Nightly build (RLS 11)

Cisco 7600 Series—Supported Technologies

The following technologies are supported by the Cisco 7600 Series in Cisco Prime Network 3.9:

- IP, page 6-199
- Routing Protocols, page 6-202

- Ethernet, page 6-205
- ATM, page 6-213
- Frame Relay, page 6-217
- PPP, page 6-219
- HDLC, page 6-220
- SONET/SDH, page 6-220
- TDM/DSx, page 6-222
- MPLS, page 6-226
- MPLS-TE, page 6-228
- MPLS-TP, page 6-231
- VPN (VRF), page 6-233
- PWE3, page 6-235
- Security, page 6-237
- Hardware, page 6-238
- Serial, page 6-242
- Additional Technologies, page 6-243
- IPoDWDM, page 6-243
- LocalSwitching, page 6-245
- BFD, page 6-246
- Carrier Ethernet, page 6-247
- CDP, page 6-249
- Discovery Protocol, page 6-249
- Ethernet OAM, page 6-250
- AccessGatewayService, page 6-262
- 6PE, page 6-264
- 6rd, page 6-264
- MLACP, page 6-265

Cisco 7600 Series—Supported Service Events

Table 6-61 Supported Service Events for Cisco 7600 Series—Cisco Prime Network 3.9

Event Name	Product_Version	Expedited
Active IP Interfaces Found	3.6.0	Y
All IP Interfaces Down	3.6.0	Y
BGP link down due to admin	3.6.0	Y
BGP link down due to oper	3.6.0	Y

Table 6-61 Supported Service Events for Cisco 7600 Series—Cisco Prime Network 3.9

Event Name	Product_Version	Expedited
Card Down	3.6.0	Y
Card In	3.6.0	Y
Card Out	3.6.0	Y
Card Up	3.6.0	Y
CPU utilization exceeded upper threshold	3.6.0	N
Device Unsupported	3.6.0	N
Dropped packet rate exceeded upper threshold	3.6.0	N
DS0 Bundle Admin down	3.7	N
DS0 Bundle Oper down	3.7	N
DS0 Bundle Up	3.7	N
DS1 Path link down due to Admin down	3.7	N
DS1 Path link down due to Oper down	3.7	N
DS1 Path link Up	3.7	N
DS1 Path up	3.7	N
EFP down due to error disabled	3.6.7	N
IMA Administratively down	3.7	N
IMA Operationally down	3.7	N
IMA Operationally up	3.7	N
Keepalive configured	3.7	N
Keepalive not configured	3.7	N
Layer 2 Tunnel Down	3.6.0	N
LDP neighbor down	3.6.0	Y
Link up	3.6.0	N
Memory utilization exceeded upper threshold	3.6.0	N
MLPPP Administratively down	3.7	N
MLPPP Operationaly down	3.7	N
MLPPP Up	3.7	N
MPLS Black Hole found	3.6.0	N
MPLS interface removed	3.6.0	Y
MPLS-TP TP Tunnel Down	Prime Network 3.8	N

Table 6-61 Supported Service Events for Cisco 7600 Series—Cisco Prime Network 3.9

Event Name	Product_Version	Expedited
MPLS-TP LSP Down	Prime Network 3.8	N
MPLS-TP Bandwidth mismatch	Prime Network 3.8	N
Pluggable transceiver out	Prime Network 3.8	N
power-supply down	Prime Network 3.8	N
Power-supply out	Prime Network 3.8	N
Primary HSRP Interface Active	3.6.0	N
rep port role change	Prime Network 3.8	Y
Primary HSRP Interface not Active	3.6.0	N
Rx utilization exceeded upper threshold	3.6.0	N
Secondary HSRP Interface Active	3.6.0	N
Secondary HSRP Interface not Active	3.6.0	N
Sonet Path link down due to Admin down	3.7	N
Sonet Path link Up	3.7	N
SONET Path up	3.7	N
Tx utilization exceeded upper threshold	3.6.0	N
VSI Down	3.6.7	N
fan-tray down	Prime Network 3.8	N
Fan-tray out	Prime Network 3.8	N

Cisco 10000 Series Routers

This section includes the following information about Cisco 10000 Series routers (for information on the NE types supported in Cisco Prime Network 3.9, see Cisco 10000 Series Routers):

- Cisco 10000 Series—Supported Software Versions, page 6-81
- Cisco 10000 Series—Supported Topologies, page 6-82
- Cisco 10000 Series—Supported Modules, page 6-82
- Cisco 10000 Series—Supported Technologies, page 6-83
- Cisco 10000 Series—Supported Service Events, page 6-84

Cisco 10000 Series—Supported Software Versions

Table 6-62 Supported Software Versions for Cisco 10000 Series—Cisco Prime Network 3.9

Software Version	Product_Version
IOS 12.0(20)	3.6.1[1]
IOS 12.0(22)S5	3.5.2[2]
IOS 12.0(23)S	3.5.2[3]
IOS 12.0(23)S2	3.6.1[4]
IOS 12.1(10)E	3.5.2[5]
IOS 12.2(18.2)	3.5.2[6]
IOS 12.2(24)S	3.6.1[7]
IOS 12.2(24)S4	3.6.1[8]
IOS 12.2(28)SB3	3.6.2[9]
IOS 12.2(31)SB	3.6.1[10]
IOS 12.2(33)SB1	3.6.7[11]
IOS 12.3(7)XI7	3.6.1[12]
IOS 12.2(33)SB8	3.7.1[13]
IOS 12.2(33)XNE	3.7.1[14]
IOS 15.0.(1)S1	3.7.1.0.4[15]
IOS 15.0.(1)S	3.7.1.0.4[16]
IOS 12.2(31)SB18	3.7.2-DP-1.0
IOS 12.2(31)SB19	3.7.2-DP-1.0
IOS 12.2(33)XNE3	3.7.2-DP-1.0
IOS 12.2(33)SB9	3.7.2-DP-1.0
IOS 15.0(1)S2	3.7.2-DP-1.0
IOS 15.0(1)S3a	3.7.2-DP-3.0
IOS 12.2(33)SB10	3.7.X-DP-4.0

Table 6-62 Supported Software Versions for Cisco 10000 Series—Cisco Prime Network 3.9

Software Version	Product_Version
IOS 12.2(31)SB20	3.7.X-DP-6.0
IOS 15.0(1)S4	3.7.X-DP-6.0

[1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 14, 15, 16]ANA models pluggable ports for this IOS version.

13ANA recognizes all maintenance builds in this IOS release train.ANA models pluggable ports for this IOS version.

Cisco 10000 Series—Supported Topologies

Table 6-63 Supported Topologies for Cisco 10000 Series—Cisco Prime Network 3.9

Topology Type	Link Type	Product_Version
ATM	ATM	3.6.0
Ethernet	Ethernet	3.6.0
MPLS	MPLS	3.6.0
PPP/HDLC	PPP or HDLC	3.6.1
Physical Layer	Physical Layer	3.6.1
MLPPP	MLPPP	3.7.1
VPN (IPv6)	VPN	3.7.0

Cisco 10000 Series—Supported Modules

Table 6-64 Supported Modules for Cisco 10000 Series—Cisco Prime Network 3.9

Module Name	Product_Version	Module Description
10000-SIP-600	3.7.1	Cisco 10000 SPA Interface Processor-600
ESR-1COC12-SMI	3.6.1	Cisco 10K 1 port channelized OC12
ESR-1GE	3.6.0	1-port Gigabit Ethernet
ESR-1OC-12/P-SMI	3.6.0	1-port OC-12/STS-12c/STM-4 OS/SDH, single mode,intermediate reach
ESR-1OC-12-ATM	3.7.1	1-port OC-12 ATM
ESR-24CT1/E1	3.6.0	24-port channelized E1/T1
ESR-4OC3-ATM-SM	3.6.0	4-port OC-3/STM-1 ATM, single mode
ESR-4OC3-CHSTM1	3.6.7	Four-port channelized STM-1/OC-3 SDH single mode line card
ESR-6CT3	3.6.0	6-port channelized T3

Table 6-64 Supported Modules for Cisco 10000 Series—Cisco Prime Network 3.9 (continued)

Module Name	Product_Version	Module Description
ESR-6OC3/P-SMI	3.6.0	6-port OC-3c/STS-3c/STM-1 POS/SDH, single mode,intermediate reach
ESR-8E3/DS3	3.7.1	8 port clear channel E3/DS3 Line Card
ESR-8E3DS3-ATM	3.6.7	8 Port Channelized E3/DS3 ATM line card
ESR-HH-1GE	3.6.0	1-port Gigabit Ethernet half-height
ESR-HH-4CT3	3.6.7	4 Port Channelized T3 Half-Height Line Card
ESR-HH-8FE-TX	3.6.0	8-port Fast Ethernet half-height
ESR-PRE1	3.6.1	Cisco 10K Performance Routing Engine-1
ESR-PRE2	3.6.1	Cisco 10K Performance Routing Engine-2
ESR-PRE3	3.6.1	Cisco 10K Performance Routing Engine-3
SPA-1XCHOC12/DSO	3.7	1 port channelized OC12 to DS0 Shared Port Adapter
SPA-2XCHOC12/DSO	3.7	2 port channelized OC12 to DS0 Shared Port Adapter

Cisco 10000 Series—Supported Technologies

The following technologies are supported by the Cisco 10000 Series in Cisco Prime Network 3.9:

- IP, page 6-199
- Routing Protocols, page 6-202
- Ethernet, page 6-205
- ATM, page 6-213
- Frame Relay, page 6-217
- PPP, page 6-219
- HDLC, page 6-220
- SONET/SDH, page 6-220
- TDM/DSx, page 6-222
- MPLS, page 6-226
- MPLS-TE, page 6-228
- VPN (VRF), page 6-233
- PWE3, page 6-235
- Security, page 6-237
- Hardware, page 6-238
- Serial, page 6-242
- Additional Technologies, page 6-243
- LocalSwitching, page 6-245
- Carrier Ethernet, page 6-247

- CDP, page 6-249
- Discovery Protocol, page 6-249
- 6PE, page 6-264

Cisco 10000 Series—Supported Service Events

Table 6-65 Supported Service Events for Cisco 10000 Series—Cisco Prime Network 3.9

Event Name	Product_Version	Expedited
Active IP Interfaces Found	3.6.0	Y
All IP Interfaces Down	3.6.0	Y
BGP process up	3.6.0	N
Card Down	3.6.0	Y
Card Up	3.6.0	Y
CPU utilization exceeded upper threshold	3.6.0	N
Device Unsupported	3.6.0	Y
DS0 Bundle Admin down	3.6.7	N
DS0 Bundle Oper down	3.6.7	N
DS0 Bundle Up	3.6.7	N
DS1 Path down due to Admin	3.6.7	N
DS1 Path down due to Card	3.6.7	N
DS1 Path down due to Oper	3.6.7	N
DS1 Path link down due to Admin down	3.6.7	N
DS1 Path link down due to Oper down	3.6.7	N
DS1 Path link Up	3.6.7	N
Layer 2 Tunnel Down	3.6.0	N
Link up	3.6.0	N
Memory utilization exceeded upper threshold	3.6.0	N
MLPPP Administratively down	3.6.7	N
MLPPP Operationaly down	3.6.7	N
MLPPP Up	3.6.7	N
Module Unsupported	3.6.0	Y
MPLS Black Hole found	3.6.0	N
Rx utilization exceeded upper threshold	3.6.0	N
SONET Path down due to Admin	3.6.7	N

Table 6-65 Supported Service Events for Cisco 10000 Series—Cisco Prime Network 3.9

Event Name	Product_Version	Expedited
Sonet Path link down due to Admin down	3.6.7	N
SONET Path Link down due to Card event	3.6.7	N
SONET Path up	3.6.7	N
Tx utilization is below lower threshold	3.6.0	N

Cisco 12000 Series Routers

This section includes the following information about Cisco 12000 Series routers (for information on the NE types supported in Cisco Prime Network 3.9, see Cisco 12000 Series Routers):

- Cisco 12000 Series—Supported Software Versions, page 6-85
- Cisco 12000 Series—Supported Topologies, page 6-86
- Cisco 12000 Series—Supported Modules, page 6-87
- Cisco 12000 Series—Supported Technologies, page 6-92
- Cisco 12000 Series—Supported Service Events, page 6-93

Cisco 12000 Series—Supported Software Versions

Table 6-66 Supported Software Versions for Cisco 12000 Series—Cisco Prime Network 3.9

Software Version	Product_Version
IOS 12.0(23)S3	3.6.0[1]
IOS 12.0(26)S	3.6.0[2]
IOS 12.0(26)S1	3.6.0[3]
IOS 12.0(26)S2	3.6.0[4]
IOS 12.0(26)S3	3.6.0[5]
IOS 12.0(26)S4	3.6.0[6]
IOS 12.0(26)S5	3.6.0[7]
IOS 12.0(26)S6	3.6.0[8]
IOS 12.0(27)	3.6.0[9]
IOS 12.0(28)	3.6.0[10]
IOS 12.0(30)	3.6.0[11]
IOS 12.0(31)S	3.6.0[12]
IOS 12.0(31)S3	3.6.0[13]

Table 6-66 Supported Software Versions for Cisco 12000 Series—Cisco Prime Network 3.9

Software Version	Product_Version
IOS 12.0(31)	3.6.0[14]
IOS 12.0(32)	3.6.0[15]
IOS 12.0(32)S10	3.6.3[16]
IOS 12.0(32)SY	3.6.0[17]
IOS 12.0(32)SY2	3.6.0[18]
IOS 12.0(32)SY3	3.6.2[19]
IOS 12.0(32)SY4	3.6.7[20]
IOS 12.0(32)SY5	3.6.3[21]
IOS 12.0(32)SY9	3.7[22]
IOS 12.0(33)S	3.6.3[23]
IOS 12.0(33)S1	3.6.7[24]
IOS 12.0(33)S6	3.7.1
IOS 12.0(32)S5	3.7.1
IOS 12.0(32)SY6b	3.7.1
IOS 12.0(32)SY12	3.7.2-DP-1.0
IOS 12.0(32)SY13	3.7.X-DP-6.0
IOS 12.0(33)S8	3.7.X-DP-6.0

[1, 2, 3, 4, 5, 6, 7, 8, 12, 13, 15, 18, 19, 20, 21, 22, 24]ANA models pluggable ports for this IOS version.

[9, 10, 11, 14, 16, 17, 23]ANA recognizes all maintenance builds in this IOS release train.ANA models pluggable ports for this IOS version.

Cisco 12000 Series—Supported Topologies

Table 6-67 Supported Topologies for Cisco 12000 Series—Cisco Prime Network 3.9

Topology Type	Link Type	Product_Version
ATM	ATM	3.6.0
BGP	BGP	3.6.0
Ethernet	Ethernet	3.6.0
Framerelay	Framerelay	3.6.0
MPLS	MPLS	3.6.0
PPP/HDLC	PPP or HDLC	3.6.0
GRE Tunnel	GRE Tunnel	3.6.0
VPN (VRF)	VPN	3.6.0
Physical Layer	Physical Layer	3.6.5

Table 6-67 Supported Topologies for Cisco 12000 Series—Cisco Prime Network 3.9 (continued)

Topology Type	Link Type	Product_Version
MLPPP	MLPPP	3.7.1
VPN (IPv6)	VPN	3.7.1

Cisco 12000 Series—Supported Modules

Table 6-68 Supported Modules for Cisco 12000 Series—Cisco Prime Network 3.9

Module Name	Product_Version	Module Description
12000/16-AC-PEM	3.6.3	Cisco 12000 16-slot Enhanced AC PEM
12000/16-AC-PEM	3.6.4	GSR16 AC POWER SUPPLY
12000/16-AC-PEM	3.6.4	Cisco 12000 16-slot Enhanced AC PEM
12000/16-AC-PEM	3.6.4	Cisco 12000 16-slot Enhanced DC PEM
12000/16-DC-PEM	3.6.3	Cisco 12000 16-slot Enhanced DC PEM
12000/4-BLOWER	3.6.2	GSR 12404 Fan tray - cevFan12404FanTray7
12000/4-DC-PEM	3.6.4	Cisco 12000 4-slot DC PEM
12000/6-AC-PEM	3.6.4	Cisco 12000 6-slot Enhanced AC PEM
12000/6-DC-PEM	3.6.4	Cisco 12000 6-slot Enhanced DC PEM
12000-SIP-401	3.6.0	Cisco 12000 Series SPA Interface Processor-401
12000-SIP-501	3.6.1	Cisco 12000 Series SPA Interface Processor-501
12000-SIP-600	3.6.1	Cisco 12000 Series SPA Interface Processor-600
12000-SIP-601	3.6.1	Cisco 12000 Series SPA Interface Processor-601
12004E/20	3.6.3	Cisco 12004/12404 Enhanced Collapsed Fabric/Alarm card
12404E/80	3.6.3	GSR 12404 Enhanced Clock Scheduler Card
12810-CSC	3.6.7	12810 Clock Scheduler Card
12DS3-SMB	3.6.0	12 Port Copper DS3 Interface Line Card
16OC3X/POS-M-MJ-B	3.6.1	GSR16-Port OC3/POS MM/I Eng3 Release B
16-OC3X/POS-IR-LC	3.6.0	16-Port Packet-Over-SONET OC-3/STM-1 with Extended Feature Set Line Card (concatenated)
16OC3X/POS-IR-LC-B.	3.6.1	GSR 16-Port OC3/POS MM/I Eng3 Release B
1X10GE-ER-SC	3.6.1	1 Port 10Giga Ethernet Line Card
1X10GE-LR-SC	3.6.1	1 Port 10Giga Ethernet Line Card
3GE-GBIC-SC	3.6.0	4 Port Gigabit Ethernet Line Card (trident)
4GE-SFP-LC	3.6.1	4 port-GE line card for Cisco 12000
4OC12/POS-IR-SC-B	3.6.0	Enhanced 4 port OC-12 Intermediate Reach Line Card

Table 6-68 Supported Modules for Cisco 12000 Series—Cisco Prime Network 3.9 (continued)

Module Name	Product_Version	Module Description
4OC12X/ATM-IR-SC	3.6.0	GSR Edge Engine 48, ATM, 4 ports OC12/STM4 Single Mode Intermediate Reach Line Card
4OC12X/POS-I-SC-B	3.6.0	4 Port OC12 SM Intermediate Reach POS
4OC12X/POS-M-SC-B	3.6.0	Four-Port OC-12c/STM-4c POS/SDH ISE Line Card, Multi-Mode
4OC3/ATM-IR-SC	3.6.1	4 port OC3/STM1 ATM line MM/IR card
4OC3/ATM-MM-SC	3.6.1	4 port OC3/STM1 ATM line MM/IR card
4OC3X/ATM-IR-SC	3.6.1	4-port OC3/STM1 ATM Single Mode, intermediate reach ISE Line Card with SC connector
4OC3X/POS-IR-LC-B	3.6.1	GSR 4-port OC3/POS IR Eng3 release B
4OC3X/POS-LR-LC-B	3.6.1	GSR 4-port OC3/POS IR Eng3 release B
4OC3X/POS-MM-MJ-B	3.6.1	GSR 4-port OC3/POS IR Eng3 release B
4OC48E/POS-LR-SC	3.6.0	Edge 4 Port OC-48c/STM-16c SONET/SDH LR with SC
4OC48E/POS-SR-SC	3.6.0	Edge 4 Port OC-48c/STM-16c SONET/SDH SR with SC
4XOC48POS/RPR	3.6.1	4-port OC48/STM16 POS/RPR Shared Port Adapter = SPA-4XOC48POS/RPR
6CT3-SMB	3.6.0	6-port Channelized DS3-to-DS1 Line Card, SMB connector
8FE-FX-SC	3.6.0	8-Port Fast Ethernet Line Card
8FE-TX-RJ45	3.6.0	8-Port Fast Ethernet Line Card
8FE-TX-RJ45-B	3.6.1	8-port 100baseTX, RJ45 connector type, version B
8OC3X/POS-IR-LC-B	3.6.1	GSR 8-Port OC3/POS MM/IR Eng3 Release B
8OC3X/POS-MM-MJ-B	3.6.1	GSR 8-Port OC3/POS MM/IR Eng3 Release B
8X1FE-V2	3.6.1	8-port Fast Ethernet Shared Port Adapter V2 = SPA-8X1FE-V2
BUS_BOARD	3.6.1	GSR16 BUS BOARD (16) =
CHOC12/DS1-IR-SC	3.6.0	Cisco 12000 Series 1-Port Channelized OC-12c/STM-4
COPPER-12DS3	3.6.0	12 Port Copper DS3 Interface Line Card
COPPER-6DS3	3.6.0	6 Port Copper DS3 Interface Line Card
CRS-16-ALARM	3.6.1	Cisco CRS-1 Series 16 Slots Alarm Board = CRS-16-ALARM
GSR10-AC-PDU	3.6.0	Cisco 12410 AC Power Distribution Unit (spare)
GSR10-ADVNCD-CSC	3.6.1	12010 Advanced Clock Scheduler Card
GSR10-ADVNCD-SFC	3.6.1	12010 Advanced Switch Fabric Card
GSR10-ALRM	3.6.1	12410, 12010 Alarm Card

Table 6-68 Supported Modules for Cisco 12000 Series—Cisco Prime Network 3.9 (continued)

Module Name	Product_Version	Module Description
GSR10-CSC	3.6.1	12410 Clock Scheduler Card
GSR10-SFC	3.6.1	Cisco 12410 Switch Fabric Card
GSR16/320-CSC	3.6.1	12416 Clock Scheduler Card
GSR16/320-SFC	3.6.1	12416 Switch Fabric Card
GSR16/80-CSC	3.6.1	Cisco 12016 80 Gbps GSR Scheduler/Fabric
GSR16/80-SFC	3.6.1	Cisco 12016 80 GbpsGSR Switch Fabric
GSR16-ALRM	3.6.0	Cisco 12016 GSR Alarm Card
GSR16-BLOWER	3.6.1	Cisco 12016, 12416 Blower
GSR-3GE	3.6.0	3 Port Gigabit Ethernet Line Card (trident)
GSR4/80-AC	3.6.2	GSR 12404 AC Power Supply - cevPowerSupply12404AC
GSR6-ADVNCD-CSC	3.6.1	12006 Advanced Clock Scheduler Card
GSR6-ALRM	3.6.1	12406, 12006 Alarm Card
GSR6-BLOWER	3.6.1	12406, 12006 Blower
GSR6-CSC	3.6.1	Cisco 12406 Clock Scheduler Card
GSR6-SFC	3.6.1	Cisco 12406 Switch Fabric Card
GSR8-CSC/ALRM	3.6.1	Cisco 12008 GSR Scheduler/Fabric/Alarm
GSR-8FE-FX	3.6.0	8 port Fast Ethernet card with Fiber Interface
GSR8-SFC	3.6.1	Switch Fabric
GSR-ALARM10	3.6.0	GSR Alarm module
GSR-ALARM16	3.6.0	GSR-Alarm
GSR-ALARM6	3.6.0	GSR Alarm module
GSR-BUS-BOARD16	3.6.0	GSR Bus Board for Power distribution
GSR-CLOCK-OC192	3.6.0	GSR Clock Scheduler
GSR-CSC	3.6.0	GSR Clock Scheduler Card
GSR-CSC12410	3.6.0	GSR 12410 Clock scheduler
GSR-CSC16	3.6.0	Scheduler/Fabric Card
GSR-CSC16-OC192	3.6.0	GSR 12406 Clock Scheduler Card
GSR-CSC16-OC192	3.6.0	GSR 12016 OC192 Clock Scheduler Card
GSR-CSC6	3.6.0	GSR Clock Scheduler
GSR-E48-ATM-4OC12-MM-SR-SC	3.6.0	GSR Edge Engine 48, ATM, 4 port OC12/STM4Multi Mode Short Reach Line Card
GSR-E48-POS-16OC3-SM-IR-LC	3.6.0	16 Port OC3 SM Intermediate Reach POS
GSR-E48-POS-OC48-SM-LR-SC	3.6.0	GSR 12406 Switch Fabric Card

Table 6-68 Supported Modules for Cisco 12000 Series—Cisco Prime Network 3.9 (continued)

Module Name	Product_Version	Module Description
GSR-E48-POS-OC48-SM-SR-SC	3.6.0	GSR, Edge Engine 48 Port OC-48 SRP Single Mode Long Reach Line Card
GSR-E48-POS-QOC12-SM-IR-SC	3.6.0	4 Port OC12 SM Intermediate Reach POS
GSR-E-OC192-SM-SR-SC	3.6.0	Enhanced 1 Port OC 192 Short Reach 2 FC Connector Line Card.
GSR-E-QOC48-SM-LR-SC	3.6.0	4 Port Enhanced OC 48 Short Reach SC Connector Line Card
GSR-E-QOC48-SM-SR-SC	3.6.0	4 Port Enhanced OC 48 Short Reach SC Connector Line Card
GSR-GEFE	3.6.0	GSR General Fan
GSR-PA-3GE	3.6.0	GSR 3 port Port Adapter
GSR-RP	3.6.0	GSR RoMman Recovery
GSR-SFC	3.6.0	GSR Switch Fabric Card
GSR-SFC12410	3.6.0	GSR 12410 Switch Fabric Card
GSR-SFC16	3.6.0	Switch Fabric Card
GSR-SFC16-OC192	3.6.0	GSR 12406 Switch Fabric Card
GSR-SFC6	3.6.0	GSR Switch Fabric Card
OC12/SRP-IR-SC-B	3.6.0	2 Port OC-12 Single Mode SRP Intermediate Reach Line Card
OC12/SRP-MM-SC-B	3.6.0	2 Port OC-12 Multi Mode SRP Line Card
OC-48E/POS-SR-SC-B	3.6.0	2 Port Packet Over Sonet OC-48, Single Mode, Short Reach, SC Connector Card
OC48X/POS-LR-SC	3.6.0	One-Port OC-48c/STM-16c POS/SDH ISE Line Card, Long Reach
OC48X/POS-SR-SC	3.6.0	One-Port OC-48c/STM-16c POS/SDH ISE Line Card, Short Reach
POS-EN-OC48-LR-SC	3.6.0	Enhanced OC-48 Long Reach SC Connector Line Card
POS-EN-OC48-SR-SC	3.6.0	Enhanced OC-48 Short Reach SC Connector Line Card
POS-EN-QOC12-IR	3.6.0	Enhanced 4 port OC-12 Intermediate Reach Line Card
POS-EN-QOC48-SM-LR-FC	3.6.0	4 Port (Quad) Enhanced OC-48 Long Reach FC Connector Line Card
POS-EN-QOC48-SM-LR-SC	3.6.0	4 Port (Quad) Enhanced OC-48 Long Reach SC Connector Line Card
POS-EN-QOC48-SM-SR-SC	3.6.0	4 Port (Quad) Enhanced OC-48 Short Reach SC Connector Line Card

Table 6-68 Supported Modules for Cisco 12000 Series—Cisco Prime Network 3.9 (continued)

Module Name	Product_Version	Module Description
POS-OC48-SM-SR-SC	3.6.0	1 Port Packet Over Sonet OC-48, Single Mode, Short Reach, SC Connector Card
POS-QOC12-MM-SR	3.6.0	4 port (Quad) OC-12 POS Card, Single Mode, Short Reach
PRP-1	3.6.0	Performance Route Processor-1
PRP-2	3.6.0	Cisco XR 12000 and 12000 Series Performance Router Processor-2
PRP-3	3.6.0	Performance Route Processor-3
PRP-4	3.6.0	Cisco XR 12000 and 12000 Series Performance Router Processor-4
SFP-GE-L	3.7	1000BASE-LH/LX pluggable transceiver
SFP-GE-S	3.7	1000BASE-Sx Short wavelength gigabit ethernet SFP.
SFP-GE-T	3.7	1000BASE-T copper gigabit ethernet SFP.
SFP-OC3-IR1	3.7	Intermediate range, single-mode fiber
SFP-OC48-IR1	3.6.1	OC-48c/STM-16c
SFP-OC48-LR2	3.6.1	OC-48c/STM-16c SFP, Long Reach (80km)
SPA-10X1GE	3.6.1	10-port 1 GbE Shared Port Adapter
SPA-1X10GE-L-V2	3.6.0	Cisco 1-Port 10GE LAN-PHY Shared Port Adapter
SPA-1XCHOC48/DS3	3.6.2	1-Port Channelized STM-16/OC-48 SPA.
SPA-1XCHSTM1/OC3	3.6.1	1-port Channelized STM-1/OC-3c to DS0 Shared Port Adapter.
SPA-1XOC12-ATM-V2	3.6.2	1-port OC12c SFP Optics ATM Shared Port Adapter
SPA-1XOC192POS-VSR	3.6.1	1-port OC192/STM64 POS VSR Optics Shared Port Adapter
SPA-1XOC3-ATM-V2	3.6.2	1-port OC3c SFP Optics ATM Shared Port Adapter
SPA-1XOC48POS/RPR	3.6.0	Port OC-48c/STM-16c POS/RPR Shared Port Adapter
SPA-1XTENGE-XFP	3.6.0	1-port 10Gigabit Ethernet Shared Port Adapter XFP based
SPA-1XTENGE-XFP-V2	3.6.0	1-port 10GbE Shared Port Adapter XFP based V2
SPA-24CHT1-CE-ATM	3.6.1	24-Port Channelized T1/E1/J1 ATM CEoP SPA
SPA-2CHT3-CE-ATM	3.6.2	2-port Channelized T3/E3 ATM + Circuit Emulation Shared Port Adapter
SPA-2X1GE	3.6.0	2 ports Gigabit Ethernet Shared Port Adapters
SPA-2X1GE-V2	3.6.1	2 ports Gigabit Ethernet Shared Port Adapters
SPA-2XCT3/DS0	3.6.1	2-port Channelized T3 to DS0 Shared Port Adapter
SPA-2XOC12-POS	3.6.0	2-Port OC-3c/STM-1 and OC-12c/STM-4 POS SPA

Table 6-68 Supported Modules for Cisco 12000 Series—Cisco Prime Network 3.9 (continued)

Module Name	Product_Version	Module Description
SPA-2XOC48POS/RPR	3.6.0	2-port OC48/STM16 POS/RPR Shared Port Adapters
SPA-2XT3/E3	3.6.1	2-port Clear Channel T3/E3 Shared Port Adapter
SPA-3XOC3-ATM-V2	3.6.2	1-port OC3c SFP Optics ATM Shared Port Adapter
SPA-4XCT3/DS0	3.6.0	4-port Channelized T3 to DS0 Shared Port Adapter
SPA-4XOC12-POS	3.6.0	4-port OC-12/STM-4 POS Shared Port Adapters
SPA-4XOC3-POS-V2	3.6.0	4-port OC-3c/STM1c POS Shared Port Adapter
SPA-4XT3/E3	3.6.1	4-port Clear Channel T3/E3 Shared Port Adapter
SPA-5X1GE	3.6.0	5-Port Gigabit Ethernet SPA
SPA-5X1GE-V2	3.6.0	5-Port Gigabit Ethernet SPA
SPA-8X1FE-TX-V2	3.6.0	8-port 10/100 Ethernet SPA TX (Fugu ASIC)
SPA-8X1GE	3.6.0	8-port Gigabit Ethernet Shared Port Adapter_V2
SPA-8X1GE-V2	3.6.2	8-port 1GbE SPA (Fugu ASIC)
SPA-8XCHT1/E1	3.6.1	8-port Channelized T1/E1 to DS0 Shared Port Adapter
SPA-8XFE-TX	3.6.0	8-port 10/100 Ethernet SPA with RJ-45
SPA-8XOC12-POS	3.6.0	8-Port OC-12c/STM-4 Multirate POS SPA
SPA-OC192POS-LR	3.6.0	1-port OC192/STM64 POS/RPR SMLR Optics
SPA-OC192POS-VSR	3.6.1	1-port OC192/STM64 POS/RPR VSR Optics
SPA-OC192POS-XFP	3.6.0	1-port OC192/STM64 POS/RPR XFP Optics Shared Port Adapter with XFP-10GLR-OC192SR
SPA-OC192RPR-XFP	3.6.0	1-port OC192/STM64 POS/RPR XFP Optics Shared Port Adapter = SPA-OC192RPR-XFP
SRP-OC12-MM	3.6.0	1 Port OC-12 Multi Mode SRP Line Card
SRP-OC12-SM-IR	3.6.0	1 Port OC-12 Single Mode SRP Intermediate Reach Line Card
SSRP-OC48-SM-LR	3.6.0	1 Port OC-48 SRP Single Mode Long Reach Line Card
SSRP-OC48-SM-SR	3.6.0	1 Port OC-48 SRP Single Mode Short Reach Line Card
XR-PRP-2	3.6.1	Cisco XR 12000 and 12000 Series Performance Router Processor-2
SPA-1X10GE-L-ITUC	3.7.1	Cisco 1-Port 10 Gigabit Ethernet (10GE) Tunable WDM-PHY Shared Port Adapter

Cisco 12000 Series—Supported Technologies

The following technologies are supported by the Cisco 12000 Series in Cisco Prime Network 3.9:

- IP, page 6-199

- Routing Protocols, page 6-202
- Ethernet, page 6-205
- ATM, page 6-213
- Frame Relay, page 6-217
- PPP, page 6-219
- HDLC, page 6-220
- SONET/SDH, page 6-220
- TDM/DSx, page 6-222
- MPLS, page 6-226
- MPLS-TE, page 6-228
- VPN (VRF), page 6-233
- PWE3, page 6-235
- Security, page 6-237
- Hardware, page 6-238
- Serial, page 6-242
- Additional Technologies, page 6-243
- LocalSwitching, page 6-245
- BFD, page 6-246
- Carrier Ethernet, page 6-247
- CDP, page 6-249
- Discovery Protocol, page 6-249
- 6PE, page 6-264

Cisco 12000 Series—Supported Service Events

Table 6-69 Supported Service Events for Cisco 12000 Series—Cisco Prime Network 3.9

Event Name	Product_Version	Expedited
Active IP Interfaces Found	3.6.0	Y
All IP Interfaces Down	3.6.0	Y
BGP process up	3.6.0	N
Card Down	3.6.0	Y
Card In	3.6.0	Y
Card Out	3.6.0	Y
Card Up	3.6.0	Y
Cloud Problem	3.6.0	N
CPU utilization exceeded upper threshold	3.6.0	N

Table 6-69 Supported Service Events for Cisco 12000 Series—Cisco Prime Network 3.9

Event Name	Product_Version	Expedited
Device Unreachable	3.6.0	N
Device Unsupported	3.6.0	Y
DS1 Path link down due to Admin down	3.7	N
DS1 Path link down due to Oper down	3.7	N
DS1 Path link Up	3.7	N
Fan-tray down	Prime Network 3.8	N
Fan-tray out	Prime Network 3.8	N
Interface status down flapping	3.6.0	Y
Interface status down flapping update	3.6.0	Y
Keepalive configured	3.6.0	N
Keepalive not configured	3.6.0	N
Layer 2 Tunnel Down	3.6.0	N
Link Down	3.6.0	N
Link up	3.6.0	N
Memory utilization exceeded upper threshold	3.6.0	N
MLPPP Administratively down	3.7	N
MLPPP Operationaly down	3.7	N
MLPPP Up	3.7	N
Module Unsupported	3.6.0	Y
Pluggable transceiver out	Prime Network 3.8	N
Power-supply down	Prime Network 3.8	N
Power-supply out	Prime Network 3.8	N
Port Down	3.6.0	N
Port Flapping	3.6.0	N
Rx utilization exceeded upper threshold	3.6.0	N

Table 6-69 Supported Service Events for Cisco 12000 Series—Cisco Prime Network 3.9

Event Name	Product_Version	Expedited
Sonet Path link down due to Admin down	3.7	N
Sonet Path link down due to Oper down	3.7	N
Sonet Path link Up	3.7	N
SONET Path up	3.7	N
Tx utilization exceeded upper threshold	3.6.0	N
Vlan Tagged Interface AdminDown	3.6.7	N
Vlan Tagged Interface Up/Down	3.6.7	N
VPN Leak	3.6.0	N

Cisco XR 12000 Series Routers

This section includes the following information about Cisco XR 12000 Series routers (for information on the NE types supported in Cisco Prime Network 3.9, see Cisco XR 12000 Series Routers):

- Cisco XR 12000 Series—Supported Software Versions, page 6-95
- Cisco XR 12000 Series—Supported Topologies, page 6-96
- Cisco XR 12000 Series—Supported Modules, page 6-97
- Cisco XR 12000 Series—Supported Technologies, page 6-103
- Cisco XR 12000 Series—Supported Service Events, page 6-104

Cisco XR 12000 Series—Supported Software Versions

Table 6-70 Supported Software Versions for Cisco XR 12000 Series—Cisco Prime Network 3.9

Software Version	Product_Version
IOX 3.4.0	3.6.0
IOX 3.4.1	3.6.0
IOX 3.4.3	3.6.3
IOX 3.5.0	3.6.1
IOX 3.5.1	3.6.1
IOX 3.6.0	3.6.3[1]
IOX 3.6.1	3.6.3
IOX 3.6.2	3.6.5
IOX 3.6.3	3.6.7

Table 6-70 Supported Software Versions for Cisco XR 12000 Series—Cisco Prime Network 3.9

Software Version	Product_Version
IOX 3.7.0	3.6.4
IOX 3.7.1	3.6.4
IOX 3.8.0	3.6.6
IOX 3.8.1	3.6.7
IOX 3.8.2	3.7[2]
IOX 3.8.4	3.7.1
IOX 3.9.0	3.7
IOX 3.9.1	3.7.1
IOX 3.9.2	3.7.1.1.0
IOX 4.0.0	3.7.1.1.0
IOX 4.0.1	3.7.2
IOX 4.0.3	Cisco-ANA-3.7.x-DP4
IOX 4.1.0	Cisco-ANA-3.7.x-DP4
IOX 4.1.1	Cisco-ANA-3.7.x-DP6
IOX4.2.0	Cisco-ANA-3.7.x-DP11, PrimeNetwork-3.8.X-DP2

[1]ANA recognizes all maintenance builds starting from this IOS XR release train.

[2]ANA models pluggable port properties starting from this IOS XR version

Cisco XR 12000 Series—Supported Topologies

Table 6-71 Supported Topologies for Cisco XR 12000 Series—Cisco Prime Network 3.9

Topology Type	Link Type	Product_Version
BGP	BGP	3.6.0
Ethernet	Ethernet	3.6.0
MPLS	MPLS	3.6.0
PWE3 (Martini)	Tunnel	3.6.0
VPN (VRF)	VPN	3.6.0
Physical Layer	Physical Layer	3.6.0
LAG	LAG	3.6.2

Table 6-71 Supported Topologies for Cisco XR 12000 Series—Cisco Prime Network 3.9

Topology Type	Link Type	Product_Version
MLPPP	MLPPP	3.7.1
BFD	BFD	3.7.1
VPN (IPv6)	VPN	3.7.1

Cisco XR 12000 Series—Supported Modules

Table 6-72 Supported Modules for Cisco XR 12000 Series—Cisco Prime Network 3.9

Module Name	Product_Version	Module Description
12000/16-AC-PEM	3.6.4	Cisco 12000 16-slot Enhanced AC PEM
12000/16-DC-PEM	3.6.4	Cisco 12000 16-slot Enhanced DC PEM
12000/4-BLOWER	3.6.2	Cisco 12000 4-slot Blower
12000/4-DC-PEM	3.6.4	Cisco 12000 4-slot DC PEM
12000/6-AC-PEM	3.6.4	Cisco 12000 6-slot Enhanced AC PEM
12000/6-DC-PEM	3.6.4	Cisco 12000 6-slot Enhanced DC PEM
12000-SIP-401	3.6.0	Cisco 12000 Series SPA Interface Processor-401
12000-SIP-501	3.6.0	Cisco 12000 Series SPA Interface Processor-501
12000-SIP-600	3.6.0	Cisco 12000 Series SPA Interface Processor-600
12000-SIP-601	3.6.0	Cisco 12000 Series SPA Interface Processor-601
12410E-CSC	3.7.0.1	CISCO 12410 Enhanced Clock Scheduler Card
GSR10-SFC	3.6.0	GSR 12410 Switch Fabric Card
12410E-SFC	3.7.0.1	Cisco 12410 Enhanced Switch Fabric Card
12810-CSC	3.6.7	12810 Clock Scheduler Card
12810E-CSC	3.7.0.1	12810 800Gbps Enhanced Clock Scheduler Card
12810-SFC	3.6.5	GSR 12810 Switch Fabric Card
12816E-CSC	3.7.0.1	CISCO 12816 1280GBPS ENHANCED CLOCK SCHEDULER
12816-SFC	3.6.4	GSR 12816 Switch Fabric Card
12DS3-SMB	3.6.0	Cisco 12000 Series 12-Port DS3 Line Card
16OC3X/POS-I-LC-B	3.6.0	16 PORT OC3 WITH EXTENDED FEATURES RELEASE B
16-OC3X/POS-IR-LC	3.6.0	16-Port Packet-Over-SONET OC-3/STM-1 with Extended Feature Set Line Card (concatenated)
16OC3X/POS-IR-LC-B	3.6.0	16-port OC-3/STM-1 POS line card, IR optics (Engine 3)

Table 6-72 Supported Modules for Cisco XR 12000 Series—Cisco Prime Network 3.9 (continued)

Module Name	Product_Version	Module Description
16OC3X/POS-M-MJ-B	3.6.0	16-port OC-3/STM-1 POS line card, multimode optics (Engine 3)
1X10GE-ER-SC	3.6.1	1 Port 10Giga Ethernet Line Card
1X10GE-LR-SC	3.6.1	1 Port 10Giga Ethernet Line Card
3GE-GBIC-SC	3.6.0	Three-Port Gigabit Ethernet Line Card with default 128-MB code and route table memory
4GE-SFP-LC	3.6.0	4 port-GE line card for Cisco 12000
4OC12/ATM-IR-SC	3.6.0	4 port OC-12/STM4 ATM LC Intermediate Reach
4OC12/ATM-MM-SC	3.6.0	4-port OC12/STM4 ATM MM ISE LC with SC connector
4OC12/POS-IR-SC	3.6.0	Four-port OC12/STM4 Packet Over SONET/SDH with Enhanced UpgradeóSM with SC
4OC12/POS-IR-SC-B	3.6.0	Four-port OC12/STM4 Packet Over SONET/SDH with Enhanced UpgradeóSM with SC
4OC12/POS-SR	3.6.0	4 port (Quad) OC-12 POS Card, Single Mode, Short Reach
4OC12X/POS-I-SC-B	3.6.0	4 Port OC12 SM Intermediate Reach POS
4OC12X/POS-I-SC-B	3.6.0	4 Port OC12 SM Intermediate Reach POS
4OC12X/POS-M-SC-B	3.6.0	Four-Port OC-12c/STM-4c POS/SDH ISE Line Card, Multi-Mode
4OC3/ATM-IR-SC	3.6.0	4-port ATM Line Card Intermediate Reach
4OC3/ATM-MM-SC	3.6.0	4-port OC3 Multi-Mode ATM Line Card
4OC3X/ATM-IR-SC	3.6.1	4-port OC3/STM1 ATM Single Mode, intermediate reach ISE Line Card with SC connector
4OC3X/POS-IR-LC-B	3.6.0	GSR 4-port OC3/POS IR Eng3 release B
4OC3X/POS-LR-LC-B	3.6.0	GSR 4-port OC3/POS IR Eng3 release B
4OC3X/POS-MM-MJ-B	3.6.0	GSR 4-port OC3/POS MM Eng3 release B
4OC48/POS-SR-SC	3.6.0	4 Port (Quad) Enhanced OC-48 Short Reach SC Connector Line Card
4XOC48POS/RPR	3.6.0	4-port OC48/STM16 POS/RPR Shared Port Adapter = SPA-4XOC48POS/RPR
6CT3-SMB	3.6.0	6-port Channelized DS3-to-DS1 Line Card, SMB connector
6DS3-SMB	3.6.0	6 Port Copper DS3 Interface Line Card
8FE-FX-SC	3.6.0	8-Port Fast Ethernet Line Card
8FE-TX-RJ45	3.6.0	8-Port Fast Ethernet Line Card
8FE-TX-RJ45-B	3.6.1	8-port 100baseTX, RJ45 connector type, version B
8OC3X/POS-IR-LC-B	3.6.0	GSR 8-port OC3/POS IR Eng3 release B

Table 6-72 Supported Modules for Cisco XR 12000 Series—Cisco Prime Network 3.9 (continued)

Module Name	Product_Version	Module Description
8OC3X/POS-MM-MJ-B	3.6.0	GSR 8-port OC3/POS MM Eng3 release B
8X1FE-V2	3.6.0	8-port Fast Ethernet Shared Port Adapter V2 = SPA-8X1FE-V2
BUS_BOARD	3.6.0	GSR16 BUS BOARD (16) =
CHOC12/DS1-IR-SC	3.6.0	Cisco 12000 Series 1-Port Channelized OC-12c/STM-4
COPPER-12DS3	3.6.0[1]	12 Port Copper DS3 Interface Line Card
CRS-16-ALARM	3.6.0	Cisco CRS-1 Series 16 Slots Alarm Board = CRS-16-ALARM
EPA-GE/FE	3.6.0	Modular Gigabit/Fast Ethernet card for GSR
GSR10-AC-PDU	3.6.0	Cisco 12410 AC Power Distribution Unit (spare)
GSR10-ADVNCD-CSC	3.6.0	12010 Advanced Clock Scheduler Card
GSR10-ADVNCD-SFC	3.6.0	12010 Advanced Switch Fabric Card
GSR10-ALRM	3.6.0	12410, 12010 Alarm Card
GSR10-CSC	3.6.0	12410 Clock Scheduler Card
GSR10-SFC	3.6.0	Cisco 12410 Switch Fabric Card
GSR16/320-CSC	3.6.0	12416 Clock Scheduler Card
GSR16/320-SFC	3.6.0	12416 Switch Fabric Card
GSR16/80-CSC	3.6.0	Cisco 12016 80 Gbps GSR Scheduler/Fabric
GSR16/80-SFC	3.6.0	Cisco 12016 80 GbpsGSR Switch Fabric
GSR16-ALRM	3.6.0	Cisco 12016 GSR Alarm Card
GSR16-BLOWER	3.6.0	Cisco 12016, 12416 Blower
GSR4/80-AC	3.6.2	GSR 12404 AC Power Supply - cevPowerSupply12404AC
GSR6-ADVNCD-CSC	3.6.0	12006 Advanced Clock Scheduler Card
GSR6-ALRM	3.6.0	12406, 12006 Alarm Card
GSR6-BLOWER	3.6.0	12406, 12006 Blower
GSR6-CSC	3.6.0	Cisco 12406 Clock Scheduler Card
GSR6-SFC	3.6.0	Cisco 12406 Switch Fabric Card
GSR8-CSC/ALRM	3.6.0	Cisco 12008 GSR Scheduler/Fabric/Alarm
GSR-8FE-FX	3.6.0	8 port Fast Ethernet card with Fiber Interface
GSR8-SFC	3.6.0	Switch Fabric
GSR-ALARM10	3.6.0	GSR Alarm module
GSR-ALARM16	3.6.0	GSR-Alarm
GSR-BUS-BOARD16	3.6.0	GSR Bus Board for Power distribution
GSR-CLOCK-OC192	3.6.0	GSR Clock Scheduler

Table 6-72 Supported Modules for Cisco XR 12000 Series—Cisco Prime Network 3.9 (continued)

Module Name	Product_Version	Module Description
GSR-CSC	3.6.0	GSR Clock Scheduler Card
GSR-CSC10	3.6.0	GSR 12410 Clock scheduler
GSR-CSC16	3.6.0	GSR Clock Scheduler
GSR-CSC16-OC192	3.6.0	GSR 12406 Clock Scheduler Card
GSR-E48-ATM-4OC12-SM-IR-SC	3.6.0	GSR Edge Engine 48, ATM, 4 ports OC12/STM4 Single Mode Intermediate Reach Line Card
GSR-E48-POS-16OC3-SM-IR-LC	3.6.0	16 Port OC3 SM Intermediate Reach POS
GSR-E48-POS-OC48-SM-LR-SC	3.6.0	GSR 12406 Switch Fabric Card
GSR-E-OC192-SM-SR-SC	3.6.0	Enhanced 1 Port OC 192 Short Reach 2 FC Connector Line Card.
GSR-E-QOC48-SM-LR-SC	3.6.0	GSR Edge 4 Port Packet over Sonet OC-48, Single Mode, Long Reach, SC Connector card
GSR-E-QOC48-SM-SR-SC	3.6.0	4 Port Enhanced OC 48 Short Reach SC Connector Line Card
GSR-PA-3GE	3.6.0	GSR 3 port Port Adapter
GSR-RP	3.6.0	GSR RoMman Recovery
GSR-SFC	3.6.0	GSR Switch Fabric Card
GSR-SFC16	3.6.0	Switch Fabric Card
GSR-SFC16-OC192	3.6.0	GSR 12406 Switch Fabric Card
OC12/SRP-IR-SC-B	3.6.0	2 Port OC-12 Single Mode SRP Intermediate Reach Line Card
OC12/SRP-MM-SC-B	3.6.0	2 Port OC-12 Multi Mode SRP Line Card
OC48E/POS-LR-SC	3.6.0	1-Port OC-48/STM-16 SONET/SDH 1550 nm long-reach with SC Connector
OC48E/POS-SR-SC	3.6.0	1-Port OC-48/STM-16 SONET/SDH 1310 nm short-reach with SC Connector
OC-48E/POS-SR-SC-B	3.6.0	2 Port Packet Over Sonet OC-48, Single Mode, Short Reach, SC Connector Card
OC48X/POS-LR-SC	3.6.0	One-Port OC-48c/STM-16c POS/SDH ISE Line Card, Long Reach
OC48X/POS-SR-SC	3.6.0	One-Port OC-48c/STM-16c POS/SDH ISE Line Card, Short Reach
POS-EN-QOC48-SM-LR-FC	3.6.0	4 Port (Quad) Enhanced OC-48 Long Reach FC Connector Line Card
POS-EN-QOC48-SM-LR-SC	3.6.0	4 Port (Quad) Enhanced OC-48 Long Reach SC Connector Line Card
PRP-1	3.6.0	Performance Route Processor-1

Table 6-72 Supported Modules for Cisco XR 12000 Series—Cisco Prime Network 3.9 (continued)

Module Name	Product_Version	Module Description
PRP-2	3.6.0	Cisco XR 12000 and 12000 Series Performance Router Processor-2
PRP-3	3.6.6	Cisco XR 12000 and 12000 Series Performance Router Processor-3
PRP-4	3.6.0	Cisco XR 12000 and 12000 Series Performance Router Processor-4
SFP-GE-L	3.6.7	1000BASE-LH/LX pluggable transceiver
SFP-GE-S	3.6.7	1000BASE-Sx Short wavelength gigabit ethernet SFP.
SFP-GE-Z	3.6.7	1000BASE-Zx Extended reach gigabit ethernet SFP.
SFP-OC48-IR1	3.6.1	OC-48c/STM-16 pluggable intermediate-reach (15 km) transceiver module, 1310-nm wavelength, LC connector
SFP-OC48-LR2	3.6.1	OC-48c/STM-16 pluggable long-reach (80 km) transceiver module, 1550-nm wavelength, LC connector
SPA-10X1GE	3.6.0	10-port 1 GbE Shared Port Adapter
SPA-10X1GE-V2	3.6.2	Cisco 10-Port Gigabit Ethernet Shared Port Adapter
SPA-1X10GE-L-V2	3.6.0	Cisco 1-Port 10GE LAN-PHY Shared Port Adapter
SPA-1XCHOC12/DS0	3.6.7	1-port OC12 Channelized DS0 line card
SPA-1XCHOC48/DS3	3.6.2	1-Port Channelized STM-16/OC-48 SPA.
SPA-1XCHSTM1/OC3	3.6.1	1-port Channelized STM-1/OC-3c to DS0 Shared Port Adapter.
SPA-1XOC12-ATM-V2	3.6.2	1-port OC12c SFP Optics ATM Shared Port Adapter
SPA-1XOC192POS-VSR	3.6.0	1-port OC192/STM64 POS VSR Optics Shared Port Adapter
SPA-1XOC3-ATM-V2	3.6.2	1-port OC3c SFP Optics ATM Shared Port Adapter
SPA-1XOC48POS/RPR	3.6.0	Port OC-48c/STM-16c POS/RPR Shared Port Adapter
SPA-1XTENGE-XFP	3.6.0	1-port 10Gigabit Ethernet Shared Port Adapter XFP based
SPA-1XTENGE-XFP-V2	3.6.0	Cisco 1-Port 10 Gigabit Ethernet Shared Port Adapter
SPA-2CHT3-CE-ATM	3.6.2	2-port Channelized T3/E3 ATM + Circuit Emulation Shared Port Adapter
SPA-2X1GE	3.6.0	2 ports Gigabit Ethernet Shared Port Adapters
SPA-2X1GE-V2	3.6.1	2 ports Gigabit Ethernet Shared Port Adapters
SPA-2XCT3/DS0	3.6.1	2-port Channelized T3 to DS0 Shared Port Adapter
SPA-2XOC12-POS	3.6.0	2-Port OC-3c/STM-1 and OC-12c/STM-4 POS SPA
SPA-2XOC48POS/RPR	3.6.0	2-port OC48/STM16 POS/RPR Shared Port Adapters

Table 6-72 Supported Modules for Cisco XR 12000 Series—Cisco Prime Network 3.9 (continued)

Module Name	Product_Version	Module Description
SPA-2XT3/E3	3.6.1	2-port Clear Channel T3/E3 Shared Port Adapter
SPA-3XOC3-ATM-V2	3.6.4	3-port OC3c SFP Optics ATM Shared Port Adapter
SPA-4XCT3/DS0	3.6.0	4-port Channelized T3 to DS0 Shared Port Adapter
SPA-4XOC12-POS	3.6.0	4-port OC-12/STM-4 POS Shared Port Adapters
SPA-4XOC3-POS-V2	3.6.3	4-Port OC-3c/STM-1 POS SPA
SPA-4XT3/E3	3.6.1	4-port Clear Channel T3/E3 Shared Port Adapter
SPA-5X1GE	3.6.0	5-Port Gigabit Ethernet SPA
SPA-5X1GE-V2	3.6.0	5-Port Gigabit Ethernet SPA
SPA-8X1FE-TX-V2	3.6.0	8-port 10/100 Ethernet SPA TX (Fugu ASIC)
SPA-8X1GE	3.6.0	8-port Gigabit Ethernet Shared Port Adapter_V2
SPA-8XCHT1/E1	3.6.1	8-port Channelized T1/E1 to DS0 Shared Port Adapter
SPA-8XFE-TX	3.6.0	8-port 10/100 Ethernet SPA with RJ-45
SPA-8XOC12-POS	3.6.0	8-Port OC-12c/STM-4 Multirate POS SPA
SPA-IPSEC-2G-2	3.6.1	Cisco XR 12000 Series IPsec VPN Shared Port Adapter
SPA-OC192POS-LR	3.6.0	1-port OC192/STM64 POS/RPR SMLR Optics
SPA-OC192POS-VSR	3.6.0	1-port OC192/STM64 POS/RPR VSR Optics
SPA-OC192POS-XFP	3.6.0	1-port OC192/STM64 POS/RPR XFP Optics Shared Port Adapter with XFP-10GLR-OC192SR
SPA-OC192RPR-XFP	3.6.0	1-port OC192/STM64 POS/RPR XFP Optics Shared Port Adapter = SPA-OC192RPR-XFP
SSRP-OC48-SM-LR	3.6.0	1 Port OC-48 SRP Single Mode Long Reach Line Card
SSRP-OC48-SM-SR	3.6.0	1 Port OC-48 SRP Single Mode Short Reach Line Card
XR-PRP-2	3.6.1	Cisco XR 12000 and 12000 Series Performance Router Processor-2
SPA-8XOC3-POS	Cisco-ANA-3.7.x-DP5	8-port OC-3c/STM-1c POS SPA
SPA-1X10GE-L-ITUC	Cisco-ANA-3.7.x-DP7	Cisco 1-port 10 Gigabit Ethernet DWDM Shared Port Adapter V2
PRP3-SMDC	Cisco-ANA-3.7.x-DP10, Cisco-ANA-3.8-DP1	Cisco XR 12000 Service Module Daughter Card for PRP-3

Table 6-72 Supported Modules for Cisco XR 12000 Series—Cisco Prime Network 3.9 (continued)

Module Name	Product_Version	Module Description
SPA-1CHOC3-CE-ATM	3.7.x-DP11,PrimeNetwork-3.8.X-DP2	1-port Channelized OC3/STM-1 ATM + Circuit Emulation SP
SPA-24CHT1-CE-ATM	3.7.x-DP11,PrimeNetwork-3.8.X-DP2	24-port Channelized T1/E1 ATM + Circuit Emulation Shared Port Adapter
SPA-2CHT3-CE-ATM	3.7.x-DP11,PrimeNetwork-3.8.X-DP2	2-port Channelized T3/E3 ATM + Circuit Emulation Shared Port Adapter
SFP-OC3-IR1	3.7.x-DP11,PrimeNetwork-3.8.X-DP2	OC-3/STM-1 pluggable intermediate-reach (15 km) transceiver module, 1310-nm wavelength, LC connector
SFP-OC3-LR1	3.7.x-DP11,PrimeNetwork-3.8.X-DP2	OC-3/STM-1 pluggable long-reach (40 km) transceiver module, 1310-nm wavelength, LC connector
SFP-OC3-LR2	3.7.x-DP11,PrimeNetwork-3.8.X-DP2	OC-3/STM-1 pluggable long-reach (80 km) transceiver module, 1550-nm wavelength, LC connector
SFP-OC3-SR	3.7.x-DP11,PrimeNetwork-3.8.X-DP2	OC-3/STM-1 pluggable short-reach (2 km) transceiver module, 1310-nm wavelength, LC connector
SFP-OC3-MM	3.7.x-DP11,PrimeNetwork-3.8.X-DP2	OC-12/STM-4 pluggable short-reach (2 km) transceiver module, 1310-nm wavelength, MMF, LC connector

[1]Derecated OID

Cisco XR 12000 Series—Supported Technologies

The following technologies are supported by the Cisco XR 12000 Series in Cisco Prime Network 3.9:

- IP, page 6-199
- Routing Protocols, page 6-202
- Ethernet, page 6-205
- ATM, page 6-213

- PPP, page 6-219
- HDLC, page 6-220
- SONET/SDH, page 6-220
- TDM/DSx, page 6-222
- MPLS, page 6-226
- MPLS-TE, page 6-228
- VPN (VRF), page 6-233
- PWE3, page 6-235
- Security, page 6-237
- Hardware, page 6-238
- Serial, page 6-242
- Additional Technologies, page 6-243
- IPoDWDM, page 6-243
- LocalSwitching, page 6-245
- BFD, page 6-246
- Carrier Ethernet, page 6-247
- CDP, page 6-249
- Discovery Protocol, page 6-249
- Ethernet OAM, page 6-250
- 6PE, page 6-264
- IPSec, page 6-266

Cisco XR 12000 Series—Supported Service Events

Table 6-73 Supported Service Events for Cisco XR 12000 Series—Cisco Prime Network 3.9

Event Name	Product_Version	Expedited
Active IP Interfaces Found	3.6.0	Y
All IP Interfaces Down	3.6.1	Y
BGP process up	3.6.0	N
Card Down	3.6.0	Y
Card In	3.6.0	Y
Card Out	3.6.0	Y
Card Up	3.6.0	Y
Cloud Problem	3.6.0	N
CPU utilization exceeded upper threshold	3.6.0	N
Device Unreachable	3.6.0	N

Table 6-73 Supported Service Events for Cisco XR 12000 Series—Cisco Prime Network 3.9

Event Name	Product_Version	Expedited
Device Unsupported	3.6.0	N
DS1 Path link down due to Admin down	3.7	N
DS1 Path link down due to Oper down	3.7	N
DS1 Path link Up	3.7	N
EFP Admin Down	3.6.7	N
EFP down due to error disabled	3.6.7	N
Interface status down flapping	3.6.0	Y
Keepalive configured	3.6.0	N
Keepalive not configured	3.6.0	N
Layer 2 Tunnel Down	3.6.0	N
Link up	3.6.0	N
Memory utilization exceeded upper threshold	3.6.0	N
MLPPP Operationaly down	3.7	N
MLPPP Up	3.7	N
Module Unsupported	3.6.0	N
Rx utilization exceeded upper threshold	3.6.0	N
Sonet Path link down due to Admin down	3.7	N
Sonet Path link down due to Oper down	3.7	N
Sonet Path link Up	3.7	N
SONET Path up	3.7	N
Tx utilization exceeded upper threshold	3.6.0	N
VSI Down	3.6.7	N
pluggable transceiver out	Prime Network 3.8	N
fan-tray down	Prime Network 3.8	N
fan-tray out	Prime Network 3.8	N

Table 6-73 Supported Service Events for Cisco XR 12000 Series—Cisco Prime Network 3.9

Event Name	Product_Version	Expedited
power-supply down	Prime Network 3.8	N
power-supply out	Prime Network 3.8	N

Cisco CRS Carrier Routing System

This section includes the following information about Cisco CRS routers (for information on the NE types supported in Cisco Prime Network 3.9, see Cisco CRS Carrier Routing System):

- Cisco CRS—Supported Software Versions, page 6-106
- Cisco CRS—Supported Topologies, page 6-107
- Cisco CRS—Supported Modules, page 6-108
- Cisco CRS—Supported Technologies, page 6-118
- Cisco CRS—Supported Service Events, page 6-119
- Cisco CRS—Additional Information, page 6-120

Cisco CRS—Supported Software Versions

Table 6-74 Supported Software Versions for Cisco CRS—Cisco Prime Network 3.9

Software Version	Product_Version
IOX 3.4.0	3.6.0
IOX 3.4.1	3.6.0
IOX 3.4.3	3.6.3
IOX 3.5.1	3.6.1
IOX 3.6.0	3.6.3[1]
IOX 3.6.1	3.6.3
IOX 3.6.2	3.6.4
IOX 3.6.3	3.6.7
IOX 3.7.0	3.6.4
IOX 3.7.1	3.6.4
IOX 3.8.0	3.6.6[2]
IOX 3.8.1	3.6.7
IOX 3.8.2	3.7

Table 6-74 Supported Software Versions for Cisco CRS—Cisco Prime Network 3.9 (continued)

Software Version	Product_Version
IOX 3.8.4	3.7.1
IOX 3.9.0	3.7[3]
IOX 3.9.1	3.7.0.1
IOX3.9.2	3.7.1.1.0
IOX4.0.0	3.7.1.1.0[4]
IOX4.0.1	3.7.2
IOX4.0.3	Cisco-ANA-3.7.x-DP4
IOX4.0.4	Cisco-ANA-3.7.x-DP9
IOX4.1.0	Cisco-ANA-3.7.x-DP4
IOX4.1.1	Cisco-ANA-3.7.x-DP6
IOX4.1.2	Cisco-ANA-3.7.x-DP10, PrimeNetwork-3.8.X-DP1
IOX4.2.0	Cisco-ANA-3.7.x-DP11, PrimeNetwork-3.8.X-DP2

[1, 2, 3]ANA recognizes all maintenance builds in this IOS XR release train.

[4]ANA recognizes all maintenance builds starting from this IOS XR release train.

Cisco CRS—Supported Topologies

Table 6-75 Supported Topologies for Cisco CRS—Cisco Prime Network 3.9

Topology Type	Link Type	Product_Version
BGP	BGP	3.6.0
Ethernet	Ethernet	3.6.0
MPLS	MPLS	3.6.0
PPP/HDLC	PPP or HDLC	3.6.0
PWE3 (Martini)	Tunnel	3.6.2
VPN (VRF)	VPN	3.6.1
Physical Layer	Physical Layer	3.6.0

Table 6-75 Supported Topologies for Cisco CRS—Cisco Prime Network 3.9 (continued)

Topology Type	Link Type	Product_Version
LAG	LAG	3.6.0
BFD	BFD	3.7.1

Cisco CRS—Supported Modules

Table 6-76 Supported Modules for Cisco CRS—Cisco Prime Network 3.9

Module Name	Product_Version	Module Description
1-100GBE	3.7.1.1.0	Cisco CRS-3 1-port 100 Gigabit Ethernet Interface Module
14X10GBE-WL-XFP	3.7.1.1.0	Cisco CRS-3 14-Port 10GE LAN/WAN-PHY Interface Module
16OC48-POS/DPT	3.6.0	Cisco CRS-1 Series 16xOC48/STM16 POS/DPT Interface Module
1OC768-DPSK/C	3.6.6	Cisco CRS-1 1xOC768 DPSK+ (C-band) DWDM PLIM
1OC768-DPSK/C-E	3.6.2	1-Port OC-768/STM-256c (DPSK C-band EVEN) DWDM PLIM
1OC768-DPSK/C-O	3.6.2	1-Port OC-768/STM-256c (DPSK C-band ODD) DWDM PLIM
1OC768-ITU/C	3.6.0	Cisco CRS-1 1-Port OC-768c/STM-256c (C-band) DWDM PLIM
1OC768-POS-SR	3.6.1	1-port OC-768c/STM-256c PLIM, with short-reach optics (POS)
20-1GE-FLEX	3.6.7	Cisco CRS-1 Series 20x1GE Flexible Interface Module
20X10GBE-WL-XFP	3.7.1.1.0	Cisco CRS-3 20x10GbE LAN/WAN Physical Interface Module
2-10GE-WL-FLEX	3.6.7	Cisco CRS-1 Series 2x10GE WAN/LAN Flexible Interface Module
4-10GBE-WL-XFP	3.7.1	Cisco CRS-1 Series 4xGbE WAN/LAN XFP Interface Module
4-10GE	3.6.7	Cisco-CRS1 series 4x10GE interface module
4-10GE-ITU/C	3.6.0	Module Crs1 4x10 Ge CDwdm Plim
42-1GE	3.6.7	Cisco CRS-1 Series 42x1GE Interface Module
4OC192-ITU/C	3.6.1	Module Crs 1 4 ports OC192 C Dwdm Plim
4OC192-POS/DPT-IR	3.6.0	Cisco CRS-1 Series 4xOC192/STM64 POS/DPT Interface Module/IR

Table 6-76 Supported Modules for Cisco CRS—Cisco Prime Network 3.9 (continued)

Module Name	Product_Version	Module Description
4OC192-POS/DPT-LR	3.6.0	Cisco CRS-1 4xOC-192/STM-64 POS/DPT Interface Module/LR
4OC192-POS/DPT-SR	3.6.0	Cisco CRS-1 Series 4xOC192/STM64 POS/DPT Interface Module/SR
4OC192-POS/DPT-VS	3.6.0	Cisco CRS-1 4xOC-192/STM-64 POS/DPT Interface Module/VS
8-10GBE	3.6.0	8x10 Gigabite Ethernet port
8-10GBE-WL-XFP	3.7.1	Cisco CRS-1 8-port 10GbE LAN/WAN-PHY Interface Module
8XOC3-OC12-PO	3.6.0	SPA POS 8XOC12 Card
CFP-100G-LR4	3.7.1.1.0	100GBASE-LR4 CFP Module for SMF
CRS-16-AC-RECT	3.6.1	Cisco CRS-1 Series AC Pwr Rectifier for 16 slot LCC and FCC
CRS-16-ALARM	3.6.0	Cisco CRS-1 Series 16 Slots Alarm
CRS-16-ALARM-C	3.7	Cisco CRS-1 Series 16 Slots Modular Power System Alarm Board
CRS-16-DC-PEM	3.6.1	DC power entry module for line card chassis
CRS-16-DC-PEM=	3.6.4	Cisco CRS-1 Series DC PEM for 16 slot LCC and FCC
CRS-16-FC/D	3.6.1	Cisco CRS-1 Series 16 Slots Fabric Card/Dual
CRS-16-FC/M	3.6.0	Cisco CRS-1 Series 16 Slots Fabric Card / Multi
CRS-16-FC/S	3.6.0	Cisco CRS-1 Series 16 Slots Fabric Card Single
CRS-16-FC140/S	3.7.1.1.0	Cisco CRS-1 Series 16 Slots Fabric Card / Single (140G)
CRS-16FCC-PSH-AC	3.7	Cisco CRS-1 Series Modular AC Power Shelf for FCC
CRS-16FCC-PSH-DC	3.7	Cisco CRS-1 Series Modular DC Power Shelf for FCC
CRS-16-LCC	3.6.0	16 slots Line Card Chassis
CRS-16-LCC-FAN-CT	3.6.0	Cisco CRS-1 Series LC Chassis Fan Controler
CRS-16-LCC-FAN-TR	3.6.1	Cisco CRS-1 16 Slots FCC fan tray with fans
CRS-16-LCC-PS-ACD	3.6.1	AC Delta power shelf for line card chassis
CRS-16-LCC-PS-ACD=	3.6.4	Cisco CRS-1 Series AC Delta Power Shelf for 16 Slots LCC
CRS-16-LCC-PS-ACW	3.6.1	AC Wye power shelf for line card chassis
CRS-16-LCC-PS-ACW=	3.6.4	Cisco CRS-1 Series AC Wye Power Shelf for 16 Slots LCC
CRS-16-LCC-PS-DC	3.6.1	DC power shelf for line card chassis
CRS-16-LCC-PS-DC=	3.6.4	Cisco CRS-1 Series DC Power Shelf for 16 Slots LCC

Table 6-76 Supported Modules for Cisco CRS—Cisco Prime Network 3.9 (continued)

Module Name	Product_Version	Module Description
CRS-16LCC-PSH-AC	3.7	Cisco CRS-1 Series Modular AC Power Shelf for 16 Slots LCC
CRS-16LCC-PSH-DC	3.7	Cisco CRS-1 Series Modular DC Power Shelf for 16 Slots LCC
CRS-16-RP	3.6.0	Module Crs1 16 slots RP
CRS-16-RP-B	3.6.0	Module Crs1 16 slots RP - B
CRS1-SIP-800	3.6.0	Module Crs1 SPA Interface Card
CRS-4-AC-SHELF	3.6.1	Cisco CRS-1 Series AC Power Shelf for CRS-4
CRS-4-AC-SUPPLY	3.6.1	AC power supplies
CRS-4-CH	3.6.0	4 slots Chassis
CRS-4-DC-INPUT	3.6.1	Cisco CRS-1 Series 4 Slot DC Input Shelf
CRS-4-DC-PIM	3.6.4	Cisco CRS-1 Series 4 Slot DC Power Input Module
CRS-4-DC-SUPPLY	3.6.1	DC power supplies
CRS-4-FAN-TR	3.6.1	Cisco CRS-1 4 Slots FCC fan tray with fans
CRS-4-FC	3.6.1	CRS-1 4-Slot Fabric Card
CRS-4-FC140/S	3.7.1.1.0	Cisco CRS Series 4 Slot Fabric Card / Single(140G)
CRS-4-LCC	3.6.0	Cisco CRS-1 Series 4 Slots Line Card Chassis
CRS-8-AC-RECT	3.6.1	Cisco CRS-1 Series AC Pwr Rectifier for 8 slot LCC
CRS-8-DC-PEM	3.6.1	Cisco CRS-1 Series DC Power Entry Module for 8 slot LCC
CRS-8-FC/M	3.6.1	Cisco CRS-1 Series 8 Slots Fabric Card/Multi
CRS-8-FC/S	3.6.0	Cisco CRS-1 Series 8 Slots Fabric Card Single
CRS-8-FC140/S	3.7.1.1.0	Cisco CRS Series 8 Slot Fabric Card / Single(140G)
CRS-8-LCC	3.6.0	8 slots Line Card Chassis
CRS-8-LCC-ACD	3.6.1	Power Supply Crs 1 8 Slots AC Delta
CRS-8-LCC-ACW	3.6.1	Power Supply Crs 1 8 Slots ACW
CRS-8-LCC-DC	3.6.1	Cisco CRS-1 Series 8 slots with redundant DC power
CRS-8-LCC-FAN-TR	3.6.1	Cisco CRS-1 8 Slots FCC fan tray with fans
CRS-8-LCC-PDU-ACD	3.6.1	Cisco CRS-1 Series AC Delta PDU for CRS-8 LCC
CRS-8-LCC-PDU-ACW	3.6.1	AC Wye PDU
CRS-8-LCC-PDU-DC	3.6.1	Cisco CRS-1 Series DC PDU for CRS-8 LCC
CRS-8-PSH-AC	3.7	Cisco CRS-1 Series Modular AC Power Shelf for 8 Slots LCC
CRS-8-PSH-DC	3.7	Cisco CRS-1 Series Modular DC Power Shelf for 8 Slots LCC
CRS-8-RP	3.6.0	Module Crs1 8 slots RP
CRS-CGSE-PLIM	3.7.1	Cisco CRS-1 Carrier Grade Service Engine

Table 6-76 Supported Modules for Cisco CRS—Cisco Prime Network 3.9 (continued)

Module Name	Product_Version	Module Description
CRS-DRP	3.6.0	Cisco CRS-1 Series Distributed Route Processor
CRS-DRP-B-CPU	3.6.0	Cisco CRS-1 Series Distributed Route Processor CPU board revision B
CRS-DRP-B-PLIM	3.6.0	Cisco CRS-1 Series Distributed Route Processor Front Accsry
CRS-DRP-CPU	3.6.0	Cisco CRS-1 Series Distributed Route Processor
CRS-DRP-PLIM	3.6.0	Cisco CRS-1 Series Distributed Route Processor Front Accsry
CRS-FCC	3.6.0	Cisco CRS-1 Series Fabric Card Chassis Only
CRS-FCC-FAN-TR	3.6.1	Cisco CRS-1 FCC fan tray with fans
CRS-FCC-LED	3.6.1	Fiber module LED card
CRS-FCC-OIM-1S	3.6.1	Optical single interface module (OIM)
CRS-FCC-OIM-2S	3.6.1	Optical dual interface module (OIM)
CRS-FCC-PS-ACD	3.6.1	CRS-1 Fabric Chassis AC Delta Power Supply
CRS-FCC-PS-ACW	3.6.1	CRS-1 Fabric Chassis AC Wye Option
CRS-FCC-PS-DC	3.6.1	CRS-1 Fabric Chassis DC Power Option
CRS-FCC-SC/GEW	3.6.1	Cisco CRS-1 Series FC Chassis Shelf/Fan/Enet cntr
CRS-FCC-SC-22GE	3.6.1	CRS-1 fan controllers
CRS-FCC-SC-GE	3.6.1	2-port Shelf controller Gigabit Ethernet
CRS-FCC-SFC	3.6.1	Switch fabric card (fabric card chassis) S2 switch fabric cards
CRS-FP140	3.7.1.1.0	Cisco CRS Series Forwarding Processor 140G
CRS-FP40	3.6.7	Cisco CRS-1 Series Forwarding Processor 40G
CRS-MSC	3.6.0	Cisco CRS-1 Series Modular Service Card
CRS-MSC-140G	3.7.1.1.0	Cisco CRS Series Modular Series Card 140G
CRS-MSC-20G-B	3.6.0	Cisco CRS-1 Series Modular Service Card B - 20G licenses
CRS-MSC-40G-B	3.6.0	Cisco CRS-1 Series Modular Service Card B - 40G licenses
CRS-MSC-B	3.6.0	Cisco CRS-1 Series Modular Services Card revision B
CRS-PM-AC	3.7	Cisco CRS-1 Series AC Power Module 2100W
CRS-PM-DC	3.7	Cisco CRS-1 Series DC Power Module 2100W
CRS-XENPAK-10GB-LR	3.6.0	XENPAK 10GBASE-LR Optics Module
OC192/POS-IR-SC	3.6.2	Cisco One-Port OC-192c/STM-64c POS Line Card 1550 nm IR, SC

Table 6-76 Supported Modules for Cisco CRS—Cisco Prime Network 3.9 (continued)

Module Name	Product_Version	Module Description
SFP-GE-L	3.7.1.1.0	1000BASE-LX/LH SFP transceiver module for MMF and SMF, 1300-nm wavelength, extended operating temperature range and DOM support, dual LC/PC connector
SFP-GE-S	3.6.7	1000BASE-SX SFP transceiver module for MMF, 850-nm wavelength, extended operating temperature range and DOM support
SFP-GE-T	3.6.7	1000BASE-TX SFP (DOM), MMF, 550/220m
SFP-GE-Z	3.6.7	1000BASE-ZX SFP transceiver module SMF, 1550-nm wavelength, extended operating temperature range and DOM support
SFP-OC12-IR1	3.7.1.1.0	OC-12/STM-4 pluggable intermediate-reach (15 km) transceiver module, 1310-nm wavelength
SFP-OC12-LR1	3.7.1.1.0	OC-12/STM-4 pluggable long-reach (40 km) transceiver module, 1310-nm wavelength, LC connector
SFP-OC12-LR2	3.7.1.1.0	OC-12/STM-4 pluggable long-reach (80 km) transceiver module, 1550-nm wavelength, LC connector
SFP-OC12-MM	3.7.1.1.0	OC-12/STM-4 pluggable short-reach (2 km) transceiver module, 1310-nm wavelength, MMF, LC connector
SFP-OC12-SR	3.7.1.1.0	OC-12/STM-4 pluggable short-reach (2 km) transceiver module, 1310-nm wavelength, LC connector
SFP-OC3-IR1	3.7.1.1.0	OC-3/STM-1 pluggable intermediate-reach (15 km) transceiver module, 1310-nm wavelength, LC connector
SFP-OC3-LR1	3.7.1.1.0	OC-3/STM-1 pluggable long-reach (40 km) transceiver module, 1310-nm wavelength, LC connector
SFP-OC3-LR2	3.7.1.1.0	OC-3/STM-1 pluggable long-reach (80 km) transceiver module, 1550-nm wavelength, LC connector
SFP-OC3-MM	3.7.1.1.0	OC-3/STM-1 pluggable short-reach (2 km) transceiver module, 1310-nm wavelength, MMF, LC connector
SFP-OC3-SR	3.7.1.1.0	OC-3/STM-1 pluggable short-reach (2 km) transceiver module, 1310-nm wavelength, LC connector
SPA-10X1GE	3.6.1	10-Port Gigabit Ethernet SPA
SPA-10X1GE-V2	3.6.1	10-Port Gigabit Ethernet SPA

Table 6-76 Supported Modules for Cisco CRS—Cisco Prime Network 3.9 (continued)

Module Name	Product_Version	Module Description
SPA-1X10GE-L-V2	3.6.1	Cisco 1-Port 10 Gigabit Ethernet Shared Port Adapter
SPA-1X10GE-WL-V2	3.6.7	Cisco 1-Port 10-Gigabit Ethernet LAN/WAN PHY Shared Port Adapter
SPA-1XCHOC12/DS0	3.6.2	Cisco 1-port Channelized OC12/STM-4 SPA
SPA-1XOC12-ATM-V2	3.6.4	Cisco 1-Port OC12c/STM4c ATM Shared Port Adapter
SPA-1XOC192POS-VSR	3.6.0	Cisco 1-Port OC-192c/STM-64c POS/RPR Shared Port Adapter with VSR Optics
SPA-1XOC192POS-XFP	3.6.0	Cisco 1-Port OC-192c/STM-64c POS/RPR Shared Port Adapter with XFP Optics
SPA-1XOC3-ATM-V2	3.6.7	Cisco 1-Port OC3c/STM1c ATM Shared Port Adapter
SPA-1XOC48POS/RPR	3.6.1	Port OC-48c/STM-16c POS/RPR Shared Port Adapter
SPA-1XTENGE-XFP	3.6.1	1-port 10 Gigabit Ethernet Shared Port Adapter XFP based
SPA-1XTENGE-XFP-V2	3.6.0	1-port 10GbE Shared Port Adapter XFP based V2 = SPA-1XTENGE-XFP-V2
SPA-2X1GE	3.6.1	2 ports Gigabit Ethernet Shared Port Adapters
SPA-2X1GE-V2	3.6.1	2 ports Gigabit Ethernet Shared Port Adapters
SPA-2XCT3/DS0	3.6.1	Cisco 2-Port Channelized T3 (DS0) Shared Port Adapter
SPA-2XOC12-POS	3.6.1	Cisco 2-Port OC-12c/STM-4 POS SPA
SPA-2XOC48POS/RPR	3.6.1	2-Port OC-48c/STM-16c POS/RPR Shared Port Adapter
SPA-2XT3/E3	3.6.1	2-Port T3/E3 Serial SPA
SPA-3XOC3-ATM-V2	3.6.4	Cisco 2-Port Clear Channel T3/E3 Shared Port Adapter
SPA-4XOC12-POS	3.6.1	Cisco 4-Port OC-12c/STM-4 POS SPA
SPA-4XOC3-POS	3.6.0	Cisco 4-Port OC-3c/STM-1c POS Shared Port Adapter
SPA-4XOC3-POS-V2	3.6.0	4-Port OC-3c/STM-1 POS SPA
SPA-4XOC48POS/RPR	3.6.1	Port OC-48c/STM-16c POS/RPR Shared Port Adapter
SPA-4XT3/E3	3.6.1	Cisco 4-Port Clear Channel T3/E3 Shared Port Adapter
SPA-5X1GE	3.6.1	5-Port Gigabit Ethernet SPA
SPA-5X1GE-V2	3.6.1	5-Port Gigabit Ethernet SPA
SPA-8X1GE	3.6.0	8-port Gigabit Ethernet Shared Port Adapter
SPA-8X1GE-V2	3.6.1	Cisco 8-Port Gigabit Ethernet Shared Port Adapter

Table 6-76 Supported Modules for Cisco CRS—Cisco Prime Network 3.9 (continued)

Module Name	Product_Version	Module Description
SPA-8XCHT1/E1	3.6.1	8-Port Channelized T1/E1 SPA
SPA-8XOC12-POS	3.6.1	Cisco 8-Port OC-12c/STM-4 POS SPA
SPA-8XOC3-POS	3.6.0	8-Port OC-3c/STM-1 POS SPA
SPA-OC192POS-LR	3.6.1	Cisco 1-Port OC-192c/STM-64c POS/RPR Shared Port Adapter with LR Optics
SPA-OC192POS-VSR	3.6.1	Cisco 1-Port OC-192c/STM-64c POS/RPR Shared Port Adapter with VSR Optics
SPA-OC192POS-XFP	3.6.0	Cisco 1-Port OC-192c/STM-64c POS/RPR Shared Port Adapter with XFP Optics
XENPAK-10GB-ER+	3.7.1.1.0	10GBASE-ER XENPAK transceiver module for SMF, 1550-nm wavelength, SC duplex connector
XENPAK-10GB-LR+	3.7.1	10GBASE-LR XENPAK transceiver module for SMF, 1310-nm wavelength, SC duplex connector (supports DOM)
XFP-10GER-192IR+	3.6.7	Multirate XFP module for 10GBASE-IR and OC192 IR
XFP10GER-192IR-L	3.7.1.1.0	Cisco Multirate XFP transciever module for 10GBASE-ER and OC-192/STM-64 IR-2 XFP Module for SMF, low power (2.5W)
XFP-10GER-OC192IR	3.6.7	Cisco multirate XFP transceiver module for 10GBASE-ER Ethernet and OC-192/STM-64 intermediate-reach (IR-2) Packet-over-SONET/SDH (POS) applications, SMF, dual LC connector
XFP10GLR-192SR-L	3.7.1.1.0	Cisco multirate XFP transceiver module for 10GBASE-LR Ethernet and OC-192/STM-64 short-reach (SR-1) Packet-over-SONET/SDH (POS) applications, SMF, dual LC connector, low power
XFP-10GLR-OC192SR	3.7.1.1.0	Cisco multirate XFP transceiver module for 10GBASE-LR Ethernet and OC-192/STM-64 short-reach (SR-1) Packet-over-SONET/SDH (POS) applications, SMF, dual LC connector
XFP-10G-MM-SR	3.7.1.1.0	Cisco 10GBASE-SR Ethernet XFP transceiver module for MMF, dual LC connector
XFP-10GZR-OC192LR	3.6.7	Cisco multirate XFP transceiver module for 10GBASE-ZR Ethernet and OC-192/STM-64 long-reach Packet-over-SONET/SDH (POS) applications, SMF, dual LC connector
DWDM-XENPAK-30.33	Cisco-ANA-3.7.x-DP3	10GBASE-DWDM 1530.33 nm XENPAK (100-GHz ITU grid)

Table 6-76 Supported Modules for Cisco CRS—Cisco Prime Network 3.9 (continued)

Module Name	Product_Version	Module Description
DWDM-XENPAK-31.12	Cisco-ANA-3.7.x-DP3	10GBASE-DWDM 1531.12 nm XENPAK (100-GHz ITU grid)
DWDM-XENPAK-31.90	Cisco-ANA-3.7.x-DP3	10GBASE-DWDM 1531.90 nm XENPAK (100-GHz ITU grid)
DWDM-XENPAK-32.68	Cisco-ANA-3.7.x-DP3	10GBASE-DWDM 1532.68 nm XENPAK (100-GHz ITU grid)
DWDM-XENPAK-34.25	Cisco-ANA-3.7.x-DP3	10GBASE-DWDM 1534.25 nm XENPAK (100-GHz ITU grid)
DWDM-XENPAK-35.04	Cisco-ANA-3.7.x-DP3	10GBASE-DWDM 1535.04 nm XENPAK (100-GHz ITU grid)
DWDM-XENPAK-35.82	Cisco-ANA-3.7.x-DP3	10GBASE-DWDM 1535.82 nm XENPAK (100-GHz ITU grid)
DWDM-XENPAK-36.61	Cisco-ANA-3.7.x-DP3	10GBASE-DWDM 1536.61 nm XENPAK (100-GHz ITU grid)
DWDM-XENPAK-38.19	Cisco-ANA-3.7.x-DP3	10GBASE-DWDM 1538.19 nm XENPAK (100-GHz ITU grid)
DWDM-XENPAK-38.98	Cisco-ANA-3.7.x-DP3	10GBASE-DWDM 1538.98 nm XENPAK (100-GHz ITU grid)
DWDM-XENPAK-39.77	Cisco-ANA-3.7.x-DP3	10GBASE-DWDM 1539.77 nm XENPAK (100-GHz ITU grid)
DWDM-XENPAK-40.56	Cisco-ANA-3.7.x-DP3	10GBASE-DWDM 1540.56 nm XENPAK (100-GHz ITU grid)
DWDM-XENPAK-42.14	Cisco-ANA-3.7.x-DP3	10GBASE-DWDM 1542.14 nm XENPAK (100-GHz ITU grid)
DWDM-XENPAK-42.94	Cisco-ANA-3.7.x-DP3	10GBASE-DWDM 1542.94 nm XENPAK (100-GHz ITU grid)
DWDM-XENPAK-43.73	Cisco-ANA-3.7.x-DP3	10GBASE-DWDM 1543.73 nm XENPAK (100-GHz ITU grid)

Table 6-76 Supported Modules for Cisco CRS—Cisco Prime Network 3.9 (continued)

Module Name	Product_Version	Module Description
DWDM-XENPAK-44.53	Cisco-ANA-3.7.x-DP3	10GBASE-DWDM 1544.53 nm XENPAK (100-GHz ITU grid)
DWDM-XENPAK-46.12	Cisco-ANA-3.7.x-DP3	10GBASE-DWDM 1546.12 nm XENPAK (100-GHz ITU grid)
DWDM-XENPAK-46.92	Cisco-ANA-3.7.x-DP3	10GBASE-DWDM 1546.92 nm XENPAK (100-GHz ITU grid)
DWDM-XENPAK-47.72	Cisco-ANA-3.7.x-DP3	10GBASE-DWDM 1547.72 nm XENPAK (100-GHz ITU grid)
DWDM-XENPAK-48.51	Cisco-ANA-3.7.x-DP3	10GBASE-DWDM 1548.51 nm XENPAK (100-GHz ITU grid)
DWDM-XENPAK-50.12	Cisco-ANA-3.7.x-DP3	10GBASE-DWDM 1550.12 nm XENPAK (100-GHz ITU grid)
DWDM-XENPAK-50.92	Cisco-ANA-3.7.x-DP3	10GBASE-DWDM 1550.92 nm XENPAK (100-GHz ITU grid)
DWDM-XENPAK-51.72	Cisco-ANA-3.7.x-DP3	10GBASE-DWDM 1551.72 nm XENPAK (100-GHz ITU grid)
DWDM-XENPAK-52.52	Cisco-ANA-3.7.x-DP3	10GBASE-DWDM 1552.52 nm XENPAK (100-GHz ITU grid)
DWDM-XENPAK-54.13	Cisco-ANA-3.7.x-DP3	10GBASE-DWDM 1554.13 nm XENPAK (100-GHz ITU grid)
DWDM-XENPAK-54.94	Cisco-ANA-3.7.x-DP3	10GBASE-DWDM 1554.94 nm XENPAK (100-GHz ITU grid)
DWDM-XENPAK-55.75	Cisco-ANA-3.7.x-DP3	10GBASE-DWDM 1555.75 nm XENPAK (100-GHz ITU grid)
DWDM-XENPAK-56.55	Cisco-ANA-3.7.x-DP3	10GBASE-DWDM 1556.55 nm XENPAK (100-GHz ITU grid)
DWDM-XENPAK-58.17	Cisco-ANA-3.7.x-DP3	10GBASE-DWDM 1558.17 nm XENPAK (100-GHz ITU grid)

Table 6-76 Supported Modules for Cisco CRS—Cisco Prime Network 3.9 (continued)

Module Name	Product_Version	Module Description
DWDM-XENPAK-58.98	Cisco-ANA-3.7.x-DP3	10GBASE-DWDM 1558.98 nm XENPAK (100-GHz ITU grid)
DWDM-XENPAK-59.79	Cisco-ANA-3.7.x-DP3	10GBASE-DWDM 1559.79 nm XENPAK (100-GHz ITU grid)
DWDM-XENPAK-60.61	Cisco-ANA-3.7.x-DP3	10GBASE-DWDM 1560.61 nm XENPAK (100-GHz ITU grid)
CRS-16-PRP-12G	Cisco-ANA-3.7.x-DP4	Cisco CRS Series 16-Slot Performance Route Processor (12 GB)
CRS-8-PRP-12G	Cisco-ANA-3.7.x-DP4	Cisco CRS Series 4/8-Slot Line Card Chassis Performance Route Processor (6 GB)
CRS-16-PRP-6G	Cisco-ANA-3.7.x-DP4	Cisco CRS Series 16-Slot Performance Route Processor (6 GB)
CRS-8-PRP-6G	Cisco-ANA-3.7.x-DP4	Cisco CRS Series 4/8-Slot Line Card Chassis Performance Route Processor (12 GB)
CRS-16-FC140/M	Cisco-ANA-3.7.x-DP4	Cisco CRS Series 16 Slots Fabric Card / Multi(140G)
CRS-FCC-SFC-140	Cisco-ANA-3.7.x-DP4	Cisco CRS Series fabric Card Chassis Switch fabric Card(140G)
CRS-LSP	Cisco-ANA-3.7.x-DP6	Cisco CRS Series Label Switch Processor 140G
CRS-16-LCC-B	Cisco-ANA-3.7.x-DP10	CRS 16 Slots Line Card Chassis for CRS-16/S-B
CRS-16-ALARM-B	Cisco-ANA-3.7.x-DP10	CRS 16 Slots Alarm Board for CRS-16/S-B
CRS-16-FAN-CT	Cisco-ANA-3.7.x-DP10	CRS 16 Slots Alarm Board for CRS-16/S-B
CRS-16-PWRSH-DC	Cisco-ANA-3.7.x-DP10	CRS 16 slots DC Power Shelf for CRS-16/S-B

Table 6-76 Supported Modules for Cisco CRS—Cisco Prime Network 3.9 (continued)

Module Name	Product_Version	Module Description
CRS-16-PWRSH-AC	Cisco-ANA-3.7.x-DP10	CRS 16 slots AC Power Shelf for CRS-16/S-B
CRS-16-FANTRAY	Cisco-ANA-3.7.x-DP10	CRS 16 Slot Fan Tray for CRS-16/S-B

Cisco CRS—Supported Technologies

The following technologies are supported by the Cisco CRS in Cisco Prime Network 3.9:

- IP, page 6-199
- Routing Protocols, page 6-202
- Ethernet, page 6-205
- ATM, page 6-213
- PPP, page 6-219
- HDLC, page 6-220
- SONET/SDH, page 6-220
- TDM/DSx, page 6-222
- MPLS, page 6-226
- MPLS-TE, page 6-228
- VPN (VRF), page 6-233
- PWE3, page 6-235
- Security, page 6-237
- Hardware, page 6-238
- Serial, page 6-242
- Additional Technologies, page 6-243
- IPoDWDM, page 6-243
- LocalSwitching, page 6-245
- BFD, page 6-246
- Carrier Ethernet, page 6-247
- CDP, page 6-249
- Discovery Protocol, page 6-249
- Ethernet OAM, page 6-250
- CGN, page 6-254
- 6PE, page 6-264

Cisco CRS—Supported Service Events

Table 6-77 Supported Service Events for Cisco CRS—Cisco Prime Network 3.9

Event Name	Product_Version	Expedited
Active IP Interfaces Found	3.6.0	Y
All IP Interfaces Down	3.6.0	Y
BGP process up	3.6.0	N
Card Down	3.6.0	Y
Card In	3.6.0	Y
Card Out	3.6.0	Y
Card Up	3.6.0	Y
CGN statistics dropsPortLimitIn2Out higher threshold exceeded	3.7.1	N
CGN statistics dropsResourceDepletionIn2Out higher threshold exceeded	3.7.1	N
CGN statistics dropsSystemLimitIn2Out higher threshold exceeded	3.7.1	N
CGN statistics fwdIn2Out higher threshold exceeded	3.7.1	N
CGN statistics fwdOut2In higher threshold exceeded	3.7.1	N
CPU utilization exceeded upper threshold	3.6.0	N
Device Unsupported	3.6.0	N
EFP down due to error disabled	3.6.7	N
Layer 2 Tunnel Down	3.6.0	N
Link up	3.6.0	N
Memory utilization exceeded upper threshold	3.6.0	N
Module Unsupported	3.6.0	N
MPLS Black Hole found	3.6.0	N
pluggable transceiver out	Prime Network 3.8	N
fan-tray down	Prime Network 3.8	N

Table 6-77 Supported Service Events for Cisco CRS—Cisco Prime Network 3.9 (continued)

Event Name	Product_Version	Expedited
fan-tray out	Prime Network 3.8	N
power-supply down	Prime Network 3.8	N
power-supply out	Prime Network 3.8	N

Cisco CRS—Additional Information

This section contains additional information about Cisco CRS-1 and CRS-3 and includes the following topics:

- Cisco Carrier Routing System (CRS) Prerequisite, page 6-120
- SDR Support for CRS, page 6-120
- Multichassis Support for CRS, page 6-121

Cisco Carrier Routing System (CRS) Prerequisite

As a prerequisite for the CRS VNE, install the Cisco IOS XR Manageability Package on top of the IOS-XR version. In addition, the device configuration must contain the command, **xml agent tty**.

When creating the SNMP community, the SystemOwner should be specified.

SDR Support for CRS

Secure Domain Router (SDR) is supported as a separate, independent VNE, with its own IP and login sequence. When adding an SDR to Prime Network, it is treated like any other network element, that is, it is added as a new VNE using Cisco Prime Network Administration. The SDR IP address is attached to the active DRP of the SDR (or to its virtual IP, if it exists).

As a prerequisite for the CRS VNE:

1. Install the Cisco IOS XR Manageability Package on top of the IOS-XR version (XR 3.4 and 3.4.1).
2. Add the command `xml agent tty` to the device configuration
3. When creating the SNMP community string, specify the SystemOwner (for SDRs, specify the SDROwner; LROwner on XR 3.5.x and below).
4. Define the IP address, snmp read community and telnet login sequence. When adding the telnet login sequence, add the user as an admin user (*username*@admin, e.g. cisco@admin).

Cisco ANA uses the management network (if available) to manage the devices. The CRS platform assigns specific management interfaces on the RP modules (DRP for an SDR). In order to retrieve the IP address of these management interfaces, login to the device and run the command `show ipv4 interface brief | include Mgmt` as shown in the following example:

```
RP/0/RP1/CPU0:P1_CRS8#show ipv4 interface brief | include Mgmt
MgmtEth0/RP1/CPU0/0            1.60.34.104     Up                  Up
MgmtEth0/4/CPU0/0              unassigned      Shutdown            Down
MgmtEth0/4/CPU1/0              unassigned      Shutdown            Down
```

In multiple (D)RP environments, there is an option to configure a virtual management interface and assign an IP address to it, so that the device is reachable via the same IP address no matter which (D)RP is active. In this environment, each (D)RP has its own IP address but it is not used in order to access the device. In order to get the virtual IP address, login to the device and run the command `show running-config ipv4 virtual address` as shown in the example:

```
DRP/0/3/CPU0:CRS-PE1#show running-config ipv4 virtual address
ipv4 virtual address 10.52.123.11 255.255.255.0
```

If the SDR is managed in-band the management IP address should be supplied by the customer. The owner SDR (namely, the main router) presents all the modules that are installed on the chassis, excluding the ports that belong to other SDRs. The VNE of the SDR only displays the modules that are associated with the SDR in the Inventory window of Cisco Prime Network Vision. It does not display the fabric, fan and power supply (namely, the shared modules).

Multichassis Support for CRS

Multichassis support is available in Prime Network for 16-slot CRS devices. The chassis functions purely as a container for the shelves, which are treated as individual chassis and are numbered incrementally starting with 0. Expanding a shelf displays the modules that are installed on that shelf.

Because each shelf is treated as a chassis, chassis parameters such as description, serial number, status, and type are displayed for each shelf, not for the actual chassis in which the shelves are installed.

When adding a multichassis device to Prime Network, it is treated like any other network element, namely, it is added as a new VNE using Cisco Prime Network Administration.

Cisco ASR 9000 Series Aggregation Services Routers

This section includes the following information about Cisco ASR 9000 routers (for information on the NE types supported in Cisco Prime Network 3.9, see Cisco ASR 9000 Series Aggregation Services Routers):

- Cisco ASR 9000—Supported Software Versions, page 6-121
- Cisco ASR 9000—Supported Topologies, page 6-122
- Cisco ASR 9000—Supported Modules, page 6-122
- Cisco ASR 9000—Supported Technologies, page 6-132
- Cisco ASR 9000—Supported Service Events, page 6-132

Cisco ASR 9000—Supported Software Versions

Table 6-78 Supported Software Versions for Cisco ASR 9000—Cisco Prime Network 3.9

Software Version	Product_Version
IOX 3.7.2	3.6.5

Table 6-78 Supported Software Versions for Cisco ASR 9000—Cisco Prime Network 3.9

Software Version	Product_Version
IOX 3.7.3	3.6.7
IOX 3.9.0	3.7
IOX 3.9.1	3.7.1
IOX 3.9.2	3.7.1.1.0
IOX 4.0.0	3.7.1.1.0
IOX 4.0.1	3.7.2
IOX 4.0.3	3.7.X-DP4
IOX 4.0.4	3.7.X-DP9
IOX 4.1.0	3.7.X-DP4
IOX 4.1.1	3.7.X-DP6
IOX 4.1.2	3.7.X-DP10, 3.8.X-DP1
IOX 4.2.0	3.7.X-DP11, 3.8.X-DP2

Cisco ASR 9000—Supported Topologies

Table 6-79 Supported Topologies for Cisco ASR 9000—Cisco Prime Network 3.9

Topology Type	Link Type	Product_Version
BGP	BGP	3.6.5
Ethernet	Ethernet	3.6.5
Physical Layer	Physical Layer	3.6.5
LAG	LAG	3.6.5
BFD	BFD	3.7.1
VPN (IPv6)	VPN	3.7.1

Cisco ASR 9000—Supported Modules

Table 6-80 Supported Modules for Cisco ASR 9000—Cisco Prime Network 3.9

Module Name	Product_Version	Module Description
A9K-1.5KW-DC	3.6.6	ASR-9K 1.5kW DC Power Module
A9K-16T/8-B	3.7.0.1	16-Port 10GE Medium Queue DX Line Card, Requires SFP+s
A9K-2KW-DC	3.6.6	ASR-9K 2kW DC Power Module

Table 6-80 Supported Modules for Cisco ASR 9000—Cisco Prime Network 3.9 (continued)

Module Name	Product_Version	Module Description
A9K-2T20GE-B	3.7	2-Port 10GE, 20-Port GE Line Card, Requires XFPs and SFPs
A9K-2T20GE-E	3.7	2-Port 10GE, 20-Port GE Extended LC, Req. XFPs and SFPs
A9K-2T20GE-L	3.7.1.1.0	2-Port 10GE, 20-Port GE Low Queue Combo Line Card, Requires XFPs for 10GE, SFPs for GE
A9K-3KW-AC	3.6.5	ASR-9K 3kW AC Power Module
A9K-40GE-B	3.6.5	40-Port, GE Line Card, Requires SFPs
A9K-40GE-E	3.6.5	40-Port, GE Line Card, Extended Memory, Requires SFPs
A9K-40GE-L	3.7	40-Port GE Low Queue Line Card, Requires SFPs
A9K-4T-B	3.6.5	4-Port,10GE Line Card, Requires XFPs
A9K-4T-E	3.6.6	Cisco ASR 9000 Series 4-Port Ten Gigabit Ethernet, extended memory
A9K-4T-L	3.7	4-Port 10GE Low Queue Line Card, Requires XFPs
A9K-8T/4-B	3.6.6	Cisco ASR 9000 Series 8-Port Ten Gigabit Ethernet DX
A9K-8T/4-E	3.6.6	Cisco ASR 9000 Series 8-Port Ten Gigabit Ethernet DX, extended memory
A9K-8T/4-L	3.7	8-Port 10GE DX Low Queue Line Card, Requires XFPs
A9K-8T-B	3.7	8-Port 10GE Line Card, Requires XFPs
A9K-8T-E	3.7	8-Port 10GE Extended Line Card, Requires XFPs
A9K-8T-L	3.7.1	8-Port 10GE Low Queue Line Card, Requires XFPs
A9K-RSP-4G	3.6.6	Route Switch Processor 4G Memory Hard Disc Drive
A9K-RSP-8G	3.7.2	Route Swith Processor 8G memory
A9K-SIP-700	3.7	Cisco ASR 9000 SPA Interface Processor-700
ASR-9006-FAN	3.6.6	Cisco ASR 9000 Series 6-Slot Fan Tray
ASR-9010-FAN	3.6.5	Cisco ASR 9000 Series 10-Slot Fan Tray
CWDM-SFP-1470	3.7.2	Cisco CWDM SFP 1470 nm; Gigabit Ethernet and 1G/2G FC
CWDM-SFP-1490	3.7.2	Cisco CWDM SFP 1490 nm; Gigabit Ethernet and 1G/2G FC
CWDM-SFP-1510	3.7.2	Cisco CWDM SFP 1510 nm; Gigabit Ethernet and 1G/2G FC
CWDM-SFP-1530	3.7.2	Cisco CWDM SFP 1530 nm; Gigabit Ethernet and 1G/2G FC
CWDM-SFP-1550	3.7.2	Cisco CWDM SFP 1550 nm; Gigabit Ethernet and 1G/2G FC

Table 6-80 Supported Modules for Cisco ASR 9000—Cisco Prime Network 3.9 (continued)

Module Name	Product_Version	Module Description
CWDM-SFP-1570	3.7.2	Cisco CWDM SFP 1570 nm; Gigabit Ethernet and 1G/2G FC
CWDM-SFP-1590	3.7.2	Cisco CWDM SFP 1590 nm; Gigabit Ethernet and 1G/2G FC
CWDM-SFP-1610	3.7.2	Cisco CWDM SFP 1610 nm; Gigabit Ethernet and 1G/2G FC
DWDM-SFP-3033	3.7.2	1000BASE-DWDM 1530.33 nm SFP (100-GHz ITU grid)
DWDM-SFP-3112	3.7.2	1000BASE-DWDM 1531.12 nm SFP (100-GHz ITU grid)
DWDM-SFP-3190	3.7.2	1000BASE-DWDM 1531.90 nm SFP (100-GHz ITU grid)
DWDM-SFP-3268	3.7.2	1000BASE-DWDM 1532.68 nm SFP (100-GHz ITU grid)
DWDM-SFP-3425	3.7.2	1000BASE-DWDM 1534.25 nm SFP (100-GHz ITU grid)
DWDM-SFP-3504	3.7.2	1000BASE-DWDM 1535.04 nm SFP (100-GHz ITU grid)
DWDM-SFP-3582	3.7.2	1000BASE-DWDM 1535.82 nm SFP (100-GHz ITU grid)
DWDM-SFP-3661	3.7.2	1000BASE-DWDM 1536.61 nm SFP (100-GHz ITU grid)
DWDM-SFP-3819	3.7.2	1000BASE-DWDM 1538.19 nm SFP (100-GHz ITU grid)
DWDM-SFP-3898	3.7.2	1000BASE-DWDM 1538.98 nm SFP (100-GHz ITU grid)
DWDM-SFP-3977	3.7.2	1000BASE-DWDM 1539.77 nm SFP (100-GHz ITU grid)
DWDM-SFP-4056	3.7.2	1000BASE-DWDM 1540.56 nm SFP (100-GHz ITU grid)
DWDM-SFP-4214	3.7.2	1000BASE-DWDM 1542.14 nm SFP (100-GHz ITU grid)
DWDM-SFP-4294	3.7.2	1000BASE-DWDM 1542.94 nm SFP (100-GHz ITU grid)
DWDM-SFP-4373	3.7.2	1000BASE-DWDM 1543.73 nm SFP (100-GHz ITU grid)
DWDM-SFP-4453	3.7.2	1000BASE-DWDM 1544.53 nm SFP (100-GHz ITU grid)
DWDM-SFP-4612	3.7.2	1000BASE-DWDM 1546.12 nm SFP (100-GHz ITU grid)

Table 6-80 Supported Modules for Cisco ASR 9000—Cisco Prime Network 3.9 (continued)

Module Name	Product_Version	Module Description
DWDM-SFP-4692	3.7.2	1000BASE-DWDM 1546.92 nm SFP (100-GHz ITU grid)
DWDM-SFP-4772	3.7.2	1000BASE-DWDM 1547.72 nm SFP (100-GHz ITU grid)
DWDM-SFP-4851	3.7.2	1000BASE-DWDM 1548.51 nm SFP (100-GHz ITU grid)
DWDM-SFP-5012	3.7.2	1000BASE-DWDM 1550.12 nm SFP (100-GHz ITU grid)
DWDM-SFP-5092	3.7.2	1000BASE-DWDM 1550.92 nm SFP (100-GHz ITU grid)
DWDM-SFP-5172	3.7.2	1000BASE-DWDM 1551.72 nm SFP (100-GHz ITU grid)
DWDM-SFP-5252	3.7.2	1000BASE-DWDM 1552.52 nm SFP (100-GHz ITU grid)
DWDM-SFP-5413	3.7.2	1000BASE-DWDM 1554.13 nm SFP (100-GHz ITU grid)
DWDM-SFP-5494	3.7.2	1000BASE-DWDM 1554.94 nm SFP (100-GHz ITU grid)
DWDM-SFP-5575	3.7.2	1000BASE-DWDM 1555.75 nm SFP (100-GHz ITU grid)
DWDM-SFP-5655	3.7.2	1000BASE-DWDM 1556.55 nm SFP (100-GHz ITU grid)
DWDM-SFP-5817	3.7.2	1000BASE-DWDM 1558.17 nm SFP (100-GHz ITU grid)
DWDM-SFP-5898	3.7.2	1000BASE-DWDM 1558.98 nm SFP (100-GHz ITU grid)
DWDM-SFP-5979	3.7.2	1000BASE-DWDM 1559.79 nm SFP (100-GHz ITU grid)
DWDM-SFP-6061	3.7.2	1000BASE-DWDM 1560.61 nm SFP (100-GHz ITU grid)
DWDM-XFP-31.12	3.7.2	10GBASE-DWDM 1531.12 nm XFP (100-GHz ITU grid)
DWDM-XFP-31.90	3.7.2	10GBASE-DWDM 1531.90 nm XFP (100-GHz ITU grid)
DWDM-XFP-32.68	3.7.2	10GBASE-DWDM 1532.68 nm XFP (100-GHz ITU grid)
DWDM-XFP-34.25	3.7.2	10GBASE-DWDM 1534.25 nm XFP (100-GHz ITU grid)
DWDM-XFP-35.04	3.7.2	10GBASE-DWDM 1535.04 nm XFP (100-GHz ITU grid)

Table 6-80 Supported Modules for Cisco ASR 9000—Cisco Prime Network 3.9 (continued)

Module Name	Product_Version	Module Description
DWDM-XFP-35.82	3.7.2	10GBASE-DWDM 1535.82 nm XFP (100-GHz ITU grid)
DWDM-XFP-36.61	3.7.2	10GBASE-DWDM 1536.61 nm XFP (100-GHz ITU grid)
DWDM-XFP-38.19	3.7.2	10GBASE-DWDM 1538.19 nm XFP (100-GHz ITU grid)
DWDM-XFP-38.98	3.7.2	10GBASE-DWDM 1538.98 nm XFP (100-GHz ITU grid)
DWDM-XFP-39.77	3.7.2	10GBASE-DWDM 1539.77 nm XFP (100-GHz ITU grid)
DWDM-XFP-40.56	3.7.2	10GBASE-DWDM 1540.56 nm XFP (100-GHz ITU grid)
DWDM-XFP-42.14	3.7.2	10GBASE-DWDM 1542.14 nm XFP (100-GHz ITU grid)
DWDM-XFP-42.94	3.7.2	10GBASE-DWDM 1542.94 nm XFP (100-GHz ITU grid)
DWDM-XFP-43.73	3.7.2	10GBASE-DWDM 1543.73 nm XFP (100-GHz ITU grid)
DWDM-XFP-44.53	3.7.2	10GBASE-DWDM 1544.53 nm XFP (100-GHz ITU grid)
DWDM-XFP-46.12	3.7.2	10GBASE-DWDM 1546.12 nm XFP (100-GHz ITU grid)
DWDM-XFP-46.92	3.7.2	10GBASE-DWDM 1546.92 nm XFP (100-GHz ITU grid)
DWDM-XFP-47.72	3.7.2	10GBASE-DWDM 1547.72 nm XFP (100-GHz ITU grid)
DWDM-XFP-48.51	3.7.2	10GBASE-DWDM 1548.51 nm XFP (100-GHz ITU grid)
DWDM-XFP-50.12	3.7.2	10GBASE-DWDM 1550.12 nm XFP (100-GHz ITU grid)
DWDM-XFP-50.92	3.7.2	10GBASE-DWDM 1550.92 nm XFP (100-GHz ITU grid)
DWDM-XFP-51.72	3.7.2	10GBASE-DWDM 1551.72 nm XFP (100-GHz ITU grid)
DWDM-XFP-52.52	3.7.2	10GBASE-DWDM 1552.52 nm XFP (100-GHz ITU grid)
DWDM-XFP-54.13	3.7.2	10GBASE-DWDM 1554.13 nm XFP (100-GHz ITU grid)
DWDM-XFP-54.94	3.7.2	10GBASE-DWDM 1554.94 nm XFP (100-GHz ITU grid)

Table 6-80 Supported Modules for Cisco ASR 9000—Cisco Prime Network 3.9 (continued)

Module Name	Product_Version	Module Description
DWDM-XFP-55.75	3.7.2	10GBASE-DWDM 1555.75 nm XFP (100-GHz ITU grid)
DWDM-XFP-56.55	3.7.2	10GBASE-DWDM 1556.55 nm XFP (100-GHz ITU grid)
DWDM-XFP-58.17	3.7.2	10GBASE-DWDM 1558.17 nm XFP (100-GHz ITU grid)
DWDM-XFP-58.98	3.7.2	10GBASE-DWDM 1558.98 nm XFP (100-GHz ITU grid)
DWDM-XFP-59.79	3.7.2	10GBASE-DWDM 1559.79 nm XFP (100-GHz ITU grid)
DWDM-XFP-60.61	3.7.2	10GBASE-DWDM 1560.61 nm XFP (100-GHz ITU grid)
DWDM-XFP-C	3.7.2	10GE Tunable DWDM XFP
GLC-BX-D	3.7	1000BASE-BX10 SFP module for single-strand SMF, 1310-nm TX/1490-nm RX wavelength
GLC-BX-U	3.7	1000BASE-BX10 SFP module for single-strand SMF, 1490-nm TX/1310-nm RX wavelength
GLC-GE-100FX	3.7.2	Cisco 100BASE-FX SFP for Gigabit SFP ports
SFP-10G-ER	3.7.2	10GBASE-ER 1550 nm SMF
SFP-GE-L	3.6.6	1000BASE-LX SFP (DOM), MMF, 550/220m
SFP-GE-S	3.6.5	1000BASE-SX SFP (DOM), MMF, 550/220m
SFP-GE-T	3.7	1000BASE-T SFP (Network Equipment Building Standards [NEBS] 3), unshielded twisted pair (UTP), 100m
SFP-GE-Z	3.6.6	1000BASE-ZX SFP (DOM), MMF, 550/220m
SFP-OC12-IR1	3.7	OC-12/STM-4 pluggable intermediate-reach (15 km) transceiver module, 1310-nm wavelength
SFP-OC12-LR1	3.7	OC-12/STM-4 pluggable long-reach (40 km) transceiver module, 1310-nm wavelength, LC connector
SFP-OC12-LR2	3.7	OC-12/STM-4 pluggable long-reach (80 km) transceiver module, 1550-nm wavelength, LC connector
SFP-OC12-MM	3.7	OC-12/STM-4 pluggable short-reach (2 km) transceiver module, 1310-nm wavelength, MMF, LC connector
SFP-OC12-SR	3.7	OC-12/STM-4 pluggable short-reach (2 km) transceiver module, 1310-nm wavelength, LC connector

Table 6-80 Supported Modules for Cisco ASR 9000—Cisco Prime Network 3.9 (continued)

Module Name	Product_Version	Module Description
SFP-OC3-IR1	3.7.2	OC-3/STM-1 pluggable intermediate-reach (15 km) transceiver module, 1310-nm wavelength, LC connector
SFP-OC3-LR1	3.7.2	OC-3/STM-1 pluggable long-reach (40 km) transceiver module, 1310-nm wavelength, LC connector
SFP-OC3-LR2	3.7.2	OC-3/STM-1 pluggable long-reach (80 km) transceiver module, 1550-nm wavelength, LC connector
SFP-OC3-MM	3.7.2	OC-3/STM-1 pluggable short-reach (2 km) transceiver module, 1310-nm wavelength, MMF, LC connector
SFP-OC3-SR	3.7.2	OC-3/STM-1 pluggable short-reach (2 km) transceiver module, 1310-nm wavelength, LC connector
SFP-OC48-IR1	3.7.2	OC-48c/STM-16 pluggable intermediate-reach (15 km) transceiver module, 1310-nm wavelength, LC connector
SFP-OC48-LR2	3.7.2	OC-48c/STM-16 pluggable long-reach (80 km) transceiver module, 1550-nm wavelength, LC connector
SFP-OC48-SR	3.7.2	OC-48c/STM-16 pluggable short-reach (2 km) transceiver module, 1310-nm wavelength, LC connector
SPA-1XCHOC48/DS3	3.7.2	1 port channelized OC48 to DS3 Shared Port Adapter
SPA-1XCHSTM1/OC3	3.7.2	1-port Channelized STM1/OC3 to DS0 SPA
SPA-2XCHOC12/DS0	3.7	2 port channelized OC12 to DS0 Shared Port Adapter
SPA-2XOC48POS/RPR	3.7.2	2-port OC 48/STM16 POS/RPR Shared Port Adapter
SPA-2XT3/E3	3.7.2	2-port Clear Channel T3/E3 SPA
SPA-4XOC3-POS-V2	3.7.2	4-port OC-3c/STM-1c POS SPA version 2
SPA-4XT3/E3	3.7.2	4-port Clear Channel T3/E3 SPA
SPA-8XOC12-POS	3.7.2	8-port OC12/STM4 POS Shared Port Adapter
SPA-8XOC3-POS	3.7.2	8-port OC-3c/STM-1c POS SPA
SPA-OC192POS-XFP	3.7.2	1-port OC192/STM64 POS/RPR XFP Optics
XFP-10GER-192IR+	3.6.6	Cisco Multirate 10GBASE-ER and OC-192/STM-64 IR-2 XFP Module
XFP-10GER-OC192IR	3.7.1	Cisco multirate XFP transceiver module for 10GBASE-ER Ethernet and OC-192/STM-64 intermediate-reach (IR-2) Packet-over-SONET/SDH (POS) applications, SMF, dual LC connector

Table 6-80 Supported Modules for Cisco ASR 9000—Cisco Prime Network 3.9 (continued)

Module Name	Product_Version	Module Description
XFP-10GLR-OC192SR	3.6.6	Multirate XFP module for 10GBASE-LR and OC192 SR-1
XFP-10G-MM-SR	3.7	Cisco 10GBASE-SR XFP transceiver module for MMF, 850-nm wavelength, dual LC connector
XFP-10GZR-OC192LR	3.6.6	Cisco multirate XFP transceiver module for 10GBASE-LR Ethernet and OC-192/STM-64 long-reach Packet-over-SONET/SDH (POS) applications, SMF, dual LC connector
DWDM-XFP-30.33	3.7.2	10GBASE-DWDM 1530.33 nm XFP (100-GHz ITU grid)
SFP-10G-LR	Cisco-ANA-3.7.2-DP3	10GBASE-LR SFP+ transceiver module for SMF, 1310-nm wavelength, LC duplex connector
SFP-10G-SR	Cisco-ANA-3.7.2-DP3	10GBASE-SR SFP+ transceiver module for MMF, 850-nm wavelength, LC duplex connector
A9K-SIM-100	Cisco-ANA-3.7.x-DP4	ASR9K Advanced Video Streaming Module
SPA-4XCT3/DS0	Cisco-ANA-3.7.x-DP4	4-port Channelized T3 to DS0 Shared Port Adapter
SPA-8XCHT1/E1	Cisco-ANA-3.7.x-DP4	8-port Channelized T1/E1 to DS0 Shared Port Adapter
A9K-24X10GE-TR	PrimeNetwork-3.8.X-DP2, Cisco-ANA3.7.X-DP11	Cisco ASR 9000 24-Port 10 GE Packet Transport Optimized Line Card, Requires SFP+ optics
A9K-24X10GE-SE	PrimeNetwork-3.8.X-DP2, Cisco-ANA3.7.X-DP11	Cisco ASR 9000 24-Port 10 GE Service Edge Optimized Line Card, Requires SFP+ optics
XFP-10GLR-OC192SR	PrimeNetwork-3.8.X-DP2, Cisco-ANA3.7.X-DP11	Cisco 10 Gigabit Ethernet LR (10 km) Optics

Table 6-80 Supported Modules for Cisco ASR 9000—Cisco Prime Network 3.9 (continued)

Module Name	Product_Version	Module Description
SPA-3XOC3-ATM-V2	PrimeNetwork-3.8.X-DP2, Cisco-ANA3.7.X-DP11	3-port OC3c SFP Optics ATM Shared Port Adapter
SPA-1XOC12-ATM-V2	PrimeNetwork-3.8.X-DP2, Cisco-ANA3.7.X-DP11	1-port OC12c SFP Optics ATM Shared Port Adapter
SPA-1CHOC3-CE-ATM	PrimeNetwork-3.8.X-DP2, Cisco-ANA3.7.X-DP11	1-port Channelized OC3/STM-1 ATM + Circuit Emulation SP
SPA-1XOC3-ATM-V2	PrimeNetwork-3.8.X-DP2, Cisco-ANA3.7.X-DP11	1-port OC3c SFP Optics ATM Shared Port Adapter
A9K-RSP440-TR	PrimeNetwork-3.8.X-DP2, Cisco-ANA3.7.X-DP11	Route Switch Processor 440 G bandwidth optimized for packet transport
A9K-RSP440-SE	PrimeNetwork-3.8.X-DP2, Cisco-ANA3.7.X-DP11	Route Switch Processor 440 G bandwidth optimized for service edge
A9K-MPA-2X10GE	PrimeNetwork-3.8.X-DP2, Cisco-ANA3.7.X-DP11	ASR 9000 2-port 10GE Modular Port Adapter

Table 6-80 Supported Modules for Cisco ASR 9000—Cisco Prime Network 3.9 (continued)

Module Name	Product_Version	Module Description
A9K-MPA-20X1GE	PrimeNetwork-3.8.X-DP2, Cisco-ANA3.7.X-DP11	ASR 9000 20-port 1GE Modular Port Adapter
A9K-MPA-4X10GE	PrimeNetwork-3.8.X-DP2, Cisco-ANA3.7.X-DP11	ASR 9000 4-port 10GE Modular Port Adapter
A9K-MOD80-TR	PrimeNetwork-3.8.X-DP2, Cisco-ANA3.7.X-DP11	ASR 9000 MOD80 Modular Linecard, Packet Transport Optimized
A9K-MOD80-SE	PrimeNetwork-3.8.X-DP2, Cisco-ANA3.7.X-DP11	ASR 9000 MOD80 Modular Linecard, Service Edge Optimized
A9K-MOD160-SE	PrimeNetwork-3.8.X-DP2, Cisco-ANA3.7.X-DP11	ASR 9000 MOD160 Modular Linecard, Service Edge Optimized
A9K-2X100GE-SE	PrimeNetwork-3.8.X-DP2, Cisco-ANA3.7.X-DP11	ASR 9000 2-port 100GE, Service Edge Optimized LC
A9K-2X100GE-TR	PrimeNetwork-3.8.X-DP2, Cisco-ANA3.7.X-DP11	ASR 9000 2-port 100GE, Packet Transport Optimized LC

Cisco ASR 9000—Supported Technologies

The following technologies are supported by the Cisco ASR 9000 in Cisco Prime Network 3.9:

- IP, page 6-199
- Routing Protocols, page 6-202
- Ethernet, page 6-205
- PPP, page 6-219
- HDLC, page 6-220
- SONET/SDH, page 6-220
- TDM/DSx, page 6-222
- MPLS, page 6-226
- MPLS-TE, page 6-228
- MPLS-TP, page 6-231
- VPN (VRF), page 6-233
- PWE3, page 6-235
- Security, page 6-237
- Hardware, page 6-238
- Serial, page 6-242
- LocalSwitching, page 6-245
- BFD, page 6-246
- Carrier Ethernet, page 6-247
- CDP, page 6-249
- Discovery Protocol, page 6-249
- Ethernet OAM, page 6-250
- AccessGatewayService, page 6-262
- 6PE, page 6-264
- MLACP, page 6-265

Cisco ASR 9000—Supported Service Events

Table 6-81 Supported Service Events for Cisco ASR 9000—Cisco Prime Network 3.9

Event Name	Product_Version	Expedited
Active IP Interfaces Found	3.6.5	Y
All IP Interfaces Down	3.6.5	Y
BFD neighbor loss	3.6.5	N
BGP link up	3.6.5	Y
BGP process down	3.6.5	N

Table 6-81 Supported Service Events for Cisco ASR 9000—Cisco Prime Network 3.9 (continued)

Event Name	Product_Version	Expedited
BGP process up	3.6.5	N
Card Down	3.6.5	Y
Card In	3.6.5	Y
Card Out	3.6.5	Y
Card Up	3.6.5	Y
CPU utilization exceeded upper threshold	3.6.5	N
Device Unsupported	3.6.5	N
Dropped packet rate exceeded upper threshold	3.6.5	N
EFP down due to error disabled	3.6.7	N
Link up	3.6.5	N
Memory utilization exceeded upper threshold	3.6.5	N
Module Unsupported	3.6.5	N
Rx utilization exceeded upper threshold	3.6.5	N
Tx utilization exceeded upper threshold	3.6.5	N
VSI Down	3.6.7	N
pluggable transceiver out	Prime Network 3.8	N
fan-tray down	Prime Network 3.8	N
fan-tray out	Prime Network 3.8	N
power-supply down	Prime Network 3.8	N
power-supply out	Prime Network 3.8	N

Cisco ASR 1000 Series Routers

This section includes the following information about Cisco ASR 1000 Series routers (for information on the NE types supported in Cisco Prime Network 3.9, see Cisco ASR 1000 Series Routers):

- Cisco ASR 1000 Series—Supported Software Versions, page 6-134
- Cisco ASR 1000 Series—Supported Topologies, page 6-135
- Cisco ASR 1000 Series—Supported Modules, page 6-136
- Cisco ASR 1000 Series—Supported Technologies, page 6-142
- Cisco ASR 1000 Series—Supported Service Events, page 6-142

Cisco ASR 1000 Series—Supported Software Versions

Table 6-82 Supported Software Versions for Cisco ASR 1000 Series—Cisco Prime Network 3.9

Software Version	Product_Version
XE 2.2.3 aka 12.2(33)XNB3	[1]
XE 2.3.0 aka 12.2(33)XNC	[2]
XE 2.3.1 aka 12.2(33)XNC1	[3]
XE 2.3.2 aka 12.2(33)XNC2	[4]
XE 2.4.0 aka 12.2(33)XND	[5]
XE 2.4.1 aka 12.2(33)XND1	[6]
XE 2.5.0 aka 12.2(33)XNE	[7]
XE 2.2.1 aka 12.2(33)XNB1	[8]
XE 2.2.2 aka 12.2(33)XNB2	[9]
XE 2.5.1 aka 12.2(33)XNE1	[10]
XE 2.4.2 aka 12.2(33)XND2	
XE 2.4.3 aka 12.2(33)XND3	
XE 2.6.0 aka 12.2(33)XNF	
XE 3.1.0 S aka 15.0(1)S	
XE 3.1.1 S aka 15.0(1)S1	
XE 3.2.0S aka 15.1(1)S	
XE 3.1.2S aka 15.0(1)S2	

Table 6-82 Supported Software Versions for Cisco ASR 1000 Series—Cisco Prime Network 3.9

Software Version	Product_Version
XE 3.1.3S aka 15.0(1)S3	
XE 3.3.0S aka 15.1(2)S	
XE 3.3.1S a.k.a 15.1(2)S1	
XE 3.2.2S aka 15.1(1)S2	
XE 2.6.2 aka 12.2(33)XNF2	
XE 2.6.1 aka 12.2(33)XNF1	
XE 2.5.2 aka 12.2(33)XNE2	
XE 2.4.4 aka 12.2(33)XND4	
XE 3.2.1S aka 15.1(1)S1	
XE3.4.1S aka 15.1(3)S1	
XE3.4.2S aka 15.1(3)S2	
XE3.5.0S -- 15.2(1)S	
XE3.3.2S aka 15.1(2)S2	
XE3.1.4S aka 15.0(1)S4	
XE3.4.0S -- 15.1(3)S	
XE3.6.0S aka 15.2(2)S	
XE3.5.1S aka 15.2(1)S1	
XE3.4.3S aka 15.1(3)S3	

[1, 2, 4, 6, 9, 10]ANA models pluggable ports for this IOS version.

[3, 7, 8]ANA recognizes all maintenance builds in this IOS release train.ANA models pluggable ports for this IOS version.

[5]ANA recognizes all maintenance builds in this IOS release trainANA models pluggable ports for this IOS version.

Cisco ASR 1000 Series—Supported Topologies

Table 6-83 Supported Topologies for Cisco ASR 1000 Series—Cisco Prime Network 3.9

Topology Type	Link Type	Product_Version
BGP	BGP	
Ethernet	Ethernet	
MPLS	MPLS	

Table 6-83 Supported Topologies for Cisco ASR 1000 Series—Cisco Prime Network 3.9

Topology Type	Link Type	Product_Version
Physical Layer	Physical Layer	
BFD	BFD	
VPN (IPv6)	VPN	

Cisco ASR 1000 Series—Supported Modules

Table 6-84 Supported Modules for Cisco ASR 1000 Series—Cisco Prime Network 3.9

Module Name	Product_Version	Module Description
4XGE-BUILT-IN		Cisco ASR1002 4 Port, Gigabit Ethernet SPA Card
ASR1000-ESP10		Cisco ASR 1000 10Gbps Embedded Services Processor
ASR1000-ESP20		Cisco ASR1000 Embedded Services Processor, 20G,Crypto
ASR1000-ESP40		Cisco ASR1000 Embedded Services Processor, 40Gbps
ASR1000-ESP5	[1]	ASR1K Embedded Services Processor,5Gbps,Crypto,ASR1002 only
ASR1000-RP1	[2]	Cisco ASR1000 Route Processor 1, 2GB DRAM
ASR1000-RP2		Cisco ASR1000 Route Processor 2
ASR1000-SIP10	[3]	Cisco ASR1000 SPA Interface Processor 10
ASR1000-SIP40		Cisco ASR1000 SPA Interface Processor 40
ASR1002-PWR-AC		Cisco ASR 1002 AC Power Supply
ASR1002-PWR-DC		Cisco ASR1002 DC Power Supply
ASR1002-RP1		Cisco ASR1002 Route Processor 1
ASR1002-SIP10		Cisco ASR1002 SIP 10
ASR1004-PWR-AC		Cisco ASR 1004 AC Power Supply
ASR1004-PWR-DC		Cisco ASR 1004 DC Power Supply
ASR1006-PWR-AC		Cisco ASR1006 AC Power Supply
ASR1006-PWR-DC		Cisco ASR 1006 DC Power Supply
ASR1013-PWR-AC		Cisco ASR1013 AC Power Supply
ASR1013-PWR-DC		Cisco ASR1013 DC Power Supply
CWDM-SFP-1470		Cisco CWDM SFP 1470 nm;Gigabit Ethernet and 1G/2G FC
CWDM-SFP-1490		Cisco CWDM SFP 1490 nm;Gigabit Ethernet and 1G/2G FC

Table 6-84 Supported Modules for Cisco ASR 1000 Series—Cisco Prime Network 3.9 (continued)

Module Name	Product_Version	Module Description
CWDM-SFP-1510		Cisco CWDM SFP 1510 nm;Gigabit Ethernet and 1G/2G FC
CWDM-SFP-1530		Cisco CWDM SFP 1530 nm;Gigabit Ethernet and 1G/2G FC
CWDM-SFP-1550		Cisco CWDM SFP 1550 nm;Gigabit Ethernet and 1G/2G FC
CWDM-SFP-1570		Cisco CWDM SFP 1570 nm;Gigabit Ethernet and 1G/2G FC
CWDM-SFP-1590		Cisco CWDM SFP 1590 nm;Gigabit Ethernet and 1G/2G FC
CWDM-SFP-1610		Cisco CWDM SFP 1610 nm;Gigabit Ethernet and 1G/2G FC
DWDM-SFP-3033		Cisco 1000BASE-DWDM SFP 1530.33 nm
DWDM-SFP-3112		Cisco 1000BASE-DWDM SFP 1531.12 nm
DWDM-SFP-3190		Cisco 1000BASE-DWDM SFP 1531.90 nm
DWDM-SFP-3268		Cisco 1000BASE-DWDM SFP 1532.68 nm
DWDM-SFP-3425		Cisco 1000BASE-DWDM SFP 1534.25 nm
DWDM-SFP-3504		Cisco 1000BASE-DWDM SFP 1535.04 nm
DWDM-SFP-3582		Cisco 1000BASE-DWDM SFP 1535.82 nm
DWDM-SFP-3661		Cisco 1000BASE-DWDM SFP 1536.61 nm
DWDM-SFP-3819		Cisco 1000BASE-DWDM SFP 1538.19 nm
DWDM-SFP-3898		Cisco 1000BASE-DWDM SFP 1539.98 nm
DWDM-SFP-3977		Cisco 1000BASE-DWDM SFP 1539.77 nm
DWDM-SFP-4056		Cisco 1000BASE-DWDM SFP 1540.56 nm
DWDM-SFP-4214		Cisco 1000BASE-DWDM SFP 1542.14 nm
DWDM-SFP-4294		Cisco 1000BASE-DWDM SFP 1542.94 nm
DWDM-SFP-4373		Cisco 1000BASE-DWDM SFP 1543.73 nm
DWDM-SFP-4453		Cisco 1000BASE-DWDM SFP 1544.53 nm
DWDM-SFP-4612		Cisco 1000BASE-DWDM SFP 1546.12 nm
DWDM-SFP-4692		Cisco 1000BASE-DWDM SFP 1546.92 nm
DWDM-SFP-4772		Cisco 1000BASE-DWDM SFP 1547.72 nm
DWDM-SFP-4851		Cisco 1000BASE-DWDM SFP 1548.51 nm
DWDM-SFP-5012		Cisco 1000BASE-DWDM SFP 1550.12 nm
DWDM-SFP-5092		Cisco 1000BASE-DWDM SFP 1550.92 nm
DWDM-SFP-5172		Cisco 1000BASE-DWDM SFP 1551.72 nm
DWDM-SFP-5252		Cisco 1000BASE-DWDM SFP 1552.52 nm
DWDM-SFP-5413		Cisco 1000BASE-DWDM SFP 1554.13 nm

Table 6-84 Supported Modules for Cisco ASR 1000 Series—Cisco Prime Network 3.9 (continued)

Module Name	Product_Version	Module Description
DWDM-SFP-5494		Cisco 1000BASE-DWDM SFP 1554.94 nm
DWDM-SFP-5575		Cisco 1000BASE-DWDM SFP 1555.75 nm
DWDM-SFP-5655		Cisco 1000BASE-DWDM SFP 1556.55 nm
DWDM-SFP-5817		Cisco 1000BASE-DWDM SFP 1558.17 nm
DWDM-SFP-5898		Cisco 1000BASE-DWDM SFP 1558.98 nm
DWDM-SFP-5979		Cisco 1000BASE-DWDM SFP 1559.79 nm
DWDM-SFP-6061		Cisco 1000BASE-DWDM SFP 1560.61 nm
DWDM-XFP-30.33		10GBASE-DWDM 1530.33 nm XFP (100-GHz ITU grid)
DWDM-XFP-31.12		10GBASE-DWDM 1531.12 nm XFP (100-GHz ITU grid)
DWDM-XFP-31.90		10GBASE-DWDM 1531.90 nm XFP (100-GHz ITU grid)
DWDM-XFP-32.68		10GBASE-DWDM 1532.68 nm XFP (100-GHz ITU grid)
DWDM-XFP-34.25		10GBASE-DWDM 1534.25 nm XFP (100-GHz ITU grid)
DWDM-XFP-35.04		10GBASE-DWDM 1535.04 nm XFP (100-GHz ITU grid)
DWDM-XFP-35.82		10GBASE-DWDM 1535.82 nm XFP (100-GHz ITU grid)
DWDM-XFP-36.61		10GBASE-DWDM 1536.61 nm XFP (100-GHz ITU grid)
DWDM-XFP-38.19		10GBASE-DWDM 1538.19 nm XFP (100-GHz ITU grid)
DWDM-XFP-38.98		10GBASE-DWDM 1538.98 nm XFP (100-GHz ITU grid)
DWDM-XFP-39.77		10GBASE-DWDM 1539.77 nm XFP (100-GHz ITU grid)
DWDM-XFP-40.56		10GBASE-DWDM 1540.56 nm XFP (100-GHz ITU grid)
DWDM-XFP-42.14		10GBASE-DWDM 1542.14 nm XFP (100-GHz ITU grid)
DWDM-XFP-42.94		10GBASE-DWDM 1542.94 nm XFP (100-GHz ITU grid)
DWDM-XFP-43.73		10GBASE-DWDM 1543.73 nm XFP (100-GHz ITU grid)
DWDM-XFP-44.53		10GBASE-DWDM 1544.53 nm XFP (100-GHz ITU grid)

Table 6-84 Supported Modules for Cisco ASR 1000 Series—Cisco Prime Network 3.9 (continued)

Module Name	Product_Version	Module Description
DWDM-XFP-46.12		10GBASE-DWDM 1546.12 nm XFP (100-GHz ITU grid)
DWDM-XFP-46.92		10GBASE-DWDM 1546.92 nm XFP (100-GHz ITU grid)
DWDM-XFP-47.72		10GBASE-DWDM 1547.72 nm XFP (100-GHz ITU grid)
DWDM-XFP-48.51		10GBASE-DWDM 1548.51 nm XFP (100-GHz ITU grid)
DWDM-XFP-50.12		10GBASE-DWDM 1550.12 nm XFP (100-GHz ITU grid)
DWDM-XFP-50.92		10GBASE-DWDM 1550.92 nm XFP (100-GHz ITU grid)
DWDM-XFP-51.72		10GBASE-DWDM 1551.72 nm XFP (100-GHz ITU grid)
DWDM-XFP-52.52		10GBASE-DWDM 1552.52 nm XFP (100-GHz ITU grid)
DWDM-XFP-54.13		10GBASE-DWDM 1554.13 nm XFP (100-GHz ITU grid)
DWDM-XFP-54.94		10GBASE-DWDM 1554.94 nm XFP (100-GHz ITU grid)
DWDM-XFP-55.75		10GBASE-DWDM 1555.75 nm XFP (100-GHz ITU grid)
DWDM-XFP-56.55		10GBASE-DWDM 1556.55 nm XFP (100-GHz ITU grid)
DWDM-XFP-58.17		10GBASE-DWDM 1558.17 nm XFP (100-GHz ITU grid)
DWDM-XFP-58.98		10GBASE-DWDM 1558.98 nm XFP (100-GHz ITU grid)
DWDM-XFP-59.79		10GBASE-DWDM 1559.79 nm XFP (100-GHz ITU grid)
DWDM-XFP-60.61		10GBASE-DWDM 1560.61 nm XFP (100-GHz ITU grid)
GLC-BX-D		1000BASE-BX10 SFP module for single-strand SMF, 1310-nm TX/1490-nm RX wavelength
GLC-BX-U		1000BASE-BX10 SFP module for single-strand SMF, 1490-nm TX/1310-nm RX wavelength
GLC-GE-100FX		100BASE-FX SFP module for Gigabit Ethernet ports, 1310 nm wavelength, 2 km over MMF
SFP-GE-L		Cisco SFP Gigabit Ethernet 1000Base LX
SFP-GE-S		SFP Gigabit Ethernet 1000Base SX
SFP-GE-T		SFP Gigabit Ethernet 1000Base Tx

Table 6-84 Supported Modules for Cisco ASR 1000 Series—Cisco Prime Network 3.9 (continued)

Module Name	Product_Version	Module Description
SFP-GE-Z		SFP Gigabit Ethernet 1000Base Zx
SFP-OC12-IR1		SFP OC12 Intermaediate Reach
SFP-OC12-LR1		SFP OC12 Long reach 1
SFP-OC12-LR2		Cisco OC 12 SFP Long Reach 2
SFP-OC12-MM		Cisco OC12 STM1 SFP Multimode
SFP-OC12-SR		Cisco OC12 STM1 SFP Short Reach
SFP-OC3-IR1		Cisco OC3 SFP Intermediate Reach
SFP-OC3-LR1		Cisco OC3 STM1 SFP Single Mode Fibre Long ReACH
SFP-OC3-LR2		Cisco OC3 STM1 SFP Single Mode Fibre Long Reach
SFP-OC3-MM		Cisco OC3 SFP Multimode
SFP-OC3-SR		Cisco OC 3 SFP Short Reach
SFP-OC48-IR1		Cisco OC 48 SFP Intermediate Reach 1
SFP-OC48-LR2		Cisco OC 48 SFP Long Reach 2
SFP-OC48-SR		SFP OC48 Short Reach
SPA-10XGE-V2		Cisco SPA 10 Port GE Version2
SPA-1X10GE-L-V2	[4]	Cisco 1-Port 10GE LAN-PHY Shared Port Adapter
SPA-1XCHOC12/DS0		1-Port Channelized OC-12/STM-4 Shared Port Adapter
SPA-1XCHSTM1/OC3		Cisco SPA 1 Port Channelized OC 3 STM 1
SPA-1XOC12-ATM-V2		1-port OC12/STM4 ATM Shared Port Adapter
SPA-1XOC12-POS		Cisco 1 Port OC 12 POS
SPA-1XOC3-ATM-V2		Cisco SPA 1 Port OC3 ATM Version3
SPA-1XOC48POS		1-port OC48c/STM16c POS/RPR SFP Optics
SPA-1XOC48POS/RPR		Cisco SPA 1 Port Oc 48 POS RPR
SPA-2X1GE-SYNCE		
SPA-2X1GE-V2	[5]	Cisco 2-Port Gigabit Ethernet Shared Port Adapter, Version 2
SPA-2XCT3/DS0		Cisco SPA 2 Port Channelised T3/DS0
SPA-2XOC12-POS		2-Port OC-3c/STM-1 and OC-12c/STM-4 POS SPA
SPA-2XOC3-POS		Cisco SPA 2 Port OC3 POS
SPA-2XOC48POS/RPR		Cisco SPA 2 Port OC48 POS
SPA-2XT3/E3		Cisco SPA 2 Port T3/E3 Serial
SPA-3XOC3-ATM-V2		Cisco SPA 3 Port OC3 ATM Version 2
SPA-4X1FE-TX-V2		Cisco 4x 1 Port Fast Ethernet Tx V2

Table 6-84 Supported Modules for Cisco ASR 1000 Series—Cisco Prime Network 3.9 (continued)

Module Name	Product_Version	Module Description
SPA-4XCT3/DS0		Cisco SPA 4 Port Channelised T3/DS0
SPA-4XOC12-POS		4-port OC-12/STM-4 POS Shared Port Adapters
SPA-4XOC3-POS		Cisco SPA 4 Port OC3 POS
SPA-4XOC48POS/RPR		Cisco SPA 4 Port Oc 48 POS RPR
SPA-4XT3/E3		Cisco SPA 4Port T3/E3
SPA-4XT-SERIAL		Cisco 4 Port Serial SPA
SPA-5X1GE-V2		Cisco SPA 5 x 1 Port Gigabit Ethernet V2
SPA-8X1FE-TX-V2	6	Cisco 8-Port 10BASE-T/100BASE Fast Ethernet Shared Port Adapter, V-2
SPA-8X1GE-V2		Cisco SPA 8 x 1 Port Gigabit Ethernet V2
SPA-8XCHT1/E1		Cisco SPA 8 Port Channelized T1/E1
SPA-8XOC12-POS		8-Port OC-12c/STM-4 Multirate POS SPA
SPA-8XOC3-POS		8-Port OC-3c/STM-1 POS SPA
SPA-DSP		
SPA-OC192POS-XFP		1-port OC192/STM64 POS/RPR XFP Optics
SPA-WMA-K9		WebEx Node Shared Port Adapter
XFP-10GER-OC192IR		Multirate XFP module for 10GBASE-IR and OC192 IR
XFP-10GLR-OC192LR		Cisco multirate XFP transceiver module for 10GBASE-LR Ethernet and OC-192/STM-64 long-reach Packet-over-SONET/SDH (POS) applications, SMF, dual LC connector
XFP-10GLR-OC192SR	7	Multirate XFP module for 10GBASE-LR and OC192 SR-1
XFP-10G-MM-SR		Cisco 10GBASE-SR XFP transceiver module for MMF, 850-nm wavelength, dual LC connector
XFP-10GZR-OC192LR		Multirate XFP module for 10GBASE-LR and OC192 LR
SPA-1CHOC3-CE-ATM	8	1-port Channelized OC3/STM1 Circuit Emulation/ATM SPA
SPA-1X10GE-WL-V2	9	1-port 10 Gigabit Ethernet Shared Port Adapter XFP based
SPA-24CHT1-CE-ATM	10	
SPA-2CHT3-CE-ATM	11	

[1, 2, 3, 4, 5, 6, 7] Also tested on ASR1004

[8, 9, 10, 11] Tested on ASR 1002

Cisco ASR 1000 Series—Supported Technologies

The following technologies are supported by the Cisco ASR 1000 Series in Cisco Prime Network 3.9:

- IP, page 6-199
- Routing Protocols, page 6-202
- Ethernet, page 6-205
- ATM, page 6-213
- Frame Relay, page 6-217
- PPP, page 6-219
- SONET/SDH, page 6-220
- TDM/DSx, page 6-222
- MPLS, page 6-226
- MPLS-TE, page 6-228
- VPN (VRF), page 6-233
- PWE3, page 6-235
- Security, page 6-237
- Hardware, page 6-238
- Serial, page 6-242
- Additional Technologies, page 6-243
- LocalSwitching, page 6-245
- BFD, page 6-246
- Carrier Ethernet, page 6-247
- CDP, page 6-249
- Discovery Protocol, page 6-249
- SBC, page 6-256
- 6PE, page 6-264
- 6rd, page 6-264
- IPSec, page 6-266

Cisco ASR 1000 Series—Supported Service Events

Table 6-85 Supported Service Events for Cisco ASR 1000 Series—Cisco Prime Network 3.9

Event Name	Product_Version	Expedited
Active IP Interfaces Found		Y
All IP Interfaces Down		Y
Card Down		Y
Card In		Y

Table 6-85 Supported Service Events for Cisco ASR 1000 Series—Cisco Prime Network 3.9

Event Name	Product_Version	Expedited
Card Out		Y
Card Up		Y
Device Unsupported		N
Dropped packet rate exceeded upper threshold		N
Link up		N

Cisco MWR 2900 Series Mobile Wireless Routers

This section includes the following information about Cisco MWR 2941 routers (for information on the NE types supported in Cisco Prime Network 3.9, see Cisco MWR 2900 Series Mobile Wireless Routers):

- Cisco MWR 2941—Supported Software Versions, page 6-143
- Cisco MWR 2941—Supported Topologies, page 6-145
- Cisco MWR 2941—Supported Modules, page 6-145
- Cisco MWR 2941—Supported Technologies, page 6-148
- Cisco MWR 2941—Supported Service Events, page 6-149

Cisco MWR 2941—Supported Software Versions

Table 6-86 Supported Software Versions for Cisco MWR 2941—Cisco Prime Network 3.9

Software Version	Product_Version
12.2(33)MRA	3.7[1]
12.4(19)MR2	3.6.6[2]
12.4(20)MR	3.6.7[3]
15.0(1)MR	3.7.2[4]
12.4(20)MR2	3.7.1.1[5]
12.2(33)MRB1	3.7.2-DP-1.0[6]
12.2(33)MRB2	3.7.2-DP-1.0[7]
12.2(33)MRB3	3.7.2-DP-1.0[8]
12.4(20)MRA1	3.7.2-DP-1.0[9]

Table 6-86 Supported Software Versions for Cisco MWR 2941—Cisco Prime Network 3.9

Software Version	Product_Version
12.4(20)MRB	3.7.2-DP-1.0 [10]
12.4(19)MR3	3.7.2-DP-1.0 [11]
12.4(20)MR1	3.7.2-DP-1.0 [12]
12.2(33)MRB4	3.7.2-DP-3.0 [13]
15.1(1)MR	3.7.x-DP-5.0 [14]
15.0(2)MR	3.7.X-DP-4.0
12.4(20)MRA	3.7.2-DP-1.0
12.2(33)MRB	3.7.2-DP-1.0
CSR 3.4.2 aka 15.1(1)MR2	Cisco-ANA3.7.X-DP9 , PrimeNetwork-3.8.X-DP1
CSR3.4.1 aka 15.1(1)MR1	Cisco-ANA3.7.X-DP7
15.1(2)S2	Cisco-ANA3.7.X-DP8
15.0(1)MR1	Cisco-ANA3.7.X-DP3
12.2(33)MRB6	Cisco-ANA3.7.X-DP7
CSR3.4.1 aka 15.1(1)MR1	Cisco-ANA3.7.X-DP7
CSR3.4.2 aka 15.1(1)MR2	Cisco-ANA3.7.X-DP9
12.2(33)MRB5	Cisco-ANA3.7.X-DP6
15.1(1)MR3	Cisco-ANA3.7.X-DP12, PrimeNetwork-3.8.X-DP3
15.1(1)MR04	Cisco-ANA3.7.X-DP15, PrimeNetwork-3.8.X-DP6

112.2(33)MRA(a.k.a)CSR 3.2; ANA models pluggable ports for this IOS version.

2, 3ANA recognizes all maintenance builds in this IOS release train.ANA models pluggable ports for this IOS version.

4ANA recognizes and models the devices with 15.0(01)MR or CSR3.3

5ANA recognizes and models the devices with 12.4(20)MR2

6ANA recognizes and models the devices with 12.2(33)MRB1

7ANA recognizes and models the devices with 12.2(33)MRB2

8ANA recognizes and models the devices with 12.2(33)MRB3

9ANA recognizes and models the devices with 12.4(20)MRA1

10ANA recognizes and models the devices with 12.4(20)MRB

11ANA recognizes and models the devices with 12.4(19)MR3

12ANA recognizes and models the devices with 12.4(20)MR1

13ANA recognizes and models the devices with 12.2(33)MRB4

14ANA recognizes ans models the devices with 15.1(1)MR

Cisco MWR 2941—Supported Topologies

Table 6-87 Supported Topologies for Cisco MWR 2941—Cisco Prime Network 3.9

Topology Type	Link Type	Product_Version
ATM	ATM	3.6.6
BGP	BGP	3.6.6
Ethernet	Ethernet	3.6.6
Framerelay	Framerelay	3.6.6
MPLS	MPLS	3.6.6
PPP/HDLC	PPP or HDLC	3.6.6
Physical Layer	Physical Layer	3.6.6
MLPPP	MLPPP	3.7.1
BFD	BFD	3.7.1
VPN (IPv6)	VPN	3.7.1

Cisco MWR 2941—Supported Modules

Table 6-88 Supported Modules for Cisco MWR 2941—Cisco Prime Network 3.9

Module Name	Product_Version	Module Description
ASM-M2900-TOP	3.6.6	Timing over Packet Accessory Serivce Module for the Cisco MWR 2900 Series Mobile Wireless Routers
CWDM-SFP-1470	3.7.1	Cisco CWDM SFP 1470 nm
CWDM-SFP-1490	3.7.1	Cisco CWDM SFP 1490 nm
CWDM-SFP-1510	3.7.1	Cisco CWDM SFP 1510 nm

Table 6-88 Supported Modules for Cisco MWR 2941—Cisco Prime Network 3.9 (continued)

Module Name	Product_Version	Module Description
CWDM-SFP-1530	3.7.1	Cisco CWDM SFP 1530 nm
CWDM-SFP-1550	3.7.1	Cisco CWDM SFP 1550 nm
CWDM-SFP-1570	3.7.1	Cisco CWDM SFP 1570 nm
CWDM-SFP-1590	3.7.1	Cisco CWDM SFP 1590 nm
CWDM-SFP-1610	3.7.1	Cisco CWDM SFP 1610 nm
DWDM-SFP-3033	3.7.1	Cisco 1000BASE-DWDM SFP 1530.33 nm
DWDM-SFP-3112	3.7.1	Cisco 1000BASE-DWDM SFP 1531.12 nm
DWDM-SFP-3190	3.7.1	Cisco 1000BASE-DWDM SFP 1531.90 nm
DWDM-SFP-3268	3.7.1	Cisco 1000BASE-DWDM SFP 1532.68 nm
DWDM-SFP-3346	3.7.1	Cisco 1000BASE-DWDM SFP 1533.46 nm
DWDM-SFP-3425	3.7.1	Cisco 1000BASE-DWDM SFP 1534.25 nm
DWDM-SFP-3504	3.7.1	Cisco 1000BASE-DWDM SFP 1535.04 nm
DWDM-SFP-3582	3.7.1	Cisco 1000BASE-DWDM SFP 1535.82 nm
DWDM-SFP-3661	3.7.1	Cisco 1000BASE-DWDM SFP 1536.61 nm
DWDM-SFP-3739	3.7.1	Cisco 1000BASE-DWDM SFP 1537.39 nm
DWDM-SFP-3819	3.7.1	Cisco 1000BASE-DWDM SFP 1538.19 nm
DWDM-SFP-3898	3.7.1	Cisco 1000BASE-DWDM SFP 1539.98 nm
DWDM-SFP-3977	3.7.1	Cisco 1000BASE-DWDM SFP 1539.77 nm
DWDM-SFP-4056	3.7.1	Cisco 1000BASE-DWDM SFP 1540.56 nm
DWDM-SFP-4134	3.7.1	Cisco 1000BASE-DWDM SFP 1541.34 nm
DWDM-SFP-4214	3.7.1	Cisco 1000BASE-DWDM SFP 1542.14 nm
DWDM-SFP-4294	3.7.1	Cisco 1000BASE-DWDM SFP 1542.94 nm
DWDM-SFP-4373	3.7.1	Cisco 1000BASE-DWDM SFP 1543.73 nm
DWDM-SFP-4453	3.7.1	Cisco 1000BASE-DWDM SFP 1544.53 nm
DWDM-SFP-4532	3.7.1	Cisco 1000BASE-DWDM SFP 1545.32 nm
DWDM-SFP-4612	3.7.1	Cisco 1000BASE-DWDM SFP 1546.12 nm
DWDM-SFP-4692	3.7.1	Cisco 1000BASE-DWDM SFP 1546.92 nm
DWDM-SFP-4772	3.7.1	Cisco 1000BASE-DWDM SFP 1547.72 nm
DWDM-SFP-4851	3.7.1	Cisco 1000BASE-DWDM SFP 1548.51 nm
DWDM-SFP-4931	3.7.1	Cisco 1000BASE-DWDM SFP 1549.31 nm
DWDM-SFP-5012	3.7.1	Cisco 1000BASE-DWDM SFP 1550.12 nm
DWDM-SFP-5092	3.7.1	Cisco 1000BASE-DWDM SFP 1550.92 nm
DWDM-SFP-5172	3.7.1	Cisco 1000BASE-DWDM SFP 1551.72 nm
DWDM-SFP-5252	3.7.1	Cisco 1000BASE-DWDM SFP 1552.52 nm
DWDM-SFP-5332	3.7.1	Cisco 1000BASE-DWDM SFP 1553.32 nm

Table 6-88 Supported Modules for Cisco MWR 2941—Cisco Prime Network 3.9 (continued)

Module Name	Product_Version	Module Description
DWDM-SFP-5413	3.7.1	Cisco 1000BASE-DWDM SFP 1554.13 nm
DWDM-SFP-5494	3.7.1	Cisco 1000BASE-DWDM SFP 1554.94 nm
DWDM-SFP-5575	3.7.1	Cisco 1000BASE-DWDM SFP 1555.75 nm
DWDM-SFP-5655	3.7.1	Cisco 1000BASE-DWDM SFP 1556.55 nm
DWDM-SFP-5736	3.7.1	Cisco 1000BASE-DWDM SFP 1557.36 nm
DWDM-SFP-5817	3.7.1	Cisco 1000BASE-DWDM SFP 1558.17 nm
DWDM-SFP-5898	3.7.1	Cisco 1000BASE-DWDM SFP 1558.98 nm
DWDM-SFP-5979	3.7.1	Cisco 1000BASE-DWDM SFP 1559.79 nm
DWDM-SFP-6061	3.7.1	Cisco 1000BASE-DWDM SFP 1560.61 nm
DWDM-SFP-6141	3.7.1	Cisco 1000BASE-DWDM SFP 1561.41 nm
GLC-LH-SM	3.6.7	1000 Base LX/LH long reach SFP transceiver
GLC-LX-SM-RGD	3.7.1	1000BASE-LX/LH SFP transceiver module for MMF and SMF, 1300-nm wavelength, industrial Ethernet
GLC-SX-MM	3.6.7	1000 Base Sx short wavelength transceiver
GLC-SX-MM-RGD	3.7.1	1000BASE-SX SFP transceiver module for MMF, 850-nm wavelength, industrial Ethernet
GLC-T	3.6.7	1000 Base T Copper Gigabit ethernet SFP
GLC-ZX-SM	3.6.7	1000 Base Zx extended reach Gigabit ethernet SFP
GLC-ZX-SM-RGD	3.7.1	1000BASE-ZX SFP transceiver module for SMF, 1550-nm wavelength, industrial Ethernet
HWIC-1ADSL	3.6.6[1]	ADSL over POTS
HWIC-1ADSLI	3.6.6[2]	ADSL over ISDN
HWIC-1GE-SFP	3.6.7	HWIC with copper and optical Gigabit ethernet connectivity
HWIC-2SHDSL	3.6.6	HWIC G.SHDSL with annex F+G
HWIC-4SHDSL	3.6.6[3]	HWIC G.SHDSL with annex F+G and IMA.
HWIC-4T1/E1	3.6.6	4 port T1/E1 clear channel HWIC
HWIC-D-9ESW	3.6.7	9 Port FE Switch
MOTHEBOARD FOR 2941	3.6.6	Cisco MWR-2941-DC Motherboard with MPC8347E CPU, Gigabit Ethernet, SFP, BITS and T1/E1 por
SFP-GE-L	3.7[4]	1000BASE-LH/LX pluggable transceiver
SFP-GE-S	3.7[5]	1000BASE-Sx Short wavelength gigabit ethernet SFP.
SFP-GE-T	3.7.1	1000BASE-T SFP transceiver module for Category 5 copper wire, extended operating temperature range and DOM support
SFP-GE-Z	3.7[6]	1000BASE-Zx Extended reach gigabit ethernet SFP.

Table 6-88 Supported Modules for Cisco MWR 2941—Cisco Prime Network 3.9 (continued)

Module Name	Product_Version	Module Description
GLC-EX-SMD	3.7.x-DP-6.0[7]	Transceiver 1000BASE-SFP EX-SMD

[1], 2, 3Not Supported on 12.2(33)MRA (CSR3.2)

4, 5, 6Supported on 12.2(33)MRA (CSR3.2)

7Supported on 15.1(1)MR

Cisco MWR 2941—Supported Technologies

The following technologies are supported by the Cisco MWR 2941 in Cisco Prime Network 3.9:

- IP, page 6-199
- Routing Protocols, page 6-202
- Ethernet, page 6-205
- ATM, page 6-213
- Frame Relay, page 6-217
- PPP, page 6-219
- TDM/DSx, page 6-222
- MPLS, page 6-226
- MPLS-TE, page 6-228
- VPN (VRF), page 6-233
- PWE3, page 6-235
- Security, page 6-237
- Hardware, page 6-238
- Serial, page 6-242
- LocalSwitching, page 6-245
- BFD, page 6-246
- Carrier Ethernet, page 6-247
- CDP, page 6-249
- Discovery Protocol, page 6-249
- Ethernet OAM, page 6-250

Cisco MWR 2941—Supported Service Events

Table 6-89 Supported Service Events for Cisco MWR 2941—Cisco Prime Network 3.9

Event Name	Product_Version	Expedited
Active IP Interfaces Found	3.6.6	Y
All IP Interfaces Down	3.6.6	Y
BGP process up	3.6.6	N
Card Down	3.6.6	Y
Card In	3.6.6	Y
Card Out	3.6.6	Y
Card Up	3.6.6	Y
CPU utilization exceeded upper threshold	3.6.6	N
Device Unsupported	3.6.6	N
Fan-tray down	Prime Network 3.8	N
Fan-tray out	Prime Network 3.8	N
IMA Administratively down	3.7	N
IMA Administratively up	3.7	N
IMA Operationally up	3.7	N
Layer 2 Tunnel Down	3.6.6	N
Link up	3.6.6	N
Memory utilization exceeded upper threshold	3.6.6	N
MLPPP Operationaly down	3.7	N
MLPPP Up	3.7	N
Module Unsupported	3.6.6	N
MPLS Black Hole found	3.6.6	N
rep port role change	Prime Network 3.8	Y
BFD neighbor found	3.7.1	N
BFD neighbor loss	3.7.1	N
CGN statistics dropsPortLimitIn2Out higher threshold exceeded	3.7.1	N

Table 6-89 Supported Service Events for Cisco MWR 2941—Cisco Prime Network 3.9 (continued)

Event Name	Product_Version	Expedited
CGN statistics dropsSystemLimitIn2Out higher threshold exceeded	3.7.1	N
CGN statistics fwdIn2Out higher threshold exceeded	3.7.1	N
CGN statistics fwdOut2In higher threshold exceeded	3.7.1	N
Device Managed	3.7.1	N
Management Unreachable	3.7.1	N
Device Partially Managed	3.7.1	N
DS3 Path Link down due to Card event	3.7.1	N
DS3 Path down due to Admin	3.7.1	N
DS3 Path down due to Card	3.7.1	N
DS3 Path down due to Oper	3.7.1	N
DS3 Path up	3.7.1	N
EFP down	3.7.1	N
EFP up	3.7.1	N
Primary HSRP Interface Active	3.7.1	N
Primary HSRP Interface not Active	3.7.1	N
Secondary HSRP Interface Active	3.7.1	N
Secondary HSRP Interface not Active	3.7.1	N
IMA Operationally down	3.7.1	N
Interface status down	3.7.1	N
Interface status up	3.7.1	N
LAG down	3.7.1	N
LAG Link down	3.7.1	N
Local switching entry down	3.7.1	N
Local switching entry up	3.7.1	N
Logical port down	3.7.1	N
MLPPP Administratively down	3.7.1	N
MPLS-TE tunnel down	3.7.1	N
OSPF Neighbor Down	3.7.1	N
OSPF Neighbor Up	3.7.1	N
Pluggable transceiver out	Prime Network 3.8	N

Table 6-89 Supported Service Events for Cisco MWR 2941—Cisco Prime Network 3.9 (continued)

Event Name	Product_Version	Expedited
Power-supply down	Prime Network 3.8	N
Power-supply out	Prime Network 3.8	N
Port up	3.7.1	N
rx dormant	3.7.1	N
Service down	3.7.1	N
Service up	3.7.1	N
tx dormant	3.7.1	N
VSI up	3.7.1	N
High priority member down	3.7.1	N
Low priority member down	3.7.1	N
Medium priority member down	3.7.1	N

Cisco 1900 Series Integrated Services Router

This section includes the following information about Cisco ISR 1900 Series routers (for information on the NE types supported in Cisco Prime Network 3.9, see Cisco 1900 Series Integrated Services Router):

- Cisco ISR 1900 Series—Supported Software Versions, page 6-151
- Cisco ISR 1900 Series—Supported Topologies, page 6-152
- Cisco ISR 1900 Series—Supported Modules, page 6-152
- Cisco ISR 1900 Series—Supported Technologies, page 6-152
- Cisco ISR 1900 Series—Supported Service Events, page 6-153

Cisco ISR 1900 Series—Supported Software Versions

Table 6-90 Supported Software Versions for Cisco ISR 1900 Series—Cisco Prime Network 3.9

Software Version	Product_Version
IOS 15.1(1)T	3.7.1.0.4
IOS 15.1(1)T1	3.7.1.0.4
IOS 15.1(1)T2	3.7.2
IOS 15.1(3)T	ANA-3.7.2-DP2

Table 6-90 Supported Software Versions for Cisco ISR 1900 Series—Cisco Prime Network 3.9

Software Version	Product_Version
IOS 15.1(1)T3	ANA-3.7.2-DP4

Cisco ISR 1900 Series—Supported Topologies

Table 6-91 Supported Topologies for Cisco ISR 1900 Series—Cisco Prime Network 3.9

Topology Type	Link Type	Product_Version
Business	Business	3.7.1.0.4
Ethernet	Ethernet	3.7.1.0.4
Physical Layer	Physical Layer	3.7.1.0.4
BFD	BFD	3.7.1.0.4
VPN (IPv6)	VPN	3.7.1.0.4

Cisco ISR 1900 Series—Supported Modules

Table 6-92 Supported Modules for Cisco ISR 1900 Series—Cisco Prime Network 3.9

Module Name	Product_Version	Module Description
C1941W MOTHER BOARD 2GE	3.7.1.0.4	Cisco 1941 Motherboard with two Gigabit Ethernet ports router and one WLAN Controller.
PWR-1941-2901-AC	3.7.1.0.4	Cisco 1941 C2901 AC Power Supply.
HWIC-1GE-SFP	3.7.1.0.4	High Speed WAN Interface Card - 1 Port Gigabit Ethernet
GLC-LH-SM	3.7.1.0.4	1000BASE-LX/LH long-wavelength/long haul; without DOM
C1941 MOTHER BOARD 2GE	3.7.1.0.4	Cisco 1941 motherboard with two Gigabit Ethernet ports router.
PWR-1941-POE	3.7.1.0.4	Cisco 1941 AC Power Supply with Power Over Ethernet (Both system + spare)

Cisco ISR 1900 Series—Supported Technologies

The following technologies are supported by the Cisco ISR 1900 Series in Cisco Prime Network 3.9:

- IP, page 6-199
- Routing Protocols, page 6-202

- Ethernet, page 6-205
- ATM, page 6-213
- Security, page 6-237
- Hardware, page 6-238
- BFD, page 6-246
- Carrier Ethernet, page 6-247
- CDP, page 6-249
- Discovery Protocol, page 6-249
- Ethernet OAM, page 6-250

Cisco ISR 1900 Series—Supported Service Events

Table 6-93 Supported Service Events for Cisco ISR 1900 Series—Cisco Prime Network 3.9

Event Name	Product_Version	Expedited
Active IP Interfaces Found	3.7.1.0.4	Y
All IP Interfaces Down	3.7.1.0.4	Y
BGP process up	3.7.1.0.4	N
Card Down	3.7.1.0.4	Y
Card Up	3.7.1.0.4	Y
Cloud Problem	3.7.1.0.4	N
CPU utilization exceeded upper threshold	3.7.1.0.4	N
Device Unreachable	3.7.1.0.4	N
Device Unsupported	3.7.1.0.4	N
Interface Status Down/Up	3.7.1.0.4	Y
IP pool exhausted	3.7.1.0.4	Y
l2tp peer established	3.7.1.0.4	N
l2tp peer is removed	3.7.1.0.4	N
LDP neighbor down	3.7.1.0.4	N
Link down due to Card event	3.7.1.0.4	N
Localswitching down	3.7.1.0.4	N
MEP connectivity down	3.7.1.0.4	N
MPLS Black Hole found	3.7.1.0.4	N
Port down due to Card down	3.7.1.0.4	N
Primary HSRP Interface not Active	3.7.1.0.4	N
Secondary HSRP Interface Active	3.7.1.0.4	N
Tx dormant normal	3.7.1.0.4	N

Table 6-93 Supported Service Events for Cisco ISR 1900 Series—Cisco Prime Network 3.9

Event Name	Product_Version	Expedited
VC removed	3.7.1.0.4	N
VSI Down	3.7.1.0.4	N
VSI Up/Down	3.7.1.0.4	N
BFD neighbor found	3.7.1.0.4	N
LAG down		N
LAG down		N
LAG Link down		N
LAG Link down		N
Port up		N
pluggable transceiver out	Prime Network 3.8	N
fan-tray down	Prime Network 3.8	N
fan-tray out	Prime Network 3.8	N
power-supply down	Prime Network 3.8	N

Cisco 2900 Series Integrated Services Router

This section includes the following information about Cisco ISR 2900 Series routers (for information on the NE types supported in Cisco Prime Network 3.9, see Cisco 2900 Series Integrated Services Router):

- Cisco ISR 2900 Series—Supported Software Versions, page 6-155
- Cisco ISR 2900 Series—Supported Topologies, page 6-155
- Cisco ISR 2900 Series—Supported Modules, page 6-155
- Cisco ISR 2900 Series—Supported Technologies, page 6-156
- Cisco ISR 2900 Series—Supported Service Events, page 6-157

Cisco ISR 2900 Series—Supported Software Versions

Table 6-94 Supported Software Versions for Cisco ISR 2900 Series—Cisco Prime Network 3.9

Software Version	Product_Version
IOS 15.1(1)T	3.7.1
IOS 15.1(1)T1	3.7.1.0.4
IOS 15.1(1)T2	3.7.2
IOS 15.1(3)T	ANA-3.7.2-DP2
IOS 15.1(1)T3	ANA-3.7.2-DP4
IOS 15.2(1)T1	ANA 3.7.x DP09

Cisco ISR 2900 Series—Supported Topologies

Table 6-95 Supported Topologies for Cisco ISR 2900 Series—Cisco Prime Network 3.9

Topology Type	Link Type	Product_Version
Business	Business	3.7.1
Ethernet	Ethernet	3.7.1
Physical Layer	Physical Layer	3.7.1
BFD	BFD	3.7.1
VPN (IPv6)	VPN	3.7.1

Cisco ISR 2900 Series—Supported Modules

Table 6-96 Supported Modules for Cisco ISR 2900 Series—Cisco Prime Network 3.9

Module Name	Product_Version	Module Description
SM-NM-ADPTR	3.7.1	Network Module Adapter for SM Slot
PWR-2911-AC	3.7.1	C2911 AC Power Supply
GE-DCARD-ESW	3.7.1	Gigabit(1000BaseT) module for EtherSwitch NM
HWIC-1GE-SFP	3.7.1	High Speed WAN Interface Card - 1 Port Gigabit Ethernet
NME-16ES-1G	3.7.1	NME-16ES-1G: EtherSwitch SM 16 10/100T + 1 GE
PWR-2921-51-AC	3.7.1	C2921/C2951 AC Power Supply

Table 6-96 Supported Modules for Cisco ISR 2900 Series—Cisco Prime Network 3.9 (continued)

Module Name	Product_Version	Module Description
NM-16ESW-1GIG	3.7.1	16-port 10/100 EtherSwitch Network Module with 1 GbE (1000BASE-T) Port
SM-D-ES2-48	3.7.1.0.4	48 10/100 Ethernet port, double-wide Layer 2 enhanced EtherSwitch service module
SM-D-ES3-48-P	3.7.1.0.4	48 10/100 Ethernet port, double-wide Layer 2 and Layer 3 enhanced EtherSwitch service module, with PoE support
SM-D-ES3G-48-P	3.7.1.0.4	48 10/100/1000 Ethernet port, double-wide Layer 2 and Layer 3 enhanced EtherSwitch service module, with PoE support
VWIC2-1MFT-G703	3.7.2	VWIC2-1MFT-G703 - 1-Port RJ-48 Multiflex Trunk - G.703
EHWIC-VA-DSL-A	ANA 3.7.x DP09	
PWR-2921-51-DC	ANA 3.7.x DP14, ANA 3.8.x DP05	C2921/C2951 DC Power Supply

Cisco ISR 2900 Series—Supported Technologies

The following technologies are supported by the Cisco ISR 2900 Series in Cisco Prime Network 3.9:

- IP, page 6-199
- Routing Protocols, page 6-202
- Ethernet, page 6-205
- MPLS, page 6-226
- Security, page 6-237
- Hardware, page 6-238
- BFD, page 6-246
- Carrier Ethernet, page 6-247
- CDP, page 6-249
- Discovery Protocol, page 6-249
- Ethernet OAM, page 6-250

Cisco ISR 2900 Series—Supported Service Events

Table 6-97 Supported Service Events for Cisco ISR 2900 Series—Cisco Prime Network 3.9

Event Name	Product_Version	Expedited
Active IP Interfaces Found	3.7.1	Y
All IP Interfaces Down	3.7.1	Y
BGP process up	3.7.1	N
Card Down	3.7.1	Y
Card Up	3.7.1	Y
Cloud Problem	3.7.1	N
CPU utilization exceeded upper threshold	3.7.1	N
Device Unreachable	3.7.1	N
Device Unsupported	3.7.1	N
Fan-tray down	Prime Network 3.8	N
Fan-tray out	Prime Network 3.8	N
Interface status down flapping	3.7.1	Y
Keepalive configured	3.7.1	N
Keepalive not configured	3.7.1	N
Layer 2 Tunnel Down	3.7.1	N
Link up	3.7.1	N
Memory utilization exceeded upper threshold	3.7.1	N
Module Unsupported	3.7.1	N
Pluggable transceiver out	Prime Network 3.8	N
Power-supply down	Prime Network 3.8	N
Power-supply out	Prime Network 3.8	N
Rx utilization exceeded upper threshold	3.7.1	N
SONET Path up	3.7	N

Table 6-97 Supported Service Events for Cisco ISR 2900 Series—Cisco Prime Network 3.9

Event Name	Product_Version	Expedited
Tx utilization exceeded upper threshold	3.7.1	N
Vlan Tagged Interface AdminDown	3.7.1	N
Vlan Tagged Interface Up/Down	3.7.1	N
VPN Leak	3.7.1	N

Cisco 3900 Series Integrated Service Routers

This section includes the following information about Cisco ISR 3900 Series routers (for information on the NE types supported in Cisco Prime Network 3.9, see Cisco 3900 Series Integrated Service Routers):

- Cisco ISR 3900 Series—Supported Software Versions, page 6-158
- Cisco ISR 3900 Series—Supported Topologies, page 6-159
- Cisco ISR 3900 Series—Supported Modules, page 6-159
- Cisco ISR 3900 Series—Supported Technologies, page 6-160
- Cisco ISR 3900 Series—Supported Service Events, page 6-160

Cisco ISR 3900 Series—Supported Software Versions

Table 6-98 Supported Software Versions for Cisco ISR 3900 Series—Cisco Prime Network 3.9

Software Version	Product_Version
IOS 15.1(1)T	3.7.1
IOS 15.1(1)T1	3.7.1.0.4
IOS 15.1(1)T2	3.7.2
IOS 15.1(3)T	ANA-3.7.2-DP2
IOS 15.1(1)T3	ANA-3.7.2-DP4
IOS 15.2(1)T1	ANA 3.7.x DP09

Cisco ISR 3900 Series—Supported Topologies

Table 6-99 Supported Topologies for Cisco ISR 3900 Series—Cisco Prime Network 3.9

Topology Type	Link Type	Product_Version
Business	Business	3.7.1
Ethernet	Ethernet	3.7.1
Physical Layer	Physical Layer	3.7.1
BFD	BFD	3.7.1
VPN (IPv6)	VPN	3.7.1

Cisco ISR 3900 Series—Supported Modules

Table 6-100 Supported Modules for Cisco ISR 3900 Series—Cisco Prime Network 3.9

Module Name	Product_Version	Module Description
C3900-SPE100/K9	3.7.1	Cisco Services Performance Engine 100 for Cisco 3900 ISR
C3900-SPE150/K9	3.7.1	Cisco Services Performance Engine 150 for Cisco 3900 ISR
C3900-SPE200/K9	3.7.1	Cisco Services Performance Engine 200 for Cisco 3900 ISR
C3900-SPE250/K9	3.7.1	Cisco Services Performance Engine 250 for Cisco 3900 ISR
GE-DCARD-ESW	3.7.1	Gigabit(1000BaseT) module for EtherSwitch NM
HWIC-1GE-SFP	3.7.1	High Speed WAN Interface Card - 1 port Gigabit Ethernet SFP slot
NM-16ESW-1GIG	3.7.1	16-port 10/100 EtherSwitch NM with 1 GE (1000BaseT) port
PWR-3900-AC	3.7.1	C3900 AC Power Supply
SM-D-ES2-48	3.7.1.0.4	48 10/100 Ethernet port, double-wide Layer 2 enhanced EtherSwitch service module
SM-D-ES3-48-P	3.7.1.0.4	48 10/100 Ethernet port, double-wide Layer 2 and Layer 3 enhanced EtherSwitch service module, with PoE support
SM-D-ES3G-48-P	3.7.1.0.4	48 10/100/1000 Ethernet port, double-wide Layer 2 and Layer 3 enhanced EtherSwitch service module, with PoE support

Cisco ISR 3900 Series—Supported Technologies

The following technologies are supported by the Cisco ISR 3900 Series in Cisco Prime Network 3.9:

- IP, page 6-199
- Routing Protocols, page 6-202
- Ethernet, page 6-205
- ATM, page 6-213
- PPP, page 6-219
- TDM/DSx, page 6-222
- Security, page 6-237
- Hardware, page 6-238
- Serial, page 6-242
- LocalSwitching, page 6-245
- BFD, page 6-246
- Carrier Ethernet, page 6-247
- CDP, page 6-249
- Discovery Protocol, page 6-249
- Ethernet OAM, page 6-250

Cisco ISR 3900 Series—Supported Service Events

Table 6-101 Supported Service Events for Cisco ISR 3900 Series—Cisco Prime Network 3.9

Event Name	Product_Version	Expedited
Active IP Interfaces Found	3.7.1	Y
All IP Interfaces Down	3.7.1	Y
BGP process up	3.7.1	N
Card Down	3.7.1	Y
Card In	3.7.1	Y
Card Out	3.7.1	Y
Card Up	3.7.1	Y
Cloud Problem	3.7.1	N
CPU utilization exceeded upper threshold	3.7.1	N
Device Unreachable	3.7.1	N
Device Unsupported	3.7.1	N
DS1 Path link down due to Admin down	3.7	N

Table 6-101 Supported Service Events for Cisco ISR 3900 Series—Cisco Prime Network 3.9

Event Name	Product_Version	Expedited
DS1 Path link down due to Oper down	3.7	N
DS1 Path link Up	3.7	N
Interface status down flapping	3.7.1	Y
Keepalive configured	3.7.1	N
Keepalive not configured	3.7.1	N
Layer 2 Tunnel Down	3.7.1	N
Link up	3.7.1	N
Memory utilization exceeded upper threshold	3.7.1	N
Module Unsupported	3.7.1	N
Rx utilization exceeded upper threshold	3.7.1	N
Vlan Tagged Interface AdminDown	3.7.1	N
Vlan Tagged Interface Up/Down	3.7.1	N
VPN Leak	3.7.1	N
VSI Admin Down	3.7.1	N
VSI Down	3.7.1	N
pluggable transceiver out	Prime Network 3.8	N
fan-tray down	Prime Network 3.8	N
fan-tray out	Prime Network 3.8	N
power-supply down	Prime Network 3.8	N

Cisco Universal Broadband Router 7200 Series

This section includes the following information about Cisco UBR7200 Series routers (for information on the NE types supported in Cisco Prime Network 3.9, see Cisco Universal Broadband Router 7200 Series):

- Cisco UBR7200 Series—Supported Software Versions, page 6-162
- Cisco UBR7200 Series—Supported Topologies, page 6-162
- Cisco UBR7200 Series—Supported Modules, page 6-162
- Cisco UBR7200 Series—Supported Technologies, page 6-163

- Cisco UBR7200 Series—Supported Service Events, page 6-163

Cisco UBR7200 Series—Supported Software Versions

Table 6-102 Supported Software Versions for Cisco UBR7200 Series—Cisco Prime Network 3.9

Software Version	Product_Version
IOS 12.3(21a)BC6	3.7.1

Cisco UBR7200 Series—Supported Topologies

Table 6-103 Supported Topologies for Cisco UBR7200 Series—Cisco Prime Network 3.9

Topology Type	Link Type	Product_Version
ATM	ATM	3.7.1
BGP	BGP	3.7.1
Ethernet	Ethernet	3.7.1
Framerelay	Framerelay	3.7.1
MPLS	MPLS	3.7.1
PPP/HDLC	PPP or HDLC	3.7.1
Physical Layer	Physical Layer	3.7.1

Cisco UBR7200 Series—Supported Modules

Table 6-104 Supported Modules for Cisco UBR7200 Series—Cisco Prime Network 3.9

Module Name	Product_Version	Module Description
UBR7200-NPE-G1	3.7.1	Cisco uBR7200 Network Processing Engine including three GE/FE/E ports, 256 MB default DRAM, and 64 MB default flash memory
UBR-MC28X	3.7.1	uBR7200 Modem Card, 2 DS, 8 US, ATDMA, Adv PHY, CPU, no Upx
UBR-MC28U	3.7.1	uBR7200 Modem Card, 2 DS w/Upx, 8 US, ATDMA, Adv PHY, CPU
WS-G5484	3.7.1	Gigabit Ethernet GBIC, SC connector SX transceiver
WS-G5486	3.7.1	Gigabit Ethernet GBIC, SC connector LX/LH transceiver
WS-G5487	3.7.1	Gigabit Ethernet GBIC, SC connector ZX transceiver

Cisco UBR7200 Series—Supported Technologies

The following technologies are supported by the Cisco UBR7200 Series in Cisco Prime Network 3.9:

- IP, page 6-199
- Routing Protocols, page 6-202
- Ethernet, page 6-205
- ATM, page 6-213
- Frame Relay, page 6-217
- PPP, page 6-219
- HDLC, page 6-220
- MPLS, page 6-226
- VPN (VRF), page 6-233
- Security, page 6-237
- Hardware, page 6-238
- Serial, page 6-242
- CDP, page 6-249
- Discovery Protocol, page 6-249

Cisco UBR7200 Series—Supported Service Events

Table 6-105 Supported Service Events for Cisco UBR7200 Series—Cisco Prime Network 3.9

Event Name	Product_Version	Expedited
Active IP Interfaces Found	3.7.1	Y
All IP Interfaces Down	3.7.1	Y
BGP process up	3.7.1	N
Card Down	3.7.1	Y
Card In	3.7.1	Y
Card Out	3.7.1	Y
Card Up	3.7.1	Y
CPU utilization exceeded upper threshold	3.7.1	N
Device Unsupported	3.7.1	N
DS0 Bundle Admin down	3.7.1	N
DS0 Bundle Oper down	3.7.1	N
DS0 Bundle Up	3.7.1	N
DS1 Path down due to Admin	3.7.1	N
DS1 Path down due to Card	3.7.1	N

Table 6-105 Supported Service Events for Cisco UBR7200 Series—Cisco Prime Network 3.9

Event Name	Product_Version	Expedited
DS1 Path down due to Oper	3.7.1	N
DS1 Path link down due to Admin down	3.7.1	N
DS1 Path link down due to Oper down	3.7.1	N
DS1 Path link Up	3.7.1	N
Keepalive configured	3.7.1	N
Keepalive not configured	3.7.1	N
Layer 2 Tunnel Down	3.7.1	N
Link up	3.7.1	N
Memory utilization exceeded upper threshold	3.7.1	N
MLPPP Administratively down	3.7.1	N
MLPPP Operationaly down	3.7.1	N
MLPPP Up	3.7.1	N
Module Unsupported	3.7.1	N
MPLS Black Hole found	3.7.1	N
SONET Path down due to Admin	3.7.1	N
SONET Path down due to Card	3.7.1	N
Sonet Path link down due to Admin down	3.7.1	N
Sonet Path link Up	3.7.1	N
pluggable transceiver out	Prime Network 3.8	N
fan-tray down	Prime Network 3.8	N
fan-tray out	Prime Network 3.8	N
power-supply down	Prime Network 3.8	N

Cisco Univeral Broadband Router 10000 Series

This section includes the following information about Cisco UBR10000 Series routers (for information on the NE types supported in Cisco Prime Network 3.9, see Cisco Univeral Broadband Router 10000 Series):

- Cisco UBR10000 Series—Supported Software Versions, page 6-165
- Cisco UBR10000 Series—Supported Topologies, page 6-165
- Cisco UBR10000 Series—Supported Modules, page 6-165
- Cisco UBR10000 Series—Supported Technologies, page 6-166
- Cisco UBR10000 Series—Supported Service Events, page 6-167

Cisco UBR10000 Series—Supported Software Versions

Table 6-106 Supported Software Versions for Cisco UBR10000 Series—Cisco Prime Network 3.9

Software Version	Product_Version
IOS 12.2(33)SCB2	3.7.1
IOS 12.2(33)SCB3	3.7.1
IOS 12.2(33)SCB6	3.7.1

Cisco UBR10000 Series—Supported Topologies

Table 6-107 Supported Topologies for Cisco UBR10000 Series—Cisco Prime Network 3.9

Topology Type	Link Type	Product_Version
ATM	ATM	3.7.1
Ethernet	Ethernet	3.7.1
MPLS	MPLS	3.7.1
PPP/HDLC	PPP or HDLC	3.7.1
Physical Layer	Physical Layer	3.7.1

Cisco UBR10000 Series—Supported Modules

Table 6-108 Supported Modules for Cisco UBR10000 Series—Cisco Prime Network 3.9

Module Name	Product_Version	Module Description
10000-SIP-600	3.7.1	Cisco 10000 SPA Interface Processor-600
ESR-PRE4	3.7.1	Performance Routing Engine 4

Table 6-108 Supported Modules for Cisco UBR10000 Series—Cisco Prime Network 3.9 (continued)

Module Name	Product_Version	Module Description
SFP-GE-T	3.7.1	1000BASE-T SFP transceiver module for Category 5 copper wire, extended operating temperature range, RJ-45 connector
SPA-1X10GE-L-V2	3.7.1	Cisco 1-Port 10GE LAN-PHY Shared Port Adapter
SPA-24XDS-SFP	3.7.1	24-port uBR10012 Wideband Downstream Shared Port Adapter
UBR10-2XDS-SIP	3.7.1	Cisco uBR10012 Wideband Downstream-only SPA Carrier Card
UBR10-5X20S-D	3.7.1	uBR10012 BPE, 5 DS w/upx, 20 US, Spec Analyzer, dense connector
UBR10-MC5X20H-D	3.7.1	uBR10K Universal Card, 5DS w/upx, 20US, Spec An, Dense
UBR10-PWR-AC	3.7.1	Cisco uBR 1000 series AC power supply
UBR10-PWR-DC	3.7.1	Cisco uBR 1000 series DC power supply
XFP-10GER-OC192IR	3.7.1	Cisco multirate XFP transceiver module for 10GBASE-ER Ethernet and OC-192/STM-64 intermediate-reach (IR-2) Packet-over-SONET/SDH (POS) applications, SMF, dual LC connector
XFP-10GLR-OC192SR	3.7.1	Cisco multirate XFP transceiver module for 10GBASE-LR Ethernet and OC-192/STM-64 short-reach (SR-1) Packet-over-SONET/SDH (POS) applications, SMF, dual LC connector
XFP-10GZR-OC192LR	3.7.1	Cisco multirate XFP transceiver module for 10GBASE-ZR Ethernet and OC-192/STM-64 long-reach Packet-over-SONET/SDH (POS) applications, SMF, dual LC connector

Cisco UBR10000 Series—Supported Technologies

The following technologies are supported by the Cisco UBR10000 Series in Cisco Prime Network 3.9:

- IP, page 6-199
- Routing Protocols, page 6-202
- Ethernet, page 6-205
- MPLS, page 6-226
- VPN (VRF), page 6-233
- Security, page 6-237
- Hardware, page 6-238
- Serial, page 6-242
- CDP, page 6-249

- Discovery Protocol, page 6-249

Cisco UBR10000 Series—Supported Service Events

Table 6-109 Supported Service Events for Cisco UBR10000 Series—Cisco Prime Network 3.9

Event Name	Product_Version	Expedited
Active IP Interfaces Found	3.7.1	Y
All IP Interfaces Down	3.7.1	Y
BGP process up	3.7.1	N
Card Down	3.7.1	Y
Card In	3.7.1	Y
Card Out	3.7.1	Y
Card Up	3.7.1	Y
CPU utilization exceeded upper threshold	3.7.1	N
Device Unsupported	3.7.1	N
DS0 Bundle Admin down	3.7.1	N
DS0 Bundle Oper down	3.7.1	N
DS0 Bundle Up	3.7.1	N
DS1 Path down due to Admin	3.7.1	N
DS1 Path down due to Card	3.7.1	N
DS1 Path down due to Oper	3.7.1	N
DS1 Path link down due to Admin down	3.7.1	N
DS1 Path link down due to Oper down	3.7.1	N
DS1 Path link Up	3.7.1	N
Keepalive configured	3.7.1	N
Keepalive not configured	3.7.1	N
Layer 2 Tunnel Down	3.7.1	N
Link up	3.7.1	N
Memory utilization exceeded upper threshold	3.7.1	N
MLPPP Administratively down	3.7.1	N
MLPPP Operationaly down	3.7.1	N
MLPPP Up	3.7.1	N
Module Unsupported	3.7.1	N
MPLS Black Hole found	3.7.1	N
SONET Path down due to Admin	3.7.1	N

Table 6-109 Supported Service Events for Cisco UBR10000 Series—Cisco Prime Network 3.9

Event Name	Product_Version	Expedited
SONET Path down due to Card	3.7.1	N
Sonet Path link down due to Admin down	3.7.1	N
Sonet Path link down due to Oper down	3.7.1	N
Sonet Path link Up	3.7.1	N
pluggable transceiver out	Prime Network 3.8	N
fan-tray down	Prime Network 3.8	N
fan-tray out	Prime Network 3.8	N
power-supply down	Prime Network 3.8	N

Cisco 4700 Series Routers

This section includes the following information about Cisco 4700 Series routers (for information on the NE types supported in Cisco Prime Network 3.9, see Cisco 4700 Series Routers):

- Cisco 4700 Series—Supported Topologies, page 6-168
- Cisco 4700 Series—Supported Technologies, page 6-169
- Cisco 4700 Series—Supported Service Events, page 6-169

Cisco 4700 Series—Supported Topologies

Table 6-110 Supported Topologies for Cisco 4700 Series—Cisco Prime Network 3.9

Topology Type	Link Type	Product_Version
Ethernet	Ethernet	3.7.1
Physical Layer	Physical Layer	3.7.1

Cisco 4700 Series—Supported Technologies

The following technologies are supported by the Cisco 4700 Series in Cisco Prime Network 3.9:

- IP, page 6-199
- Routing Protocols, page 6-202
- Ethernet, page 6-205
- ATM, page 6-213
- Frame Relay, page 6-217
- PPP, page 6-219
- HDLC, page 6-220
- SONET/SDH, page 6-220
- TDM/DSx, page 6-222
- MPLS, page 6-226
- MPLS-TE, page 6-228
- VPN (VRF), page 6-233
- PWE3, page 6-235
- Security, page 6-237
- Hardware, page 6-238
- Serial, page 6-242
- IPoDWDM, page 6-243
- LocalSwitching, page 6-245
- BFD, page 6-246
- Carrier Ethernet, page 6-247
- CDP, page 6-249
- Discovery Protocol, page 6-249

Cisco 4700 Series—Supported Service Events

Table 6-111 Supported Service Events for Cisco 4700 Series—Cisco Prime Network 3.9

Event Name	Product_Version	Expedited
Active IP Interfaces Found	3.7.1	Y
All IP Interfaces Down	3.7.1	Y
BGP process up	3.7.1	N
Card Down	3.7.1	Y
Card In	3.7.1	Y
Card Out	3.7.1	Y
Card Up	3.7.1	Y

Table 6-111 Supported Service Events for Cisco 4700 Series—Cisco Prime Network 3.9

Event Name	Product_Version	Expedited
CPU utilization exceeded upper threshold	3.7.1	N
Device Unsupported	3.7.1	N
Fan-tray down	Prime Network 3.8	N
Fan-tray out	Prime Network 3.8	N
Layer 2 Tunnel Down	3.7.1	N
Link up	3.7.1	N
Memory utilization exceeded upper threshold	3.7.1	N
Module Unsupported	3.7.1	N
MPLS Black Hole found	3.7.1	N
Pluggable transceiver out	Prime Network 3.8	N
Power-supply down	Prime Network 3.8	N
Power-supply out	Prime Network 3.8	N

Cisco ASR901 Series Mobile Wireless Routers

This section includes the following information about Cisco ASR901 routers (for information on the NE types supported in Cisco Prime Network 3.9, see Cisco ASR901 Series Mobile Wireless Routers):

- Cisco ASR901—Supported Software Versions, page 6-171
- Cisco ASR901—Supported Topologies, page 6-171
- Cisco ASR901—Supported Modules, page 6-173
- Cisco ASR901—Supported Technologies, page 6-181
- Cisco ASR901—Supported Service Events, page 6-182

Cisco ASR901—Supported Software Versions

Table 6-112 Supported Software Versions for Cisco ASR901—Cisco Prime Network 3.9

Software Version	Product_Version
IOS 15.1(2)SNG	Cisco-ANA3.7.X-DP10 , PrimeNetwork-3.8.X-DP1[1]
IOS 15.1(2)SNH	Cisco-ANA3.7.X-DP12 , PrimeNetwork-3.8.X-DP3[2]
IOS 15.1(2)SNI	Cisco-ANA3.7.X-DP15 , PrimeNetwork-3.8.X-DP6[3]

[1, 2, 3]All ASR-901-C capabilities are being tested

Cisco ASR901—Supported Topologies

Table 6-113 Supported Topologies for Cisco ASR901—Cisco Prime Network 3.9

Topology Type	Link Type	Product_Version
ATM	ATM	Cisco-ANA3.7.X-DP10 , PrimeNetwork-3.8.X-DP1
BGP	BGP	Cisco-ANA3.7.X-DP10 , PrimeNetwork-3.8.X-DP1
Ethernet	Ethernet	Cisco-ANA3.7.X-DP10 , PrimeNetwork-3.8.X-DP1

Table 6-113 Supported Topologies for Cisco ASR901—Cisco Prime Network 3.9 (continued)

Topology Type	Link Type	Product_Version
Framerelay	Framerelay	Cisco-ANA3.7.X-DP10 , PrimeNetwork-3.8.X-DP1
MPLS	MPLS	Cisco-ANA3.7.X-DP10 , PrimeNetwork-3.8.X-DP1
PPP/HDLC	PPP or HDLC	Cisco-ANA3.7.X-DP10 , PrimeNetwork-3.8.X-DP1
Physical Layer	Physical Layer	Cisco-ANA3.7.X-DP10 , PrimeNetwork-3.8.X-DP1
MLPPP	MLPPP	Cisco-ANA3.7.X-DP10 , PrimeNetwork-3.8.X-DP1
BFD	BFD	Cisco-ANA3.7.X-DP10 , PrimeNetwork-3.8.X-DP1
VPN (IPv6)	VPN	Cisco-ANA3.7.X-DP10 , PrimeNetwork-3.8.X-DP1

Cisco ASR901—Supported Modules

Table 6-114 Supported Modules for Cisco ASR901—Cisco Prime Network 3.9

Module Name	Product_Version	Module Description
GLC-LH-SM	Cisco-ANA3.7.X-DP10 , PrimeNetwork-3.8.X-DP1	GE SFP,LC connector LX/LH transceiver
GLC-LX-SM-RGD	Cisco-ANA3.7.X-DP10 , PrimeNetwork-3.8.X-DP1	1000Mbps Single Mode Rugged SFP
GLC-SX-MM	Cisco-ANA3.7.X-DP10 , PrimeNetwork-3.8.X-DP1	GE SFP, LC connector SX transceiver
GLC-SX-MM-RGD	Cisco-ANA3.7.X-DP10 , PrimeNetwork-3.8.X-DP1	1000Mbps Multi-Mode Rugged SFP
GLC-ZX-SM	Cisco-ANA3.7.X-DP10 , PrimeNetwork-3.8.X-DP1	1000BASE-ZX SFP
GLC-ZX-SM-RGD	Cisco-ANA3.7.X-DP10 , PrimeNetwork-3.8.X-DP1	1000BASE-ZX Single Mode RuggedSFP
SFP-GE-L	Cisco-ANA3.7.X-DP10 , PrimeNetwork-3.8.X-DP1	1000BASE-LX/LH SFP (DOM)

Table 6-114 Supported Modules for Cisco ASR901—Cisco Prime Network 3.9 (continued)

Module Name	Product_Version	Module Description
SFP-GE-S	Cisco-ANA3.7.X-DP10 , PrimeNetwork-3.8.X-DP1	1000BASE-SX SFP (DOM)
SFP-GE-Z	Cisco-ANA3.7.X-DP10 , PrimeNetwork-3.8.X-DP1	1000BASE-ZX Gigabit Ethernet SFP (DOM)
SFP-GE-T	Cisco-ANA3.7.X-DP10 , PrimeNetwork-3.8.X-DP1	1000BASE-T SFP (NEBS 3 ESD)
CWDM-SFP-1470	Cisco-ANA3.7.X-DP10 , PrimeNetwork-3.8.X-DP1	CWDM 1470 NM SFP Gigabit Ethernet and 1G/2G FC
CWDM-SFP-1490	Cisco-ANA3.7.X-DP10 , PrimeNetwork-3.8.X-DP1	CWDM 1490 NM SFP Gigabit Ethernet and 1G/2G FC
CWDM-SFP-1510	Cisco-ANA3.7.X-DP10 , PrimeNetwork-3.8.X-DP1	CWDM 1510 NM SFP Gigabit Ethernet and 1G/2G FC
CWDM-SFP-1530	Cisco-ANA3.7.X-DP10 , PrimeNetwork-3.8.X-DP1	CWDM 1530 NM SFP Gigabit Ethernet and 1G/2G FC

Table 6-114 Supported Modules for Cisco ASR901—Cisco Prime Network 3.9 (continued)

Module Name	Product_Version	Module Description
CWDM-SFP-1550	Cisco-ANA3.7.X-DP10 , PrimeNetwork-3.8.X-DP1	CWDM 1550 NM SFP Gigabit Ethernet and 1G/2G FC
CWDM-SFP-1570	Cisco-ANA3.7.X-DP10 , PrimeNetwork-3.8.X-DP1	CWDM 1570 NM SFP Gigabit Ethernet and 1G/2G FC
CWDM-SFP-1590	Cisco-ANA3.7.X-DP10 , PrimeNetwork-3.8.X-DP1	CWDM 1590 NM SFP Gigabit Ethernet and 1G/2G FC
CWDM-SFP-1610	Cisco-ANA3.7.X-DP10 , PrimeNetwork-3.8.X-DP1	CWDM 1610 NM SFP Gigabit Ethernet and 1G/2G FC
DWDM-SFP-3033	Cisco-ANA3.7.X-DP10 , PrimeNetwork-3.8.X-DP1	DWDM SFP 1530.33 nm SFP (100 GHz ITU grid)
DWDM-SFP-3112	Cisco-ANA3.7.X-DP10 , PrimeNetwork-3.8.X-DP1	DWDM SFP 1531.12 nm SFP (100 GHz ITU grid)
DWDM-SFP-3190	Cisco-ANA3.7.X-DP10 , PrimeNetwork-3.8.X-DP1	DWDM SFP 1531.90 nm SFP (100 GHz ITU grid)

Table 6-114 Supported Modules for Cisco ASR901—Cisco Prime Network 3.9 (continued)

Module Name	Product_Version	Module Description
DWDM-SFP-3268	Cisco-ANA3.7.X-DP10 , PrimeNetwork-3.8.X-DP1	DWDM SFP 1532.68 nm SFP (100 GHz ITU grid)
DWDM-SFP-3346	Cisco-ANA3.7.X-DP10 , PrimeNetwork-3.8.X-DP1	DWDM SFP 1533.47 nm SFP (100 GHz ITU grid)
DWDM-SFP-3425	Cisco-ANA3.7.X-DP10 , PrimeNetwork-3.8.X-DP1	DWDM SFP 1534.25 nm SFP (100 GHz ITU grid)
DWDM-SFP-3504	Cisco-ANA3.7.X-DP10 , PrimeNetwork-3.8.X-DP1	DWDM SFP 1535.04 nm SFP (100 GHz ITU grid)
DWDM-SFP-3582	Cisco-ANA3.7.X-DP10 , PrimeNetwork-3.8.X-DP1	DWDM SFP 1535.82 nm SFP (100 GHz ITU grid)
DWDM-SFP-3661	Cisco-ANA3.7.X-DP10 , PrimeNetwork-3.8.X-DP1	DWDM SFP 1536.61 nm SFP (100 GHz ITU grid)
DWDM-SFP-3739	Cisco-ANA3.7.X-DP10 , PrimeNetwork-3.8.X-DP1	DWDM SFP 1537.40nm SFP (100 GHz ITU grid)

Table 6-114 Supported Modules for Cisco ASR901—Cisco Prime Network 3.9 (continued)

Module Name	Product_Version	Module Description
DWDM-SFP-3819	Cisco-ANA3.7.X-DP10 , PrimeNetwork-3.8.X-DP1	DWDM SFP 1538.19 nm SFP (100 GHz ITU grid)
DWDM-SFP-3898	Cisco-ANA3.7.X-DP10 , PrimeNetwork-3.8.X-DP1	DWDM SFP 1538.98 nm SFP (100 GHz ITU grid)
DWDM-SFP-3977	Cisco-ANA3.7.X-DP10 , PrimeNetwork-3.8.X-DP1	DWDM SFP 1539.77 nm SFP (100 GHz ITU grid)
DWDM-SFP-4056	Cisco-ANA3.7.X-DP10 , PrimeNetwork-3.8.X-DP1	DWDM SFP 1540.56 nm SFP (100 GHz ITU grid)
DWDM-SFP-4134	Cisco-ANA3.7.X-DP10 , PrimeNetwork-3.8.X-DP1	DWDM SFP 1541.35nm SFP (100 GHz ITU grid)
DWDM-SFP-4214	Cisco-ANA3.7.X-DP10 , PrimeNetwork-3.8.X-DP1	DWDM SFP 1542.14 nm SFP (100 GHz ITU grid)
DWDM-SFP-4294	Cisco-ANA3.7.X-DP10 , PrimeNetwork-3.8.X-DP1	DWDM SFP 1542.94 nm SFP (100 GHz ITU grid)

Table 6-114 Supported Modules for Cisco ASR901—Cisco Prime Network 3.9 (continued)

Module Name	Product_Version	Module Description
DWDM-SFP-4373	Cisco-ANA3.7.X-DP10 , PrimeNetwork-3.8.X-DP1	DWDM SFP 1543.73 nm SFP (100 GHz ITU grid)
DWDM-SFP-4453	Cisco-ANA3.7.X-DP10 , PrimeNetwork-3.8.X-DP1	DWDM SFP 1544.53 nm SFP (100 GHz ITU grid)
DWDM-SFP-4532	Cisco-ANA3.7.X-DP10 , PrimeNetwork-3.8.X-DP1	DWDM SFP 1545.32nm SFP (100 GHz ITU grid)
DWDM-SFP-4612	Cisco-ANA3.7.X-DP10 , PrimeNetwork-3.8.X-DP1	DWDM SFP 1546.12 nm SFP (100 GHz ITU grid)
DWDM-SFP-4692	Cisco-ANA3.7.X-DP10 , PrimeNetwork-3.8.X-DP1	DWDM SFP 1546.92 nm SFP (100 GHz ITU grid)
DWDM-SFP-4772	Cisco-ANA3.7.X-DP10 , PrimeNetwork-3.8.X-DP1	DWDM SFP 1547.72 nm SFP (100 GHz ITU grid)
DWDM-SFP-4851	Cisco-ANA3.7.X-DP10 , PrimeNetwork-3.8.X-DP1	DWDM SFP 1548.51 nm SFP (100 GHz ITU grid)

Table 6-114 Supported Modules for Cisco ASR901—Cisco Prime Network 3.9 (continued)

Module Name	Product_Version	Module Description
DWDM-SFP-4931	Cisco-ANA3.7.X-DP10 , PrimeNetwork-3.8.X-DP1	DWDM SFP 1549.32nm SFP (100 GHz ITU grid)
DWDM-SFP-5012	Cisco-ANA3.7.X-DP10 , PrimeNetwork-3.8.X-DP1	DWDM SFP 1550.12 nm SFP (100 GHz ITU grid)
DWDM-SFP-5092	Cisco-ANA3.7.X-DP10 , PrimeNetwork-3.8.X-DP1	DWDM SFP 1550.92 nm SFP (100 GHz ITU grid)
DWDM-SFP-5172	Cisco-ANA3.7.X-DP10 , PrimeNetwork-3.8.X-DP1	DWDM SFP 1551.72 nm SFP (100 GHz ITU grid)
DWDM-SFP-5252	Cisco-ANA3.7.X-DP10 , PrimeNetwork-3.8.X-DP1	DWDM SFP 1552.52 nm SFP (100 GHz ITU grid)
DWDM-SFP-5332	Cisco-ANA3.7.X-DP10 , PrimeNetwork-3.8.X-DP1	DWDM SFP 1553.33nm SFP (100 GHz ITU grid)
DWDM-SFP-5413	Cisco-ANA3.7.X-DP10 , PrimeNetwork-3.8.X-DP1	DWDM SFP 1554.13 nm SFP (100 GHz ITU grid)

Table 6-114 Supported Modules for Cisco ASR901—Cisco Prime Network 3.9 (continued)

Module Name	Product_Version	Module Description
DWDM-SFP-5494	Cisco-ANA3.7.X-DP10 , PrimeNetwork-3.8.X-DP1	DWDM SFP 1554.94 nm SFP (100 GHz ITU grid)
DWDM-SFP-5575	Cisco-ANA3.7.X-DP10 , PrimeNetwork-3.8.X-DP1	DWDM SFP 1555.75 nm SFP (100 GHz ITU grid)
DWDM-SFP-5655	Cisco-ANA3.7.X-DP10 , PrimeNetwork-3.8.X-DP1	DWDM SFP 1556.55 nm SFP (100 GHz ITU grid)
DWDM-SFP-5736	Cisco-ANA3.7.X-DP10 , PrimeNetwork-3.8.X-DP1	DWDM SFP 1557.36nm SFP (100 GHz ITU grid)
DWDM-SFP-5817	Cisco-ANA3.7.X-DP10 , PrimeNetwork-3.8.X-DP1	DWDM SFP 1558.17 nm SFP (100 GHz ITU grid)
DWDM-SFP-5898	Cisco-ANA3.7.X-DP10 , PrimeNetwork-3.8.X-DP1	DWDM SFP 1558.98 nm SFP (100 GHz ITU grid)
DWDM-SFP-5979	Cisco-ANA3.7.X-DP10 , PrimeNetwork-3.8.X-DP1	DWDM SFP 1559.79 nm SFP (100 GHz ITU grid)

Table 6-114 Supported Modules for Cisco ASR901—Cisco Prime Network 3.9 (continued)

Module Name	Product_Version	Module Description
DWDM-SFP-6061	Cisco-ANA3.7.X-DP10 , PrimeNetwork-3.8.X-DP1	DWDM SFP 1560.61 nm SFP (100 GHz ITU grid)
DWDM-SFP-6141	Cisco-ANA3.7.X-DP10 , PrimeNetwork-3.8.X-DP1	DWDM SFP 1561.42 nm SFP (100 GHz ITU grid)

Cisco ASR901—Supported Technologies

The following technologies are supported by the Cisco ASR901 in Cisco Prime Network 3.9:

- IP, page 6-199
- Routing Protocols, page 6-202
- Ethernet, page 6-205
- PPP, page 6-219
- TDM/DSx, page 6-222
- MPLS, page 6-226
- MPLS-TE, page 6-228
- VPN (VRF), page 6-233
- PWE3, page 6-235
- Security, page 6-237
- Hardware, page 6-238
- Serial, page 6-242
- BFD, page 6-246
- Carrier Ethernet, page 6-247
- CDP, page 6-249
- Discovery Protocol, page 6-249
- Ethernet OAM, page 6-250

Cisco ASR901—Supported Service Events

Table 6-115 Supported Service Events for Cisco ASR901—Cisco Prime Network 3.9

Event Name	Product_Version	Expedited
BFD connectivity down		N
BFD connectivity up		N
BGP process down		N
BGP process up	Cisco-ANA3.7.X-DP10 , PrimeNetwork-3.8.X-DP1	N
CPU utilization exceeded upper threshold	Cisco-ANA3.7.X-DP10 , PrimeNetwork-3.8.X-DP1	N
CPU utilization less than lower threshold		N
Device Unsupported	Cisco-ANA3.7.X-DP10 , PrimeNetwork-3.8.X-DP1	N
GRE tunnel down		N
GRE tunnel up		N
Keepalive configured		N
Keepalive not configured		N
LDP neighbor down		Y
LDP neighbor up		Y
Link down due to admin down		N
Link down due to Card event		N
Link down due to oper down		N
Link down on unreachable		N
Link up	Cisco-ANA3.7.X-DP10 , PrimeNetwork-3.8.X-DP1	N

Table 6-115 Supported Service Events for Cisco ASR901—Cisco Prime Network 3.9 (continued)

Event Name	Product_Version	Expedited
Memory utilization exceeded upper threshold	Cisco-ANA3.7.X-DP10 , PrimeNetwork-3.8.X-DP1	N
Memory utilization less than lower threshold		N
Module Unsupported	Cisco-ANA3.7.X-DP10 , PrimeNetwork-3.8.X-DP1	N
Port down due to admin		N
Port down due to oper		N
BFD neighbor found	Cisco-ANA3.7.X-DP10 , PrimeNetwork-3.8.X-DP1	N
BFD neighbor loss	Cisco-ANA3.7.X-DP10 , PrimeNetwork-3.8.X-DP1	N
Device Managed	Cisco-ANA3.7.X-DP10 , PrimeNetwork-3.8.X-DP1	N
Management Unreachable	Cisco-ANA3.7.X-DP10 , PrimeNetwork-3.8.X-DP1	N

Table 6-115 Supported Service Events for Cisco ASR901—Cisco Prime Network 3.9 (continued)

Event Name	Product_Version	Expedited
Device Partially Managed	Cisco-ANA3.7.X-DP10 , PrimeNetwork-3.8.X-DP1	N
EFP down	Cisco-ANA3.7.X-DP10 , PrimeNetwork-3.8.X-DP1	N
EFP up	Cisco-ANA3.7.X-DP10 , PrimeNetwork-3.8.X-DP1	N
Interface status down	Cisco-ANA3.7.X-DP10 , PrimeNetwork-3.8.X-DP1	N
Interface status up	Cisco-ANA3.7.X-DP10 , PrimeNetwork-3.8.X-DP1	N
OSPF Neighbor Down	Cisco-ANA3.7.X-DP10 , PrimeNetwork-3.8.X-DP1	N
OSPF Neighbor Up	Cisco-ANA3.7.X-DP10 , PrimeNetwork-3.8.X-DP1	N

Table 6-115 Supported Service Events for Cisco ASR901—Cisco Prime Network 3.9 (continued)

Event Name	Product_Version	Expedited
Port up	Cisco-ANA3.7.X-DP10 , PrimeNetwork-3.8.X-DP1	N

Cisco ASR903 Series Routers

This section includes the following information about Cisco ASR903 Series routers (for information on the NE types supported in Cisco Prime Network 3.9, see Cisco ASR903 Series Routers):

- Cisco ASR903 Series—Supported Software Versions, page 6-185
- Cisco ASR903 Series—Supported Topologies, page 6-186
- Cisco ASR903 Series—Supported Modules, page 6-186
- Cisco ASR903 Series—Supported Technologies, page 6-189
- Cisco ASR903 Series—Supported Service Events, page 6-189

Cisco ASR903 Series—Supported Software Versions

Table 6-116 Supported Software Versions for Cisco ASR903 Series—Cisco Prime Network 3.9

Software Version	Product_Version
IOS 15.2	Prime Network 3.8-DP2
IOS 15.2(1)S1	Cisco-ANA-3.7.x-DP13, Cisco-ANA-3.8-DP4
IOS 15.2(2)S	Cisco-ANA-3.7.x-DP14, Cisco-ANA-3.8-DP5

Cisco ASR903 Series—Supported Topologies

Table 6-117 Supported Topologies for Cisco ASR903 Series—Cisco Prime Network 3.9

Topology Type	Link Type	Product_Version
ATM	ATM	3.8
BGP	BGP	3.8
Ethernet	Ethernet	3.8
Framerelay	Framerelay	3.8
MPLS	MPLS	3.8
PPP/HDLC	PPP or HDLC	3.8
Physical Layer	Physical Layer	3.8
LAG	LAG	3.8
MLPPP	MLPPP	3.8
BFD	BFD	3.8
MPLS-TP	Tunnel	Prime Network 3.8

Cisco ASR903 Series—Supported Modules

Table 6-118 Supported Modules for Cisco ASR903 Series—Cisco Prime Network 3.9

Module Name	Product_Version	Module Description
A903-FAN	Prime Network 3.8-DP2	ASR 903 FAN
A900-PWR550-D	Prime Network 3.8-DP2	ASR 900 500W DC Power Supply
A903-RSP1A-55	Prime Network 3.8-DP2	ASR 900 Route Switch Processor 1, basic service scale, 55Gbps throughput
A903-RSP1B-55	Prime Network 3.8-DP2	ASR 900 Route Switch Processor 1, basic service scale, 55Gbps throughput
A900-IMA8T	Prime Network 3.8-DP2	A900-IMA8T
A900-IMA8S	Prime Network 3.8-DP2	8-port Gigabit Ethernet Interface Module

Table 6-118 Supported Modules for Cisco ASR903 Series—Cisco Prime Network 3.9 (continued)

Module Name	Product_Version	Module Description
A900-IMA1X	Prime Network 3.8-DP2	1-port Ten Gigabit Ethernet XFP Interface Module
A900-IMA16D	Prime Network 3.8-DP2	A900-IMA16D
GLC-FE-100FX-RGD	Prime Network 3.8-DP2	100BASE FX-GE
GLC-LX-SM-RGD	Prime Network 3.8-DP2	GE LX
GLC-SX-MM-RGD	Prime Network 3.8-DP2	GE SX
GLC-ZX-SM-RGD	Prime Network 3.8-DP2	GE ZX
GLC-BX-U	Prime Network 3.8-DP2	1000BASE BX10-U
GLC-BX-D	Prime Network 3.8-DP2	1000BASE BX10-D
GLC-EX-SMD	Prime Network 3.8-DP2	GE EX
SFP-GE-T	Prime Network 3.8-DP2	GE T
XFP-10GLR192SR-RGD	Prime Network 3.8-DP2	OC192 + 10GBASE-S
XFP-10GER192IR-RGD	Prime Network 3.8-DP2	OC192 + 10GBASE-E
XFP-10GZR192LR-RGD	Prime Network 3.8-DP2	OC192 + 10GBASE-L
XFP-10G-MM-SR	Prime Network 3.8-DP2	10GBASE-SR

Table 6-118 Supported Modules for Cisco ASR903 Series—Cisco Prime Network 3.9 (continued)

Module Name	Product_Version	Module Description
DWDM-XFP-C	Prime Network 3.8-DP2	TUNABLE DWDM XFP
A900-IMA4OS	Prime Network 3.8-DP5	4 port OC3/1 port OC12 IM
SFP-GE-S	Prime Network 3.8-DP5	GE SX
ONS-SI-155-SR-MM	Prime Network 3.8-DP5	OC3 SR-1/STM1 MM
ONS-SI-155-I1	Prime Network 3.8-DP5	OC3 IR-1/STM1 S-1.1
ONS-SI-155-L1	Prime Network 3.8-DP5	OC3 LR-1/STM1 L-1.1
ONS-SI-155-L2	Prime Network 3.8-DP5	OC3 LR-2/STM1 L-1.2
SFP-OC3-MM	Prime Network 3.8-DP5	OC3 SR-1/STM1 MM
ONS-SC-155-EL	Prime Network 3.8-DP5	STM-1E
DWDM-SFP-3033	Prime Network 3.8-DP5	DWDM SFP 1530.33
CWDM-SFP-1610	Prime Network 3.8-DP5	GE CWDM 1610
GLC-ZX-SMD	Prime Network 3.8-DP5	GE ZX
GLC-SX-MMD	Prime Network 3.8-DP5	GE SX
GLC-LH-SMD	Prime Network 3.8-DP5	GE LX

Table 6-118 Supported Modules for Cisco ASR903 Series—Cisco Prime Network 3.9 (continued)

Module Name	Product_Version	Module Description
XFP10GLR-192SR-L	Prime Network 3.8-DP5	OC192 + 10GBASE-L
XFP10GER-192IR-L	Prime Network 3.8-DP5	OC192 + 10GBASE-E
XFP-10GZR-OC192LR	Prime Network 3.8-DP5	OC192 + 10GBASE-Z
SFP-OC3-SR	Prime Network 3.8-DP5	OC3 SR-1/STM1 I-1
SFP-OC3-IR1	Prime Network 3.8-DP5	OC3 IR-1/STM1 S-1.1
DWDM-SFP-6141	Prime Network 3.8-DP5	DWDM SFP 1561_41
CWDM-SFP-1470	Prime Network 3.8-DP5	GE CWDM 1470

Cisco ASR903 Series—Supported Technologies

The following technologies are supported by the Cisco ASR903 Series in Cisco Prime Network 3.9:

Cisco ASR903 Series—Supported Service Events

Table 6-119 Supported Service Events for Cisco ASR903 Series—Cisco Prime Network 3.9

Event Name	Product_Version	Expedited
Active IP Interfaces Found	3.8	Y
All IP Interfaces Down	3.8	Y
BFD connectivity down	3.8	N
BFD connectivity up	3.8	N
BFD neighbor found	3.8	N
BFD neighbor loss	3.8	N
BGP link down due to admin	3.8	Y
BGP link down due to oper	3.8	Y

Table 6-119 Supported Service Events for Cisco ASR903 Series—Cisco Prime Network 3.9

Event Name	Product_Version	Expedited
BGP link down vrf due to admin	3.8	N
BGP link down vrf due to oper	3.8	N
BGP link up	3.8	Y
BGP neighbor found	3.8	N
BGP neighbor loss due to admin	3.8	N
BGP neighbor loss due to oper	3.8	N
BGP neighbor loss VRF due to admin	3.8	N
BGP neighbor loss VRF due to oper	3.8	N
BGP process down	3.8	N
BGP process up	3.8	N
Card Down	3.8	Y
Card In	3.8	Y
Card Out	3.8	Y
Card Up	3.8	Y
CGN statistics dropsPortLimitIn2Out higher threshold exceeded	3.8	N
CGN statistics dropsPortLimitIn2Out lower threshold exceeded	3.8	N
CGN statistics dropsPortLimitIn2Out threshold normal	3.8	N
CGN statistics dropsResourceDepletionIn2Out higher threshold exceeded	3.8	N
CGN statistics dropsResourceDepletionIn2Out lower threshold exceeded	3.8	N
CGN statistics dropsResourceDepletionIn2Out threshold normal	3.8	N
CGN statistics dropsSystemLimitIn2Out higher threshold exceeded	3.8	N
CGN statistics dropsSystemLimitIn2Out lower threshold exceeded	3.8	N
CGN statistics dropsSystemLimitIn2Out threshold normal	3.8	N
CGN statistics fwdIn2Out higher threshold exceeded	3.8	N

Table 6-119 Supported Service Events for Cisco ASR903 Series—Cisco Prime Network 3.9

Event Name	Product_Version	Expedited
CGN statistics fwdIn2Out lower threshold exceeded	3.8	N
CGN statistics fwdIn2Out threshold normal	3.8	N
CGN statistics fwdOut2In higher threshold exceeded	3.8	N
CGN statistics fwdOut2In lower threshold exceeded	3.8	N
CGN statistics fwdOut2In threshold normal	3.8	N
CGN statistics translationsCreate higher threshold exceeded	3.8	N
CGN statistics translationsCreate lower threshold exceeded	3.8	N
CGN statistics translationsCreate threshold normal	3.8	N
CGN statistics translationsDelete higher threshold exceeded	3.8	N
CGN statistics translationsDelete lower threshold exceeded	3.8	N
CGN statistics translationsDelete threshold normal	3.8	N
CPU utilization exceeded upper threshold	3.8	N
CPU utilization less than lower threshold	3.8	N
Device Unsupported	3.8	N
Discarded packet rate exceeded upper threshold	3.8	N
Discarded packet rate is below lower threshold	3.8	N
Dropped packet rate exceeded upper threshold	3.8	N
Dropped packet rate is below lower threshold	3.8	N
DS0 Bundle Admin down	3.8	N
DS0 Bundle Oper down	3.8	N
DS0 Bundle Up	3.8	N
DS1 Path down due to Admin	3.8	N
DS1 Path down due to Card	3.8	N

Table 6-119 Supported Service Events for Cisco ASR903 Series—Cisco Prime Network 3.9

Event Name	Product_Version	Expedited
DS1 Path down due to Oper	3.8	N
DS1 Path link down due to Admin down	3.8	N
DS1 Path Link down due to Card event	3.8	N
DS1 Path link down due to Oper down	3.8	N
DS1 Path Link down on unreachable	3.8	N
DS1 Path link Up	3.8	N
DS1 Path up	3.8	N
DS3 path link down due to admin down	3.8	N
DS3 path link down due to oper down	3.8	N
DS3 path link down on unreachable	3.8	N
DS3 path link up	3.8	N
Dual stack IP added	3.8	N
Dual stack IP removed	3.8	N
DWDM controller down	3.8	N
DWDM controller up	3.8	N
DWDM g709 status down	3.8	N
DWDM g709 status up	3.8	N
EFP down due to error disabled	3.8	N
GRE tunnel down	3.8	N
GRE tunnel up	3.8	N
High Priority MPLS-TE tunnel down	3.8	N
IMA Administratively down	3.8	N
IMA Administratively up	3.8	N
IMA Operationally down	3.8	N
IMA Operationally up	3.8	N
IP pools exhausted	3.8	N
IP pools normal	3.8	N
Keepalive configured	3.8	N
Keepalive not configured	3.8	N
l2tp peer established	3.8	N
l2tp peer is removed	3.8	N
l2tp peer not established	3.8	N
LAG link up	3.8	N

Table 6-119 Supported Service Events for Cisco ASR903 Series—Cisco Prime Network 3.9

Event Name	Product_Version	Expedited
LAG up	3.8	N
Layer 2 Tunnel Down	3.8	N
Layer 2 tunnel up	3.8	N
LDP neighbor down	3.8	Y
LDP neighbor up	3.8	Y
Link down due to admin down	3.8	N
Link down due to Card event	3.8	N
Link down due to oper down	3.8	N
Link down on unreachable	3.8	N
Link over utilized	3.8	N
Link up	3.8	N
Link utilization normal	3.8	N
Logical port up	3.8	N
Low Priority MPLS-TE tunnel down	3.8	N
Medium Priority MPLS-TE tunnel down	3.8	N
Memory utilization exceeded upper threshold	3.8	N
Memory utilization less than lower threshold	3.8	N
MLPPP Administratively down	3.8	N
MLPPP Operationaly down	3.8	N
MLPPP Up	3.8	N
Module Unsupported	3.8	N
MPLS Black hole cleared	3.8	N
MPLS Black Hole found	3.8	N
MPLS interface added	3.8	Y
MPLS interface removed	3.8	Y
MPLS TE FRR State Changed to Active	3.8	N
MPLS TE FRR State Changed to Ready	3.8	N
MPLS-TE tunnel reoptimized	3.8	N
MPLS-TE tunnel rerouted	3.8	N
MPLS-TE tunnel up	3.8	N
MPLS-TP TP Tunnel Down	3.8	N
MPLS-TP LSP Down	3.8	N

Table 6-119 Supported Service Events for Cisco ASR903 Series—Cisco Prime Network 3.9

Event Name	Product_Version	Expedited
MPLS-TP Bandwidth mismatch	3.8	N
OSPFneighbor down	3.8	N
OSPFneighbor up	3.8	N
Pluggable transceiver out	3.8	N
power-supply down	3.8	N
Power-supply out	3.8	N
Port down due to admin	3.8	N
Port down due to Card down	3.8	N
Port down due to Card out	3.8	N
Port down due to oper	3.8	N
Primary HSRP Interface Active	3.8	N
rep port role change	3.8	Y
Primary HSRP Interface not Active	3.8	N
Rx dormant normal	3.8	N
Rx utilization exceeded upper threshold	3.8	N
Rx utilization is below lower threshold	3.8	N
Secondary HSRP Interface Active	3.8	N
Secondary HSRP Interface not Active	3.8	N
Shelf in	3.8	N
Shelf out	3.8	N
SONET Path down due to Admin	3.8	N
SONET Path down due to Card	3.8	N
Sonet Path link down due to Admin down	3.8	N
SONET Path Link down due to Card event	3.8	N
SONET Path Link down due to Oper down	3.8	N
SONET Path Link down on unreachable	3.8	N
Sonet Path link Up	3.8	N
SONET Path up	3.8	N
Tx dormant normal	3.8	N
Tx utilization exceeded upper threshold	3.8	N

Table 6-119 Supported Service Events for Cisco ASR903 Series—Cisco Prime Network 3.9

Event Name	Product_Version	Expedited
Tx utilization is below lower threshold	3.8	N
VC changed	3.8	N
VC removed	3.8	N
VC restored	3.8	N
VLAN Sub Interface down	3.8	N
VLAN Sub Interface up	3.8	N
VSI Down	3.8	N
Device Managed	3.8	N
Management Unreachable	3.8	N
Device Partially Managed	3.8	N
DS3 Path Link down due to Card event	3.8	N
DS3 Path down due to Admin	3.8	N
DS3 Path down due to Card	3.8	N
DS3 Path down due to Oper	3.8	N
DS3 Path up	3.8	N
EFP down	3.8	N
EFP up	3.8	N
fan-tray down	3.8	N
Fan-tray out	3.8	N
Interface status up	3.8	N
LAG down	3.8	N
LAG Link down	3.8	N
Logical port down	3.8	N
MPLS-TE tunnel down	3.8	N
Port up	3.8	N
rx dormant	3.8	N
Service down	3.8	N
Service up	3.8	N
tx dormant	3.8	N
VSI up	3.8	N
High priority member down	3.8	N
Low priority member down	3.8	N
Medium priority member down	3.8	N
Local switching entry down	3.8	N

Table 6-119 Supported Service Events for Cisco ASR903 Series—Cisco Prime Network 3.9

Event Name	Product_Version	Expedited
Local switching entry up	3.8	N
Interface status down	3.8	N

Cisco ASR 5000 Series Routers

This section includes the following information about Cisco ASR 5000 Series routers (for information on the NE types supported in Cisco Prime Network 3.9, see Cisco ASR 5000 Series Routers):

- Cisco ASR 5000 Series—Supported Software Versions, page 6-196
- Cisco ASR 5000 Series—Supported Topologies, page 6-196
- Cisco ASR 5000 Series—Supported Modules, page 6-197
- Cisco ASR 5000 Series—Supported Technologies, page 6-197

Cisco ASR 5000 Series—Supported Software Versions

Table 6-120 Supported Software Versions for Cisco ASR 5000 Series—Cisco Prime Network 3.9

Software Version	Product_Version
StarOS 10.0	
StarOS 11.0	
StarOS 12.0	
StarOS 12.2	
StarOS 12.3	

Cisco ASR 5000 Series—Supported Topologies

Table 6-121 Supported Topologies for Cisco ASR 5000 Series—Cisco Prime Network 3.9

Topology Type	Link Type	Product_Version
Ethernet	Ethernet	

Cisco ASR 5000 Series—Supported Modules

Table 6-122 Supported Modules for Cisco ASR 5000 Series—Cisco Prime Network 3.9

Module Name	Product_Version	Module Description
ASR5K-01100E-K9		FELC Ethernet 10/100 Line Card
ASR5K-0110G-MM-K9		XGLC 1-Port 10 Gigabit Ethernet Line Card w/MM SFP+
ASR5K-0110G-SM-K9		XGLC 1-Port 10 Gigabit Ethernet Line Card w/SM SFP+
ASR5K-011GE-LX-K9		GELC Ethernet 1000 Line Card w/LX Single-Mode SFP
ASR5K-011GE-SX-K9		GELC Ethernet 1000 Line Card w/SX Multi-Mode Short Haul SFP
ASR5K-011GE-T-K9		GELC Ethernet 1000 Line Card w/Copper SFP
ASR5K-041GE-LX-K9		QGLC 4-Port Ethernet 1000 Line Card with LX SM SFP
ASR5K-041GE-SX-K9		QGLC 4-Port Ethernet 1000 Line Card with SX MM Short Haul SFP
ASR5K-041GE-T-K9		QGLC 4-Port Ethernet 1000 Line Card with copper SFP
ASR5K-PSC-32G-K9		Packet Services Card 32GB
ASR5K-RCC-K9		Redundancy crossbar
ASR5K-SMC-K9		System Management Card
ASR5K-SPIO-3PN-K9		Switch Processor Input/Output Switch Processor I/O, 3-Pin BITS
ASR5K-SPIO-BNC-K9		Switch Processor Input/Output Switch Processor I/O, BNC BITS with Stratum 3 module
ASR55-MIO-10GL20-K9		Management Input/Output (MIO) with (2) 10 X 10GBASE-LR daughter cards
ASR55-MIO-10GS20-K9		Management Input/Output (MIO) with (2) 10 X 110GBASE-SR daughter cards
ASR55-DPC-K9		Data Processing Card (DPC)
ASR-55-FSC-K9		Fabric and Storage Card (FSC)
ASR55-SSC-K9		System Status Card (SSC)

Cisco ASR 5000 Series—Supported Technologies

The following technologies are supported by the Cisco ASR 5000 Series in Cisco Prime Network 3.9:

- IP, page 6-199
- Routing Protocols, page 6-202

- Ethernet, page 6-205
- VPN (VRF), page 6-233
- Security, page 6-237
- Hardware, page 6-238
- Serial, page 6-242
- Mobile, page 6-266

Supported Technologies on Cisco Routers

The following sections list the objects and attributes that are supported on Cisco routers in Cisco Prime Network 3.9 per technology:

- IP, page 6-199
- Routing Protocols, page 6-202
- Ethernet, page 6-205
- ATM, page 6-213
- Frame Relay, page 6-217
- PPP, page 6-219
- HDLC, page 6-220
- SONET/SDH, page 6-220
- TDM/DSx, page 6-222
- MPLS, page 6-226
- MPLS-TE, page 6-228
- MPLS-TP, page 6-231
- VPN (VRF), page 6-233
- PWE3, page 6-235
- Security, page 6-237
- Hardware, page 6-238
- Serial, page 6-242
- Additional Technologies, page 6-243
- IPoDWDM, page 6-243
- LocalSwitching, page 6-245
- BFD, page 6-246
- Carrier Ethernet, page 6-247
- CDP, page 6-249
- Discovery Protocol, page 6-249
- Ethernet OAM, page 6-250
- CGN, page 6-254
- SBC, page 6-256

- AccessGatewayService, page 6-262
- 6PE, page 6-264
- 6rd, page 6-264
- MLACP, page 6-265
- IPSec, page 6-266
- Mobile, page 6-266

IP

Table 6-123 IP Attribute Support on Cisco Routers—Cisco Prime Network 3.9

Attribute	800	1000	1600	1700	1800	2500	2600	2800	3600	3700	3800	7200	7300	7400	7500	7600	10000	12000	XR 12000	CRS	ASR 9000	ASR 1000	MWR 2941	ISR1900	ISR2900	ISR 3900	UBR7200	UBR10000	Cisco 4700	ASR901	ASR903	ASR 5000
IMO Name—IIPInterface																																
IP Address	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y
Subnetwork Mask	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y
IP Interface Addresses Array	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y
Interface Name	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y
Interface Description	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	
IP Interface State	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y
OSPF Interface Cost																																
Broadcast Address																																
MTU																																
Lookup Method																																
Address Resolution Type																																
ARP Timeout																																
Secured ARP																																
ICMP Mask Reply																																
IGMP Proxy																																
HSRP Groups		Y			Y	Y		Y	Y	Y	Y	Y		Y		Y	Y	Y					Y			Y	Y	Y	Y	Y	Y	
IP Multiplexing Table																																
IANA Type	Y		Y	Y		Y	Y	Y																								
Containing CTPs																																
Contained CTPs																																

Table 6-123 IP Attribute Support on Cisco Routers—Cisco Prime Network 3.9 (continued)

Attribute	800	1000	1600	1700	1800	2500	2600	2800	3600	3700	3800	7200	7300	7400	7500	7600	10000	12000	XR 12000	CRS	ASR 9000	ASR 1000	MWR 2941	ISR1900	ISR2900	ISR 3900	UBR7200	UBR10000	Cisco 4700	ASR901	ASR903	ASR 5000
IMO Name—IIPMuxEntry																																
Termination Point	Y	Y		Y	Y	Y	Y	Y	Y	Y		Y		Y		Y	Y	Y					Y			Y	Y	Y	Y	Y	Y	
Destination IP Subnet	Y	Y		Y	Y	Y	Y	Y	Y	Y		Y		Y		Y	Y	Y					Y			Y	Y	Y	Y	Y	Y	
IMO Name—IRoutingEntity																																
Routing Table	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y
ARP Entity	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y		Y		Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y
Routing Table Changes													Y		Y													Y				
Name	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y
Logical Sons	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y
IMO Name—IRoutingEntry																																
Destination IP Subnet	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y
Next Hop IP Address	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y
Type	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y
Routing Protocol Type	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y
Outgoing Interface Name	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y
IMO Name—IARPEntity																																
ARP Table	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y
IMO Name—IARPEntry																																
IP Address	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y
MAC Address	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y
Port	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y
Entry Type	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y		Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y
IMO Name—IIPPool																																
IP Address Pool Entries																																
Name																																
Index																																
IMO Name—IIPRangeBasedIPPoolEntry																																
Start IP Address																																
End IP Address																																

Table 6-123 IP Attribute Support on Cisco Routers—Cisco Prime Network 3.9 (continued)

Attribute	800	1000	1600	1700	1800	2500	2600	2800	3600	3700	3800	7200	7300	7400	7500	7600	10000	12000	XR 12000	CRS	ASR 9000	ASR 1000	MWR 2941	ISR1900	ISR2900	ISR 3900	UBR7200	UBR10000	Cisco 4700	ASR901	ASR903	ASR 5000
Unused Addresses																																
Used Addresses																																
Reserved Addresses																																
IMO Name—IIPSubnetBasedIPPoolEntry																																
IP Subnet																																
Unused Addresses																																
Used Addresses																																
Reserved Addresses																																
IMO Name—HSRPGroupEntry																																
Group Number			Y	Y	Y	Y	Y		Y	Y		Y		Y		Y	Y	Y				Y	Y [1]			Y	Y	Y	Y		Y	
Port Description			Y	Y	Y	Y	Y	Y	Y	Y	Y	Y		Y		Y	Y	Y				Y	Y [2]			Y	Y	Y	Y		Y	
Priority			Y	Y	Y	Y	Y	Y	Y	Y	Y	Y		Y		Y	Y	Y				Y	Y [3]			Y	Y	Y	Y		Y	
Coupled Router			Y	Y	Y	Y	Y	Y	Y	Y	Y	Y		Y		Y	Y	Y				Y	Y [4]			Y	Y	Y	Y		Y	
State			Y	Y	Y	Y	Y	Y	Y	Y	Y	Y		Y		Y	Y	Y				Y	Y [5]			Y	Y	Y	Y		Y	
Tracking Interfaces																																
Virtual IP Address			Y	Y	Y	Y	Y	Y	Y	Y	Y	Y		Y		Y	Y	Y				Y	Y [6]			Y	Y	Y	Y		Y	
Virtual MAC Address			Y	Y	Y	Y	Y	Y	Y	Y	Y	Y		Y		Y	Y	Y				Y	Y [7]			Y	Y	Y	Y		Y	
IMO Name—ITunnelGRE																																
Name	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y		Y		Y	Y	Y				Y	Y			Y			Y		Y	
Tunnel Destination and Source	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y		Y		Y	Y	Y				Y	Y			Y			Y		Y	
IP Address	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y		Y		Y	Y	Y				Y	Y			Y			Y		Y	
IP Interface State								Y			Y	Y					Y	Y														
IANA Type								Y																								
Containing CTPs																																
Contained CTPs																																
Keep Alive Time												Y				Y															Y	
Keep Alive Retry												Y				Y															Y	

Table 6-123 IP Attribute Support on Cisco Routers—Cisco Prime Network 3.9 (continued)

Attribute	800	1000	1600	1700	1800	2500	2600	2800	3600	3700	3800	7200	7300	7400	7500	7600	10000	12000	XR 12000	CRS	ASR 9000	ASR 1000	MWR 2941	ISR1900	ISR2900	ISR 3900	UBR7200	UBR10000	Cisco 4700	ASR901	ASR903	ASR 5000
IMO Name—IVrrpGroupEntry																																
Group Number																Y			Y	Y	Y	Y									Y	
State																Y			Y	Y	Y	Y									Y	
Port Description																Y			Y	Y	Y	Y									Y	
Master IP Address																Y			Y	Y	Y	Y									Y	
Primary IP Address																Y			Y	Y	Y	Y									Y	
Priority																Y			Y	Y	Y	Y									Y	
Virtual Mac Address																Y			Y	Y	Y	Y									Y	
Preempt Mode																Y			Y	Y	Y	Y									Y	
Admin State																Y			Y	Y	Y	Y									Y	
Advertisement Interval																Y			Y	Y	Y	Y									Y	
Tracking Interfaces																Y			Y	Y	Y	Y									Y	
IMO Name—IIPSLAResponderService																																
responderStatus																																
TWAMPResponder Status																																
tcpConnect																																
udpEcho																																
IMO Name—IIPAddressPortPair																																
type																																
ipAddress																																
port																																

[1, 2, 3, 4, 5, 6, 7]Not Supported on IOS 12.2(33)MRA (CSR3.2)

Routing Protocols

Table 6-124 Routing Protocols Attribute Support on Cisco Routers—Cisco Prime Network 3.9

Attribute	800	1000	1600	1700	1800	2500	2600	2800	3600	3700	3800	7200	7300	7400	7500	7600	10000	12000	XR 12000	CRS	ASR 9000	ASR 1000	MWR 2941	ISR1900	ISR2900	ISR 3900	UBR7200	UBR10000	Cisco 4700	ASR901	ASR903	ASR 5000
IMO Name—IBgpNeighborEntry																																
Remote Identifier	Y		Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y		Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y

Table 6-124 Routing Protocols Attribute Support on Cisco Routers—Cisco Prime Network 3.9 (continued)

Attribute	800	1000	1600	1700	1800	2500	2600	2800	3600	3700	3800	7200	7300	7400	7500	7600	10000	12000	XR 12000	CRS	ASR 9000	ASR 1000	MWR 2941	ISR1900	ISR2900	ISR 3900	UBR7200	UBR10000	Cisco 4700	ASR901	ASR903	ASR 5000
Neighbor Type				Y		Y	Y	Y			Y							Y	Y	Y	Y											Y
Distributing Interfaces											Y																					
Remote Address	Y		Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y
Remote Autonomous System	Y		Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y
Peer State	Y		Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y
Peer AdminState											Y	Y					Y	Y	Y	Y	Y	Y	Y							Y		Y
Hold Time	Y		Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y
Keep Alive Time	Y		Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y
VrfName																			Y	Y			Y							Y		Y
Address family												Y	Y		Y	Y		Y		Y			Y			Y	Y		Y	Y	Y	Y
IMO Name—IOspfEntry																																
Area Identifier	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y		Y	Y	Y	Y	Y	
IP Address	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y		Y	Y	Y	Y	Y	
Type	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y		Y	Y	Y	Y	Y	
Administrative Status	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y		Y	Y	Y	Y	Y	
Ospf Entry State	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y		Y	Y	Y	Y	Y	
IMO Name—IOspfProcess																																
Process Id												Y				Y			Y	Y	Y			Y	Y	Y				Y	Y	
OSPF Version												Y				Y			Y	Y	Y			Y	Y	Y				Y	Y	
Router Id												Y				Y			Y	Y	Y			Y	Y	Y				Y	Y	
IMO Name—IOspfNeighbor																																
Neighbor Id												Y				Y			Y	Y	Y			Y	Y	Y				Y	Y	
Outgoing Interface												Y				Y			Y	Y	Y			Y	Y	Y				Y	Y	
State												Y				Y			Y	Y	Y			Y	Y	Y				Y	Y	
Neighbor Interface Address												Y				Y			Y	Y	Y			Y	Y	Y				Y	Y	
Area Id												Y				Y			Y	Y	Y			Y	Y	Y				Y	Y	
IMO Name—IOspfInterface																																
Area Id												Y				Y			Y	Y	Y			Y	Y	Y				Y	Y	
Network Type												Y				Y			Y	Y	Y			Y	Y	Y				Y	Y	
Cost												Y				Y			Y	Y	Y			Y	Y	Y				Y	Y	
State												Y				Y			Y	Y	Y			Y	Y	Y				Y	Y	

Table 6-124 Routing Protocols Attribute Support on Cisco Routers—Cisco Prime Network 3.9 (continued)

Attribute	800	1000	1600	1700	1800	2500	2600	2800	3600	3700	3800	7200	7300	7400	7500	7600	10000	12000	XR 12000	CRS	ASR 9000	ASR 1000	MWR 2941	ISR1900	ISR2900	ISR 3900	UBR7200	UBR10000	Cisco 4700	ASR901	ASR903	ASR 5000
Interface Address																							Y	Y							Y	Y
Type												Y				Y			Y	Y	Y			Y	Y	Y				Y	Y	
IF Proirity												Y				Y			Y	Y	Y			Y	Y	Y				Y	Y	
DR Id												Y				Y			Y	Y	Y			Y	Y	Y				Y	Y	
BDR Id												Y				Y			Y	Y	Y			Y	Y	Y				Y	Y	
IMO Name—ISpfTimers																																
Schedule Delay												Y				Y			Y	Y	Y			Y	Y	Y				Y	Y	
Min Hold Time												Y				Y			Y	Y	Y			Y	Y	Y				Y	Y	
Max Wait Time												Y				Y			Y	Y	Y			Y	Y	Y				Y	Y	
IMO Name—IISISProcess																																
ISIS Version																Y			Y	Y	Y									Y	Y	
Manual Area Address																Y			Y	Y	Y									Y	Y	
IS Type																Y			Y	Y	Y									Y	Y	
System Id																Y			Y	Y	Y									Y	Y	
Process Id																Y			Y	Y	Y									Y	Y	
IMO Name—IISISMetric																																
IS Type																Y			Y	Y	Y									Y	Y	
Metric Style																Y			Y	Y	Y									Y	Y	
Metric Value																Y			Y	Y	Y									Y	Y	
Address Family																Y			Y	Y	Y									Y	Y	
IMO Name—IISISInterface																																
Interface Name																Y			Y	Y	Y									Y	Y	
IMO Name—IISISNeighbor																																
IS Type																Y			Y	Y	Y									Y	Y	
System Id																Y			Y	Y	Y									Y	Y	
Admin State																Y			Y	Y	Y									Y	Y	
Hold Time																Y			Y	Y	Y									Y	Y	
SNPA																Y			Y	Y	Y									Y	Y	
Interface Name																Y			Y	Y	Y									Y	Y	
IP Address																Y			Y	Y	Y									Y	Y	
Adress Family																Y			Y	Y	Y									Y	Y	

Ethernet

Table 6-125 Ethernet Attribute Support on Cisco Routers—Cisco Prime Network 3.9

Attribute	800	1000	1600	1700	1800	2500	2600	2800	3600	3700	3800	7200	7300	7400	7500	7600	10000	12000	XR 12000	CRS	ASR 9000	ASR 1000	MWR 2941	ISR1900	ISR2900	ISR 3900	UBR7200	UBR10000	Cisco 4700	ASR901	ASR903	ASR 5000
IMO Name—ILinkAggregationGroup802dot3ad																																
dot3adAggMACAddress										Y				Y[1]		Y		Y[2]	Y	Y	Y					Y				Y	Y	
dot3adAggActorSystemPriority					Y					Y				Y[3]		Y		Y[4]	Y	Y	Y					Y				Y	Y	
dot3adAggActorSystemID										Y				Y[5]		Y		Y[6]	Y	Y	Y					Y				Y	Y	
dot3adAggActorAdminKey										Y				Y[7]		Y		Y[8]	Y	Y	Y					Y				Y	Y	
dot3adAggActorOperKey										Y				Y[9]		Y		Y[10]	Y	Y	Y					Y				Y	Y	
dot3adAggPartnerSystemID										Y				Y[11]		Y		Y[12]	Y	Y	Y					Y				Y	Y	
dot3adAggPartnerSystemPriority										Y				Y[13]		Y		Y[14]	Y	Y	Y					Y				Y	Y	
dot3adAggPartnerOperKey										Y				Y[15]		Y		Y[16]	Y	Y	Y					Y				Y	Y	
dot3adAggCollectorMaxDelay								Y		Y				Y[17]		Y		Y[18]	Y	Y	Y					Y				Y	Y	
GroupNumber										Y				Y[19]		Y		Y	Y	Y	Y					Y				Y	Y	
AggregationProtocolType										Y				Y[20]		Y		Y	Y	Y	Y					Y				Y	Y	
MacAddress										Y				Y[21]		Y		Y	Y	Y	Y					Y				Y	Y	
ChannelAdminStatus										Y				Y[22]		Y		Y	Y	Y	Y					Y				Y	Y	

Table 6-125 Ethernet Attribute Support on Cisco Routers—Cisco Prime Network 3.9 (continued)

Attribute	800	1000	1600	1700	1800	2500	2600	2800	3600	3700	3800	7200	7300	7400	7500	7600	10000	12000	XR 12000	CRS	ASR 9000	ASR 1000	MWR 2941	ISR1900	ISR2900	ISR 3900	UBR7200	UBR10000	Cisco 4700	ASR901	ASR903	ASR 5000
ChannelOperStatus										Y				Y [2] [3]		Y		Y	Y	Y	Y					Y				Y	Y	
IMO Name—IEthernet																																
MAC Address	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y		Y	Y	Y	Y
Duplex Mode																														Y		
Output Flow Control																														Y		
Input Flow Control																																
IANA Type	Y			Y	Y	Y	Y					Y		Y			Y		Y	Y	Y						Y					
Containing CTPs																																
Contained CTPs																																
Port Type																																
isElmiEnabled																Y														Y	Y	
isLOAMEnabled																Y					Y		Y	Y	Y	Y				Y	Y	
IMO Name—IVlanInterface																																
Mode																Y							Y							Y	Y	Y
Native VLAN Identification				Y	Y																		Y							Y		
Virtual LAN Table								Y																								
IANA Type				Y	Y						Y																					
Containing CTPs																																
Contained CTPs																																
vlanAdminType																Y		Y												Y	Y	Y
vlanencapType																Y		Y												Y	Y	Y
getAccess																																
Allowed Vlans																Y		Y												Y	Y	Y
IMO Name—IVlanEncapMux																																
IANA Type				Y	Y				Y							Y							Y							Y		
Containing CTPs																																
Contained CTPs																																
IMO Name—IVlanMapping																																
direction																Y										Y						
vlanMatchCriteria																Y										Y						
vlanRewriteDefinition																Y										Y						

Table 6-125 Ethernet Attribute Support on Cisco Routers—Cisco Prime Network 3.9 (continued)

Attribute	800	1000	1600	1700	1800	2500	2600	2800	3600	3700	3800	7200	7300	7400	7500	7600	10000	12000	XR 12000	CRS	ASR 9000	ASR 1000	MWR 2941	ISR1900	ISR2900	ISR 3900	UBR7200	UBR10000	Cisco 4700	ASR901	ASR903	ASR 5000
Drop																Y										Y						
Vlan																Y										Y						
innerVlan																Y										Y						
translatedVlan																Y										Y						
translatedInnerVlan																Y										Y						
IMO Name—IIEEE802																																
VLAN Identification	Y				Y		Y	Y		Y	Y	Y	Y	Y	Y	Y	Y	Y		Y	Y	Y	Y			Y	Y	Y	Y	Y	Y	
Binding Information																																
Binding Status																																
IANA Type							Y	Y	Y	Y		Y	Y	Y	Y	Y	Y	Y		Y	Y	Y	Y			Y	Y	Y	Y	Y	Y	
Containing CTPs																																
Contained CTPs																																
IMO Name—IStpService																																
StpProtocol	Y													Y		Y					Y		Y						Y		Y	
StpMaxAge	Y										Y			Y		Y				[24]			Y						Y		Y	
StpHelloTime	Y										Y			Y		Y				[25]			Y						Y		Y	
StpBridgeForwardDelay	Y										Y			Y		Y				[26]			Y						Y		Y	
StpInstanceInfoTable	Y										Y			Y		Y				[27]	Y [28]		Y						Y		Y	
Same as ISystemService																																
StpUplinkFastState	Y										Y			Y		Y							Y						Y		Y	
StpBackboneFastState	Y										Y			Y		Y							Y						Y		Y	
StpForwardDelay	Y													Y		Y					Y [29]		Y						Y		Y	
StpBridgeMaxAge	Y													Y		Y					Y [30]		Y						Y		Y	

Table 6-125 Ethernet Attribute Support on Cisco Routers—Cisco Prime Network 3.9 (continued)

Attribute	800	1000	1600	1700	1800	2500	2600	2800	3600	3700	3800	7200	7300	7400	7500	7600	10000	12000	XR 12000	CRS	ASR 9000	ASR 1000	MWR 2941	ISR1900	ISR2900	ISR 3900	UBR7200	UBR10000	Cisco 4700	ASR901	ASR903	ASR 5000
StpBridgeHelloTime	Y													Y		Y					Y [3 1]		Y						Y		Y	
IMO Name—IMstService																																
MstProperties																																
Same as IStpService																																
IMO Name—IPvstpService																																
UpLinkFast	Y													Y		Y							Y						Y		Y	
BackboneFast	Y													Y		Y							Y						Y		Y	
IMO Name—IMstProperties																																
MstForceVersion	Y													Y							Y		Y						Y	Y		
MstCfgIdFmtSel	Y													Y		Y					Y		Y						Y	Y	Y	
MstExternalRootCost	Y													Y		Y					Y		Y						Y	Y	Y	
MstMaxInstances	Y													Y		Y					Y		Y						Y	Y	Y	
MstCfgIdName	Y													Y		Y							Y						Y	Y	Y	
MstCfgIdRevLevel	Y													Y		Y							Y						Y	Y	Y	
IMO Name—IStpInstanceInfo																																
Object Identification																																
StpBridgeId	Y													Y		Y							Y						Y		Y	
BridgePriority	Y													Y		Y							Y						Y		Y	
Designated Parent and Root Bridges	Y										Y			Y		Y					Y		Y						Y		Y	
StpRootCost	Y										Y			Y		Y					Y		Y						Y		Y	
IsRoot	Y										Y			Y		Y					Y		Y						Y		Y	
StpRootPort	Y										Y			Y		Y					Y		Y						Y		Y	
StpPortInfoTable	Y													Y		Y					Y		Y						Y		Y	
STP Instance Id	Y										Y			Y		Y					Y		Y						Y		Y	
Vlan Id											Y										Y											
StpDesignatedBridge	Y													Y		Y							Y						Y		Y	
StpDesignatedRoot	Y													Y		Y							Y						Y		Y	
IMO Name—IMstInstanceInfo																																
MstVlanIds	Y													Y		Y					Y		Y						Y	Y	Y	

Table 6-125 Ethernet Attribute Support on Cisco Routers—Cisco Prime Network 3.9 (continued)

Attribute	800	1000	1600	1700	1800	2500	2600	2800	3600	3700	3800	7200	7300	7400	7500	7600	10000	12000	XR 12000	CRS	ASR 9000	ASR 1000	MWR 2941	ISR1900	ISR2900	ISR 3900	UBR7200	UBR10000	Cisco 4700	ASR901	ASR903	ASR 5000
Same as IStpInstanceInfo	Y													Y		Y					Y		Y						Y	Y	Y	
IMO Name—IPvstpInstanceInfo																																
Protocol Type	Y										Y			Y		Y							Y						Y		Y	
StpBridgeMaxAge	Y										Y			Y		Y							Y						Y		Y	
StpBridgeHelloTime	Y										Y			Y		Y							Y						Y		Y	
StpBridgeForwardDelay	Y										Y			Y		Y							Y						Y		Y	
StpProtocolSpecification	Y													Y		Y							Y						Y		Y	
StpVlanId	Y													Y		Y							Y						Y		Y	
StpForwardDelay	Y													Y		Y							Y						Y		Y	
StpMaxAge	Y													Y		Y							Y						Y		Y	
IMO Name—IRstpInstanceInfo																																
StpForceVersion	Y													Y									Y						Y			
Same as IStpInstanceInfo	Y													Y		Y							Y						Y		Y	
IMO Name—IStpPortInfo																																
StpPort											Y			Y		Y					Y		Y						Y		Y	
StpPortPriority											Y			Y		Y					Y		Y						Y		Y	
StpPortState											Y			Y		Y					Y		Y						Y		Y	
StpPortPathCost											Y			Y		Y					Y		Y						Y		Y	
StpPortEdgePort											Y			Y		Y					Y		Y						Y		Y	
StpPortPointToPoint											Y			Y		Y					Y		Y						Y		Y	
StpPortRole											Y			Y		Y					Y		Y						Y		Y	
StpDesignatedPortIdentifier														Y		Y							Y						Y		Y	
StpDesignatedBridge														Y		Y							Y						Y		Y	
StpPortIdentifier														Y		Y							Y						Y		Y	
StpPortBpduGuardState														Y		Y							Y						Y		Y	
StpPortBpduFilterState														Y		Y							Y						Y		Y	

Table 6-125 Ethernet Attribute Support on Cisco Routers—Cisco Prime Network 3.9 (continued)

Attribute	800	1000	1600	1700	1800	2500	2600	2800	3600	3700	3800	7200	7300	7400	7500	7600	10000	12000	XR 12000	CRS	ASR 9000	ASR 1000	MWR 2941	ISR1900	ISR2900	ISR 3900	UBR7200	UBR10000	Cisco 4700	ASR901	ASR903	ASR 5000
IMO Name—IMstPortInfo																																
MstPortHelloTime														Y		Y					Y		Y 32						Y	Y	Y	
Same as IStpPortInfo														Y		Y					Y		Y 33						Y	Y	Y	
IMO Name—IPvstpPortInfo																																
PvstpPortFastState														Y		Y							Y 34						Y		Y	
IMO Name—IEthernetChannel																																
Group Number	Y					Y	Y	Y	Y	Y	Y	Y 35		Y 36		Y		Y	Y 37	Y 38	Y	Y		Y	Y	Y				Y	Y	
Bandwidth	Y								Y	Y	Y	Y 39		Y 40		Y		Y	Y 41	Y 42	Y	Y		Y	Y	Y 43				Y	Y	
Aggregation Protocol									Y	Y	Y	Y 44		Y 45		Y		Y	Y 46	Y 47	Y	Y		Y	Y	Y				Y	Y	
IANA Type	Y		Y	Y		Y	Y		Y	Y	Y	Y 48		Y 49		Y	Y	Y	Y 50	Y 51	Y	Y		Y	Y	Y				Y	Y	
Containing CTPs																																
Contained CTPs																																
Mac Address												Y 52				Y						Y								Y		
Admin Status												Y 53				Y						Y								Y		
Oper Status												Y 54				Y						Y								Y		
IMO Name—ITokenRingLayer2																																
MAC Address																																
IANA Type																																
Containing CTPs																																
Contained CTPs																																

Table 6-125 Ethernet Attribute Support on Cisco Routers—Cisco Prime Network 3.9 (continued)

Attribute	800	1000	1600	1700	1800	2500	2600	2800	3600	3700	3800	7200	7300	7400	7500	7600	10000	12000	XR 12000	CRS	ASR 9000	ASR 1000	MWR 2941	ISR1900	ISR2900	ISR 3900	UBR7200	UBR10000	Cisco 4700	ASR901	ASR903	ASR 5000
IMO Name—ITokenRingLayer1																																
Same as IPhysicalLayer																																
IMO Name—IVtpService																																
Version					Y			Y								Y					55								Y		Y	
OperatingMode					Y			Y								Y					56								Y		Y	
DomainName					Y			Y								Y					57								Y		Y	
ConfigurationRevision					Y			Y								Y					58								Y		Y	
isPruningEnabled					Y			Y								Y					59								Y		Y	
isAuthenticationEnabled					Y			Y								Y					60								Y		Y	
IMO Name—IREPService																																
version																Y							Y 61							Y	Y	
administrativeVlan																Y							Y 62							Y	Y	
notificationEnabled																Y							Y 63							Y	Y	
IMO Name—IREPSegmentInfo																																
segmentId																Y							Y 64							Y	Y	
segmentComplete																Y							Y 65							Y	Y	
IMO Name—IREPPortInfo																																
portName																Y							Y 66							Y	Y	
portKey																Y							Y 67							Y	Y	
segmentId																Y							Y 68							Y	Y	
portType																Y							Y 69							Y	Y	
portRole																Y							Y 70							Y	Y	

Table 6-125 Ethernet Attribute Support on Cisco Routers—Cisco Prime Network 3.9 (continued)

Attribute	800	1000	1600	1700	1800	2500	2600	2800	3600	3700	3800	7200	7300	7400	7500	7600	10000	12000	XR 12000	CRS	ASR 9000	ASR 1000	MWR 2941	ISR1900	ISR2900	ISR 3900	UBR7200	UBR10000	Cisco 4700	ASR901	ASR903	ASR 5000
operStatus																Y							Y [71]							Y	Y	
blockedVlans																Y							Y [72]							Y	Y	
preemptTimer																Y							Y [73]							Y	Y	
lslAgeoutTimer																Y							Y [74]							Y	Y	
remoteDeviceName																Y							Y [75]							Y	Y	
remoteDeviceMac																Y							Y [76]							Y	Y	
remotePortName																Y							Y [77]							Y	Y	
configuredLoadBalancingBlockedVlans																Y							Y [78]							Y	Y	
IMO Name—IBridgeILan																																
Id																					Y											
IMO Name—IIBBridgeEntry																																
IS Id																					Y											
IBridge																					Y											
BBridge																					Y											

1, 2, 3, 4, 5, 6, 7Supported in IOS version 12.2(33)SRD1 and 12.2(40)T only.

8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25Supported in IOS versions 12.2(33)SRD1 and 12.2(40)T only.

26, 27, 28, 29, 30, 31, 32, 33, 34LAG is not supported for 12.0(33)S1

35, 37, 38Added show lacp bundle from ANA 3.6.3.1, From XR 4.0, we use show lacp instead of show lacp bundle

36In ANA Prime Network 3.8 , the command 'show interface $ifDescr$' is used to show bandwidth . Added show lacp bundle from ANA 3.6.3.1, From XR 4.0, we use show lacp instead of show lacp bundle

39The current value used and the value that all bridges should use when this bridge is acting as the root of the maximum age of learned spanning tree protocol port information (hundredths' of seconds)

40The current value used and the value that all bridges should use when this bridge is acting as the root for hello time messages' keep alive interval of a spanning tree protocol root (in hundredths of seconds)

41The current value used and the value that all bridges should use when this bridge is acting as the root for port delay in each of the listening and learning states, preceding the forwarding one (in hundredths of seconds)

42, 47Array of Spanning Tree Protocol Bridge information

43, 45, 46SNMP supported with ANA 3.6.0. The ìshow lacp bundleî command is supported with ANA 3.6.3 and later. From xr 4.0, we use show lacp instead of show lacp bundle

44Before ANA Prime Network 3.8 , the bandwidth property was taken from the command 1.2.840.10006.300.43.1.1.1.1,show bundle,show lacp bundle,show lacp . From ANA Prime Network 3.8 , The new registration is added to get the bandwidth property and the bandwidth is taken from the show interface $ifDescr$.

48Only the Bridge Forward Delay is supported and not the Current value.

49Only the Bridge Max Age is supported and not the Current value.

50Only the Bridge Hello Time is supported and not the Current value.

51, 52, 53, 54, 55, 56The MIB provides data by default, but the device does not support VTP.

57, 58, 59Supported only for 12.2(33)MRA

60, 61, 62, 63, 64, 65, 66, 67, 68, 69, 70, 71, 72, 73, 74, 75, 76, 77REP Supported only on IOS 12.2(33)MRA(CSR 3.2)

78This property was earlier updated by framework. From Prime Network 3.8 onwards, vne-drivers is populating this attribute.

ATM

Table 6-126 ATM Attribute Support on Cisco Routers—Cisco Prime Network 3.9

Attribute	800	1000	1600	1700	1800	2500	2600	2800	3600	3700	3800	7200	7300	7400	7500	7600	10000	12000	XR 12000	CRS	ASR 9000	ASR 1000	MWR 2941	ISR1900	ISR2900	ISR 3900	UBR7200	UBR10000	Cisco 4700	ASR901	ASR903	ASR 5000
IMO Name—IAtm																																
ATM Address			Y	Y	Y	Y	Y			Y		Y	Y	Y	Y	Y						Y	Y	Y		Y	Y		Y			
Interface Type												Y						Y	Y	Y				Y								
VP and VC Ranges			Y	Y		Y	Y	Y				Y															Y					
VC Table		Y	Y	Y	Y	Y	Y	Y	Y	Y		Y	Y	Y	Y	Y	Y	Y	Y	Y		Y	Y	Y		Y	Y					
Cross-Connect Table																																
IANA Type		Y	Y	Y	Y	Y			Y	Y			Y	Y	Y	Y	Y	Y	Y	Y		Y	Y			Y	Y		Y			
Containing CTPs																																
Contained CTPs																																
Tx Allocated Bandwidth												Y	Y		Y	Y		Y	Y	Y		Y	Y	Y		Y	Y		Y		Y	
Tx Maximum Bandwidth												Y	Y		Y	Y		Y	Y	Y		Y	Y	Y		Y	Y		Y		Y	
Tx UBR Allocated Bandwidth												Y	Y		Y	Y		Y		Y		Y	Y	Y		Y	Y		Y		Y	
Tx CBR Allocated Bandwidth												Y	Y		Y	Y		Y		Y		Y	Y	Y		Y	Y		Y		Y	

Table 6-126 ATM Attribute Support on Cisco Routers—Cisco Prime Network 3.9 (continued)

Attribute	800	1000	1600	1700	1800	2500	2600	2800	3600	3700	3800	7200	7300	7400	7500	7600	10000	12000	XR 12000	CRS	ASR 9000	ASR 1000	MWR 2941	ISR1900	ISR2900	ISR 3900	UBR7200	UBR10000	Cisco 4700	ASR901	ASR903	ASR 5000
Rx Allocated Bandwidth												Y	Y		Y	Y		Y	Y	Y		Y	Y	Y		Y	Y		Y		Y	
Rx Maximum Bandwidth												Y	Y		Y	Y		Y	Y	Y		Y	Y	Y		Y	Y		Y		Y	
Rx UBR Allocated Bandwidth												Y	Y		Y	Y		Y		Y		Y	Y	Y		Y	Y		Y		Y	
Rx CBR Allocated Bandwidth												Y	Y		Y	Y		Y		Y		Y	Y	Y		Y	Y		Y		Y	
IMO Name—IAtmVc																																
Virtual Channel Identifier	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y		Y	Y	Y		Y	Y		Y		Y	
Virtual Path Identifier	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y		Y	Y	Y		Y	Y		Y		Y	
Shaping Profile																																
Discarded and Received Input Data Counters	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y				Y	Y	Y		Y	Y		Y		Y	
Dropped and Forward Output Data Counters	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y				Y	Y	Y		Y	Y		Y		Y	
Ingress Traffic Descriptor	Y	Y	Y		Y	Y	Y		Y	Y		Y	Y	Y	Y	Y	Y	Y	Y	Y		Y	Y	Y		Y	Y		Y		Y	
Egress Traffic Descriptor	Y	Y	Y		Y	Y	Y		Y	Y		Y	Y	Y	Y	Y	Y	Y	Y	Y		Y	Y	Y		Y	Y		Y		Y	
Administrative Status	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y		Y	Y	Y		Y	Y		Y		Y	
Operational Status	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y		Y	Y	Y		Y	Y		Y		Y	
IANA Type	Y											Y						Y	Y	Y							Y					
Containing CTPs																																
Contained CTPs																																
IMO Name—IAtmTrafficDescriptor																																
Traffic Descriptor Type			Y	Y	Y				Y	Y		Y	Y	Y	Y	Y	Y	Y	Y	Y		Y	Y	Y		Y	Y		Y		Y	
Service Category			Y	Y	Y				Y	Y		Y	Y	Y	Y	Y	Y	Y	Y	Y		Y	Y	Y		Y	Y		Y		Y	
Cell Loss Priority			Y	Y	Y			Y	Y	Y		Y	Y	Y	Y	Y	Y	Y	Y	Y		Y	Y	Y		Y	Y		Y		Y	
Cell Delay Variation								Y																							Y	

Table 6-126 ATM Attribute Support on Cisco Routers—Cisco Prime Network 3.9 (continued)

Attribute	800	1000	1600	1700	1800	2500	2600	2800	3600	3700	3800	7200	7300	7400	7500	7600	10000	12000	XR 12000	CRS	ASR 9000	ASR 1000	MWR 2941	ISR1900	ISR2900	ISR 3900	UBR7200	UBR10000	Cisco 4700	ASR901	ASR903	ASR 5000
Cell Delay Variation Tolerance			Y	Y	Y			Y	Y	Y		Y	Y	Y	Y	Y	Y	Y	Y	Y		Y	Y	Y		Y	Y		Y		Y	
Maximum High Priority and Aggregate Cell Rates	Y		Y	Y	Y				Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y		Y	Y	Y		Y	Y		Y		Y	
Minimum High Priority and Aggregate Cell Rates	Y		Y	Y	Y				Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y		Y	Y	Y		Y	Y		Y		Y	
Sustainable High Priority and Aggregate Cell Rates	Y		Y	Y	Y				Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y		Y	Y	Y		Y	Y		Y		Y	
Peak High Priority and Aggregate Cell Rates	Y		Y	Y	Y				Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y		Y	Y	Y		Y	Y		Y		Y	
Name																																
Index				Y									Y		Y	Y	Y	Y	Y	Y		Y	Y	Y		Y			Y		Y	
IMO Name—IAtmTrafficShapingDescriptor																																
Maximum Burst Size																																
Sustainable and Peak Cell Rates																																
Cell Delay Variation																																
State																																
Buffer Size																																
Cell Loss Priority Discarded Size																																
Name																																
Index																																
IMO Name—IAtmTrunk																																
Same as IAtm																																
IMO Name—IAtmLogicalPort/Trunk																																
Resource Management Cell Termination																																

Table 6-126 ATM Attribute Support on Cisco Routers—Cisco Prime Network 3.9 (continued)

Attribute	800	1000	1600	1700	1800	2500	2600	2800	3600	3700	3800	7200	7300	7400	7500	7600	10000	12000	XR 12000	CRS	ASR 9000	ASR 1000	MWR 2941	ISR1900	ISR2900	ISR 3900	UBR7200	UBR10000	Cisco 4700	ASR901	ASR903	ASR 5000
Resource Management Cell Generation																																
Effective Check Input and Output Capacities																																
Admin Status																																
Oper Status																																
Same as IAtm																																
IMO Name—IAtmTrunkVc																																
Destination Description																																
Same as IAtmVc																																
IMO Name—IVcSwitchingEntity																																
Cross Connect Table												Y				Y							Y			Y			Y		Y	
crossConnectTable Size												Y				Y							Y			Y					Y	
Logical Sons																																
IMO Name—IIMAGroup																																
AdminStatus												Y				Y							Y			Y					Y	
OperStatus												Y				Y							Y			Y					Y	
GroupNumber												Y				Y							Y			Y					Y	
ImaVersion												Y				Y							Y			Y					Y	
Speed												Y				Y							Y			Y					Y	
ConfiguredBandwidth												Y				Y							Y			Y					Y	
NumberOfLinks												Y				Y							Y			Y					Y	
NumberOfActiveLinks												Y				Y							Y			Y					Y	
MinimumNumberOfTxLinks												Y				Y							Y			Y					Y	
MinimumNumberOfRxLinks												Y				Y							Y			Y					Y	
ClockMode												Y				Y							Y			Y					Y	
FrameLength												Y				Y							Y			Y					Y	
interfaceName												Y				Y							Y			Y					Y	

Table 6-126 ATM Attribute Support on Cisco Routers—Cisco Prime Network 3.9 (continued)

Attribute	800	1000	1600	1700	1800	2500	2600	2800	3600	3700	3800	7200	7300	7400	7500	7600	10000	12000	XR 12000	CRS	ASR 9000	ASR 1000	MWR 2941	ISR1900	ISR2900	ISR 3900	UBR7200	UBR10000	Cisco 4700	ASR901	ASR903	ASR 5000
groupStatus												Y				Y							Y			Y					Y	

Frame Relay

Table 6-127 Frame Relay Attribute Support on Cisco Routers—Cisco Prime Network 3.9

Attribute	800	1000	1600	1700	1800	2500	2600	2800	3600	3700	3800	7200	7300	7400	7500	7600	10000	12000	XR 12000	CRS	ASR 9000	ASR 1000	MWR 2941	ISR1900	ISR2900	ISR 3900	UBR7200	UBR10000	Cisco 4700	ASR901	ASR903	ASR 5000
IMO Name—IFrameRelay/IFrTrunk																																
Protocol Type		Y								Y		Y		Y		Y	Y	Y				Y					Y		Y		Y	
VC Table		Y	Y		Y				Y	Y		Y		Y		Y		Y				Y					Y		Y		Y	
Cross-Connect Table																																
IANA Type																	Y															
Containing CTPs																																
Contained CTPs																																
IMO Name—IFrVc																																
Data Link Connection Identifier		Y	Y	Y	Y	Y	Y	Y	Y	Y		Y		Y		Y	Y	Y				Y					Y		Y		Y	
Traffic Descriptor		Y	Y		Y				Y	Y		Y		Y		Y	Y	Y				Y					Y		Y		Y	
Discard and Received Input Data Counters																																
Dropped and Forward Output Data Counters																																
Ingress Traffic Descriptor		Y	Y						Y	Y		Y		Y		Y	Y	Y				Y					Y		Y		Y	
Egress Traffic Descriptor		Y	Y						Y	Y		Y		Y		Y	Y	Y				Y					Y		Y		Y	
Administrative Status		Y	Y	Y	Y	Y	Y	Y	Y	Y		Y		Y		Y	Y	Y				Y					Y		Y		Y	
Operational Status		Y	Y	Y	Y	Y	Y	Y	Y	Y		Y		Y		Y	Y	Y				Y					Y		Y		Y	
IANA Type				Y	Y							Y		Y																		
Containing CTPs																																

Table 6-127 Frame Relay Attribute Support on Cisco Routers—Cisco Prime Network 3.9 (continued)

Attribute	800	1000	1600	1700	1800	2500	2600	2800	3600	3700	3800	7200	7300	7400	7500	7600	10000	12000	XR 12000	CRS	ASR 9000	ASR 1000	MWR 2941	ISR1900	ISR2900	ISR 3900	UBR7200	UBR10000	Cisco 4700	ASR901	ASR903	ASR 5000
Contained CTPs																																
IMO Name—IFRTrafficDescriptor																																
Committed Rate		Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y		Y		Y	Y	Y				Y					Y		Y		Y	
Excess Burst Rate		Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y		Y		Y	Y	Y				Y					Y		Y		Y	
Name								Y																								
Index								Y				Y															Y					
IMO Name—IFrameRelayLogicalPort/Trunk																																
Admin Status																																
Oper Status																																
Same as IFrameRelay																																
IMO Name—IFrTrunkVc																																
Destination Description																																
Same as IFrVc																																
IMO Name—IEncapsulation																																
Virtual Connection Interface		Y	Y						Y	Y		Y		Y		Y	Y	Y				Y	Y				Y		Y			
Binding Information								Y									Y															
IMO Name—IFramerelayLogicalPort/Trunk																																
Admin Status											Y													Y								
Oper Status											Y													Y								
Same as IFrameRelay													Y				Y															
IMO Name—Iframerelay/IFrTrunk																																
Protocol Type																																
VC Table																																
Cross-Connect Table																																
IANA Type																																
Containing CTPs																																
Contained CTPs																																

PPP

Table 6-128 PPP Attribute Support on Cisco Routers—Cisco Prime Network 3.9

Attribute	800	1000	1600	1700	1800	2500	2600	2800	3600	3700	3800	7200	7300	7400	7500	7600	10000	12000	XR 12000	CRS	ASR 9000	ASR 1000	MWR 2941	ISR1900	ISR2900	ISR 3900	UBR7200	UBR10000	Cisco 4700	ASR901	ASR903	ASR 5000
IMO Name—IVcBasedEncapsulation																																
Virtual Connection								Y											Y		Y											
Binding Information				Y	Y		Y	Y			Y								Y		Y											
Binding Status		Y	Y	Y	Y		Y	Y	Y	Y	Y	Y		Y		Y	Y	Y	Y		Y		Y			Y	Y		Y		Y	
IANA Type		Y	Y	Y	Y		Y		Y	Y		Y		Y		Y	Y	Y	Y		Y		Y			Y	Y		Y		Y	
Containing CTPs																			Y		Y											
Contained CTPs																			Y		Y											
IMO Name—IMLPPP																																
InterfaceName												Y				Y	Y	Y	Y	Y	Y	Y	Y							Y	Y	
GroupNumber												Y				Y	Y	Y	Y	Y	Y	Y	Y							Y	Y	
MTU												Y				Y	Y	Y	Y	Y		Y	Y							Y	Y	
FragmentDelay												Y				Y	Y	Y				Y	Y							Y	Y	
FragmentDisable												Y				Y	Y	Y	Y	Y	Y	Y	Y							Y	Y	
FragmentMaximum												Y				Y	Y	Y				Y	Y							Y	Y	
FragmentSize												Y				Y	Y	Y				Y	Y							Y	Y	
Interleave												Y				Y	Y	Y	Y	Y	Y	Y	Y							Y	Y	
Keepalive												Y				Y	Y	Y	Y	Y	Y	Y	Y							Y	Y	
KeepaliveTime												Y				Y	Y	Y	Y	Y	Y	Y	Y							Y	Y	
KeepaliveRetry												Y				Y	Y	Y				Y	Y							Y	Y	
ActiveLink												Y				Y	Y	Y	Y	Y	Y	Y	Y							Y	Y	
MinimumConfiguredLink												Y				Y	Y	Y				Y	Y							Y	Y	
MaximumConfiguredLink												Y				Y	Y	Y				Y	Y							Y	Y	
LocalMRRU												Y				Y	Y	Y	Y	Y		Y	Y							Y	Y	
RemoteMRRU												Y				Y	Y	Y	Y	Y		Y	Y							Y	Y	
LoadThreshold												Y				Y	Y	Y				Y	Y							Y	Y	
LCPStatus												Y				Y	Y	Y	Y	Y		Y	Y							Y	Y	
AdminStatus												Y				Y	Y	Y	Y	Y		Y	Y							Y	Y	
OperStatus												Y				Y	Y	Y	Y	Y		Y	Y							Y	Y	

HDLC

Table 6-129 HDLC Attribute Support on Cisco Routers—Cisco Prime Network 3.9

Attribute	800	1000	1600	1700	1800	2500	2600	2800	3600	3700	3800	7200	7300	7400	7500	7600	10000	12000	XR 12000	CRS	ASR 9000	ASR 1000	MWR 2941	ISR1900	ISR2900	ISR 3900	UBR7200	UBR10000	Cisco 4700	ASR901	ASR903	ASR 5000
IMO Name—IEncapsulation (HDLC/PPP)																																
Virtual Connection		Y	Y					Y			Y	Y	Y	Y	Y	Y	Y	Y			Y						Y [1]		Y		Y	
Binding Information								Y			Y	Y	Y		Y	Y					Y						Y [2]		Y		Y	
Binding Status		Y	Y	Y	Y		Y	Y			Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y						Y [3]		Y		Y	
IANA Type		Y	Y	Y	Y		Y					Y		Y		Y	Y	Y			Y						Y [4]		Y		Y	
Containing CTPs																																
Contained CTPs																																
IMO Name—Iencapsulation (HDLC/PPP)																																
Virtual Connection																																
Binding Information																																
Binding Status																																
IANA Type																																
Containing CTPs																																
Contained CTPs																																

[1, 2, 3, 4] HDLC is not supported

SONET/SDH

Table 6-130 SONET/SDH Attribute Support on Cisco Routers—Cisco Prime Network 3.9

Attribute	800	1000	1600	1700	1800	2500	2600	2800	3600	3700	3800	7200	7300	7400	7500	7600	10000	12000	XR 12000	CRS	ASR 9000	ASR 1000	MWR 2941	ISR1900	ISR2900	ISR 3900	UBR7200	UBR10000	Cisco 4700	ASR901	ASR903	ASR 5000
IMO Name—ISonetSdh																																
Specific Type																					Y											
Loopback Type						Y	Y		Y	Y		Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y							Y		Y	
Scrambling Mode		Y	Y	Y	Y	Y	Y	Y	Y	Y		Y	Y	Y	Y	Y	Y	Y				Y							Y		Y	

Table 6-130 SONET/SDH Attribute Support on Cisco Routers—Cisco Prime Network 3.9 (continued)

Attribute	800	1000	1600	1700	1800	2500	2600	2800	3600	3700	3800	7200	7300	7400	7500	7600	10000	12000	XR 12000	CRS	ASR 9000	ASR 1000	MWR 2941	ISR1900	ISR2900	ISR 3900	UBR7200	UBR10000	Cisco 4700	ASR901	ASR903	ASR 5000
Same as IPhysicalLayer													Y		Y																	
TCAThresholdB1																			Y	Y	Y											
TCAThresholdB2																			Y	Y	Y											
TCAThresholdB3																			Y	Y	Y											
clocking																			Y	Y	Y											
IMO Name—IDS1PdhChannelized																																
Au4Number												Y				Y	Y	Y													Y	
Au3Number												Y				Y	Y	Y	Y	Y	Y										Y	
Sts1Number																Y	Y	Y	Y	Y	Y										Y	
Tug3Number												Y				Y	Y	Y													Y	
Tug2Number												Y				Y	Y	Y													Y	
VtNumber																Y	Y	Y	Y	Y	Y										Y	
C11Number																Y	Y	Y													Y	
C12Number												Y				Y	Y	Y													Y	
Vt15Number																Y	Y	Y	Y	Y	Y										Y	
Vt2Number																Y	Y	Y													Y	
T1Number												Y				Y	Y	Y	Y	Y	Y										Y	
E1Number												Y				Y	Y	Y	Y	Y	Y										Y	
PathType												Y				Y	Y	Y	Y	Y	Y										Y	
Description												Y				Y	Y	Y	Y	Y	Y										Y	
Sts3CNumber	Y	Y	Y																													
Sts12CNumber	Y	Y	Y																													
T3Number	Y	Y	Y																													
E3Number	Y	Y	Y																													
IMO Name—ISonetSdhHop																																
Description												Y				Y	Y	Y	Y	Y	Y										Y	
AppliqueType												Y				Y	Y	Y	Y	Y	Y										Y	
PathType												Y				Y	Y	Y	Y	Y	Y										Y	
IMO Name—ISonetSts1																																
Sts1Number																Y	Y	Y	Y	Y	Y										Y	
IMO Name—ISdhAu4																																
Au4Number												Y				Y	Y	Y													Y	
IMO Name—ISdhAu3																																
Au3Number												Y				Y	Y	Y	Y	Y	Y										Y	

TDM/DSx

Table 6-131 TDM/DSx Attribute Support on Cisco Routers—Cisco Prime Network 3.9

Attribute	800	1000	1600	1700	1800	2500	2600	2800	3600	3700	3800	7200	7300	7400	7500	7600	10000	12000	XR 12000	CRS	ASR 9000	ASR 1000	MWR 2941	ISR1900	ISR2900	ISR 3900	UBR7200	UBR10000	Cisco 4700	ASR901	ASR903	ASR 5000
IMO Name—IDS0Bundle																																
Bundled Time Slots	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y		Y		Y	Y	Y			Y					Y			Y	Y	Y	
Bundle Location	Y	Y	Y	Y	Y	Y	Y	Y			Y	Y		Y		Y	Y	Y	Y		Y					Y			Y	Y	Y	
IANA Type	Y	Y	Y	Y	Y			Y			Y					Y			Y		Y					Y			Y	Y	Y	
Containing CTPs																																
Contained CTPs																																
AdminStatus												Y				Y			Y		Y					Y			Y	Y	Y	
OperStatus												Y				Y			Y		Y					Y			Y	Y	Y	
IMO Name—IDS1Pdh / IDS3Pdh																																
Framing Type																																
Cell Mapping Type																																
Loopback Type									Y	Y																						
Scrambling Mode	Y	Y	Y	Y	Y		Y	Y	Y	Y	Y	Y [1]		Y		Y	Y	Y				Y	Y [2]			Y			Y		Y	
Same as IPhysicalLayer																																
portDescription					Y			Y				Y				Y			Y	Y	Y		Y [3]			Y			Y		Y	
internationalBit					Y			Y								Y							Y [4]			Y			Y		Y	
nationalBits					Y			Y								Y							Y [5]			Y			Y		Y	
framing					Y			Y				Y				Y					Y		Y [6]			Y			Y		Y	
lineCode					Y			Y				Y [7]				Y							Y [8]			Y			Y		Y	
cableLength					Y			Y				Y [9]				Y							Y [10]			Y			Y		Y	
recoveredClocking Id					Y							Y [11]				Y							Y [12]			Y			Y		Y	
clocking					Y			Y				Y				Y			Y	Y	Y		Y [13]			Y			Y		Y	

Table 6-131 TDM/DSx Attribute Support on Cisco Routers—Cisco Prime Network 3.9 (continued)

Attribute	800	1000	1600	1700	1800	2500	2600	2800	3600	3700	3800	7200	7300	7400	7500	7600	10000	12000	XR 12000	CRS	ASR 9000	ASR 1000	MWR 2941	ISR1900	ISR2900	ISR 3900	UBR7200	UBR10000	Cisco 4700	ASR901	ASR903	ASR 5000
loopback					Y			Y				Y				Y							Y [14]			Y			Y		Y	
alarmState					Y							Y [15]				Y			Y		Y		Y [16]			Y			Y		Y	
IMO Name—IClockService																																
ActiveClockSource																Y							Y							Y	Y	
NcsMode																Y							Y							Y	Y	
HoldTimeout																Y							Y							Y	Y	
UseStratum4																Y							Y							Y	Y	
Mode																Y							Y							Y	Y	
NcsPriorityList																Y							Y							Y	Y	
PtpService																Y							Y							Y	Y	
ClockSourceTable																															Y	
PseudowireClockRecovery																															Y	
SynchronousEthernet																															Y	
IMO Name—IClockSource																																
Priority																Y							Y							Y	Y	
Source																Y							Y							Y	Y	
Status																Y							Y							Y	Y	
Type																Y							Y							Y	Y	
IMO Name—IPtpService																																
Mode																Y							Y							Y	Y	
ClockId																Y							Y							Y	Y	
Domain																Y							Y							Y	Y	
Priority1																Y							Y							Y	Y	
Priority2																Y							Y							Y	Y	
PtpEnabled																Y							Y							Y	Y	
PtpInterfaceList																Y							Y							Y	Y	
ptpState																															Y	
PtpState	Y																															
IMO Name—IPtpInterface																																
Version																Y							Y							Y	Y	

Table 6-131 TDM/DSx Attribute Support on Cisco Routers—Cisco Prime Network 3.9 (continued)

Attribute	800	1000	1600	1700	1800	2500	2600	2800	3600	3700	3800	7200	7300	7400	7500	7600	10000	12000	XR 12000	CRS	ASR 9000	ASR 1000	MWR 2941	ISR1900	ISR2900	ISR 3900	UBR7200	UBR10000	Cisco 4700	ASR901	ASR903	ASR 5000
AnnounceInterval																Y							Y							Y	Y	
AnnounceTimeout																Y							Y							Y	Y	
DestinationAddress																Y							Y							Y	Y	
SourceAddress																Y							Y							Y	Y	
DelayReq																Y							Y							Y	Y	
MasterMode																Y							Y							Y	Y	
SlaveMode																Y							Y							Y	Y	
SyncInterval																Y							Y							Y	Y	
SyncLimit																Y							Y							Y	Y	
InterfaceXid																Y							Y							Y	Y	
Role																Y														Y	Y	
Transport																Y															Y	
State																Y															Y	
IMO Name—IACRService																																
RecoveredClockSource																Y							Y								Y	
RecoveredClockMode																Y							Y								Y	
CemInterface																Y							Y								Y	
RecoveredClockList																Y							Y								Y	
IMO Name—IRecoveredClock																																
ClockId																Y							Y								Y	
RecoveredClockMode																Y							Y								Y	
Port																Y							Y								Y	
Cem																Y							Y								Y	
Status																Y							Y								Y	
FrequencyOffset																Y							Y								Y	
CEMGroupId																Y															Y	
CEMInterfaceName																Y															Y	
TransferType																Y															Y	
IMO Name—ICEMEncap																																
cemIfName																Y						Y	Y							Y	Y	

Table 6-131 TDM/DSx Attribute Support on Cisco Routers—Cisco Prime Network 3.9 (continued)

Attribute	800	1000	1600	1700	1800	2500	2600	2800	3600	3700	3800	7200	7300	7400	7500	7600	10000	12000	XR 12000	CRS	ASR 9000	ASR 1000	MWR 2941	ISR1900	ISR2900	ISR 3900	UBR7200	UBR10000	Cisco 4700	ASR901	ASR903	ASR 5000
IMO Name—ICEMGroup																																
IdlePattern																Y						Y	Y							Y	Y	
IdleCAS																Y						Y	Y							Y	Y	
DeJitter																Y						Y	Y							Y	Y	
PayloadSize																Y						Y	Y							Y	Y	
RTP																Y						Y	Y							Y	Y	
RTPHeader																Y						Y	Y							Y	Y	
TimeSlots																Y						Y	Y							Y	Y	
AdminStatus																Y						Y	Y							Y	Y	
OperStatus																Y						Y	Y							Y	Y	
IMO Name—ISyncE																																
synchronousMode																Y														Y	Y	
equipmentClock																Y														Y	Y	
clockMode																Y														Y	Y	
ssmOption																Y														Y	Y	
esmcMode																Y														Y	Y	
holdOffTimer																Y														Y	Y	
waitToRestore																Y														Y	Y	
Revertive																Y														Y	Y	
IMO Name—ISyncEInterface																																
InterfaceName																													Y			
selectionInput																Y														Y	Y	
ingressESMCMode																Y														Y	Y	
egressESMCMode																Y														Y	Y	
ingressQLMode																Y															Y	
ingressQuality																Y														Y	Y	
egressQLMode																Y															Y	
egressQuality																Y														Y	Y	
waitToRestore																Y														Y	Y	
holdOffTimer																Y														Y	Y	
ingressConfQuality																Y														Y	Y	
egressConfQuality																Y														Y	Y	
Priority																Y														Y	Y	

Table 6-131 TDM/DSx Attribute Support on Cisco Routers—Cisco Prime Network 3.9 (continued)

Attribute	800	1000	1600	1700	1800	2500	2600	2800	3600	3700	3800	7200	7300	7400	7500	7600	10000	12000	XR 12000	CRS	ASR 9000	ASR 1000	MWR 2941	ISR1900	ISR2900	ISR 3900	UBR7200	UBR10000	Cisco 4700	ASR901	ASR903	ASR 5000
ingressSSM																Y														Y	Y	
egressSSM																Y														Y	Y	
clockModeStr																Y														Y	Y	

[1, 2, 3, 4, 5] Supported only for DS1

[6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16] Not Supported on IOS 12.2(33)MRA (CSR3.2)

MPLS

Table 6-132 MPLS Attribute Support on Cisco Routers—Cisco Prime Network 3.9

Attribute	800	1000	1600	1700	1800	2500	2600	2800	3600	3700	3800	7200	7300	7400	7500	7600	10000	12000	XR 12000	CRS	ASR 9000	ASR 1000	MWR 2941	ISR1900	ISR2900	ISR 3900	UBR7200	UBR10000	Cisco 4700	ASR901	ASR903	ASR 5000
IMO Name—IMpls																																
Distribution Protocol									Y	Y	Y	Y		Y		Y	Y	Y	Y	Y	Y	Y	Y				Y	Y		Y	Y	
LabelStack																																
TopLabel																																
Outer and Inner Labels																			Y	Y	Y											
Traffic Engineering Properties									Y	Y		Y		Y		Y	Y	Y				Y	Y						Y	Y	Y	
Resource reservation Properties																																
IANA Type									Y	Y		Y				Y	Y	Y	Y	Y	Y	Y	Y				Y	Y	Y	Y	Y	
Containing CTPs																																
Contained CTPs																																
IMO Name—ILse																																
MPLS Table										Y		Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y				Y	Y	Y	Y	Y	
MPLS Aggregate Table										Y		Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y				Y	Y	Y	Y	Y	
MPLS Tunnel Segments									Y			Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y				Y		Y	Y	Y	
LDP Service												Y		Y		Y	Y	Y	Y	Y	Y	Y	Y				Y	Y	Y	Y	Y	
Logical Sons						Y				Y		Y	Y	Y	Y	Y	Y	Y	Y	Y		Y	Y				Y	Y	Y	Y	Y	

Table 6-132 MPLS Attribute Support on Cisco Routers—Cisco Prime Network 3.9 (continued)

Attribute	800	1000	1600	1700	1800	2500	2600	2800	3600	3700	3800	7200	7300	7400	7500	7600	10000	12000	XR 12000	CRS	ASR 9000	ASR 1000	MWR 2941	ISR1900	ISR2900	ISR 3900	UBR7200	UBR10000	Cisco 4700	ASR901	ASR903	ASR 5000
IMO Name—ILdpService																																
Local Identification Status												Y		Y		Y	Y	Y	Y	Y	Y	Y	Y				Y	Y	Y	Y	Y	
LDP Peers									Y	Y	Y	Y		Y		Y	Y	Y	Y	Y	Y	Y	Y				Y	Y	Y	Y	Y	
IMO Name—ILdpPeer																																
Peer Identification									Y	Y	Y	Y		Y		Y	Y	Y	Y	Y	Y	Y	Y				Y	Y	Y	Y	Y	
Transport Address									Y	Y	Y	Y		Y		Y	Y	Y	Y	Y	Y	Y	Y				Y	Y	Y	Y	Y	
Distribution Method									Y	Y	Y	Y		Y		Y	Y	Y	Y	Y	Y	Y	Y				Y	Y	Y	Y	Y	
Protocol Type									Y		Y	Y		Y		Y	Y	Y	Y	Y	Y	Y	Y				Y	Y	Y	Y	Y	
Path Vector Limit										Y				Y		Y		Y				Y	Y						Y	Y	Y	
Session Status									Y	Y	Y	Y		Y		Y	Y	Y	Y	Y	Y	Y	Y				Y	Y	Y	Y	Y	
Protocol Version Hold Time									Y	Y	Y																					
Hold Time									Y	Y	Y	Y		Y		Y	Y	Y	Y	Y	Y	Y	Y				Y	Y	Y	Y	Y	
Keep Alive Time									Y	Y	Y								Y	Y	Y											
Peer Discovery Sources									Y	Y	Y	Y		Y		Y	Y	Y	Y	Y	Y	Y	Y				Y	Y	Y	Y	Y	
IMO Name—ILdpDiscoverySource																																
Interface Name									Y	Y		Y		Y		Y	Y	Y	Y	Y	Y	Y	Y				Y	Y	Y	Y	Y	
Source Address									Y	Y		Y		Y		Y	Y	Y	Y	Y	Y	Y	Y				Y	Y	Y	Y	Y	
Type									Y	Y		Y		Y		Y	Y	Y	Y	Y	Y	Y	Y				Y	Y	Y	Y	Y	
IMO Name—IMplsEntry																																
Incoming Label									Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y				Y	Y	Y	Y	Y	
Outgoing Interface and Label									Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y				Y	Y	Y	Y	Y	
Switching Action									Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y				Y	Y	Y	Y	Y	
Next Hop IP Address									Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y				Y	Y	Y	Y	Y	
Destination Mask									Y	Y		Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y				Y	Y	Y	Y	Y	
Destination address									Y	Y		Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y				Y	Y	Y	Y	Y	
IMO Name—IMplsAggregateEntry																																
Virtual Routing Entity									Y	Y		Y		Y		Y	Y	Y	Y	Y	Y	Y	Y				Y	Y	Y	Y	Y	
Incoming Label									Y	Y		Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y				Y	Y	Y	Y	Y	

Table 6-132 MPLS Attribute Support on Cisco Routers—Cisco Prime Network 3.9 (continued)

Attribute	800	1000	1600	1700	1800	2500	2600	2800	3600	3700	3800	7200	7300	7400	7500	7600	10000	12000	XR 12000	CRS	ASR 9000	ASR 1000	MWR 2941	ISR1900	ISR2900	ISR 3900	UBR7200	UBR10000	Cisco 4700	ASR901	ASR903	ASR 5000
Outgoing Interface and Label									Y	Y		Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y				Y	Y	Y	Y	Y	
Switching Action									Y	Y		Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y				Y	Y	Y	Y	Y	
Next Hop IP Address									Y	Y		Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y				Y	Y	Y	Y	Y	
IMO Name—IMplsLabelRange																																
Type						Y			Y	Y	Y	Y		Y	Y	Y	Y	Y	Y	Y	Y	Y	Y		Y				Y	Y	Y	
minValue						Y			Y	Y	Y	Y		Y	Y	Y	Y	Y	Y	Y	Y	Y	Y		Y				Y	Y	Y	
MaxValue						Y			Y	Y	Y	Y		Y	Y	Y	Y	Y	Y	Y	Y	Y	Y		Y				Y	Y	Y	

MPLS-TE

Table 6-133 MPLS-TE Attribute Support on Cisco Routers—Cisco Prime Network 3.9

Attribute	800	1000	1600	1700	1800	2500	2600	2800	3600	3700	3800	7200	7300	7400	7500	7600	10000	12000	XR 12000	CRS	ASR 9000	ASR 1000	MWR 2941	ISR1900	ISR2900	ISR 3900	UBR7200	UBR10000	Cisco 4700	ASR901	ASR903	ASR 5000
IMO Name—IMplsTETunnel																																
Destination Address									Y	Y	Y	Y		Y		Y	Y	Y	Y	Y	Y	Y	Y[1]						Y	Y	Y	
Outgoing Interface and Label									Y	Y	Y	Y		Y		Y	Y	Y	Y	Y	Y	Y	Y[2]						Y	Y	Y	
LSP Identification									Y	Y	Y	Y		Y		Y	Y	Y	Y	Y	Y	Y	Y[3]						Y	Y	Y	
Requested Bandwidth									Y	Y	Y	Y		Y		Y	Y	Y	Y	Y	Y	Y	Y[4]						Y	Y	Y	
Measured Average Burst and Peak Bandwidth									Y	Y	Y	Y		Y		Y	Y	Y	Y	Y	Y	Y	Y[5]						Y	Y	Y	
Setup and Hold Priority									Y	Y	Y	Y		Y		Y	Y	Y	Y	Y	Y	Y	Y[6]						Y	Y	Y	
Affinity Bits and Mask									Y	Y	Y	Y		Y		Y	Y	Y	Y	Y	Y	Y	Y[7]						Y	Y	Y	
Automatic Route Announcement Status									Y	Y	Y	Y		Y		Y	Y	Y	Y	Y	Y	Y	Y[8]						Y	Y	Y	
Optimization Lock Down Status									Y	Y	Y	Y		Y		Y	Y	Y	Y	Y	Y	Y	Y[9]						Y	Y	Y	

Table 6-133 MPLS-TE Attribute Support on Cisco Routers—Cisco Prime Network 3.9 (continued)

Attribute	800	1000	1600	1700	1800	2500	2600	2800	3600	3700	3800	7200	7300	7400	7500	7600	10000	12000	XR 12000	CRS	ASR 9000	ASR 1000	MWR 2941	ISR1900	ISR2900	ISR 3900	UBR7200	UBR10000	Cisco 4700	ASR901	ASR903	ASR 5000
Path Option									Y	Y	Y	Y		Y		Y	Y	Y	Y	Y	Y	Y	Y [10]						Y	Y	Y	
Name									Y	Y	Y	Y		Y		Y	Y	Y	Y	Y	Y	Y	Y [11]						Y	Y	Y	
Description									Y	Y	Y	Y		Y		Y	Y	Y	Y	Y	Y	Y	Y [12]						Y	Y	Y	
Administrative Status									Y	Y	Y	Y		Y		Y	Y	Y	Y	Y	Y	Y	Y [13]						Y	Y	Y	
Operational Status									Y	Y	Y	Y		Y		Y	Y	Y	Y	Y	Y	Y	Y [14]						Y	Y	Y	
IANA Type									Y	Y	Y	Y		Y		Y	Y	Y	Y	Y	Y	Y	Y [15]						Y	Y	Y	
is FRR Enabled									Y	Y	Y	Y		Y		Y	Y	Y	Y	Y	Y	Y	Y [16]						Y	Y	Y	
TunnelType												Y				Y	Y	Y	Y	Y	Y	Y									Y	
DestinationAddress												Y				Y	Y	Y	Y		Y	Y									Y	
Sub Lsp Status												Y				Y	Y	Y	Y		Y	Y									Y	
OutInterface		Y																														
OutLabel		Y																														
TunnelAffinity		Y																														
TunnelAffinityMask		Y																														
TunnelAutoRoute												Y				Y	Y	Y	Y	Y	Y	Y									Y	
TunnelBandwidthKbps		Y																														
TunnelAverageRateKbps		Y																														
TunnelBurstKbps		Y																														
TunnelPeakRateKbps		Y																														
TunnelSetupPriority		Y																														
TunnelHoldPriority		Y																														
TunnelLockdown		Y																														
TunnelPolicyClass																		Y	Y	Y	Y	Y										
P2MPDestinations												Y				Y	Y	Y	Y	Y	Y	Y									Y	

Table 6-133 MPLS-TE Attribute Support on Cisco Routers—Cisco Prime Network 3.9 (continued)

Attribute	800	1000	1600	1700	1800	2500	2600	2800	3600	3700	3800	7200	7300	7400	7500	7600	10000	12000	XR 12000	CRS	ASR 9000	ASR 1000	MWR 2941	ISR1900	ISR2900	ISR 3900	UBR7200	UBR10000	Cisco 4700	ASR901	ASR903	ASR 5000
IMO Name—IMplsTEProperties																																
Administrative Weight									Y	Y		Y		Y		Y	Y	Y	Y	Y	Y	Y	Y [17]						Y	Y	Y	
Attributes Identifier																			Y	Y	Y											
Signaling Protocol									Y	Y	Y	Y		Y		Y	Y	Y	Y	Y	Y	Y	Y [18]						Y	Y	Y	
Available Physical and Reservable Bandwidth									Y	Y	Y	Y		Y		Y	Y	Y	Y	Y	Y	Y	Y [19]						Y	Y	Y	
Reserved Bandwidth									Y	Y	Y	Y		Y		Y	Y	Y	Y	Y	Y	Y	Y [20]						Y	Y	Y	
IMO Name—IMplsTEPropertiesAllocationEntry																																
Priority Level											Y	Y					Y															
Allocated and Cumulative Bandwidth											Y	Y					Y															
IMO Name—IMplsTESegment																																
Segment Type									Y	Y		Y		Y		Y	Y	Y	Y	Y	Y	Y	Y [21]						Y	Y	Y	
Measured Average Burst and Peak Bandwidth									Y	Y		Y		Y		Y	Y	Y	Y	Y	Y	Y	Y [22]						Y	Y	Y	
LSP Identification									Y	Y		Y		Y		Y	Y	Y	Y	Y	Y	Y	Y [23]						Y	Y	Y	
Name									Y	Y		Y		Y		Y	Y	Y	Y	Y	Y	Y	Y [24]						Y	Y	Y	
FRRTunnelName									Y	Y	Y	Y		Y		Y	Y	Y	Y	Y	Y	Y	Y [25]						Y	Y	Y	
FRRTunnelState									Y	Y	Y	Y		Y		Y	Y	Y	Y	Y	Y	Y	Y [26]						Y	Y	Y	
AverageBandwidth									Y	Y		Y		Y		Y	Y	Y	Y	Y	Y	Y	Y [27]						Y	Y	Y	
In Interface									Y	Y		Y		Y		Y	Y	Y	Y	Y	Y	Y	Y [28]						Y	Y	Y	
Out interface									Y	Y		Y		Y		Y	Y	Y	Y	Y	Y	Y	Y [29]						Y	Y	Y	
In Label									Y	Y		Y		Y		Y	Y	Y	Y	Y	Y	Y	Y [30]						Y	Y	Y	

Table 6-133 MPLS-TE Attribute Support on Cisco Routers—Cisco Prime Network 3.9 (continued)

Attribute	800	1000	1600	1700	1800	2500	2600	2800	3600	3700	3800	7200	7300	7400	7500	7600	10000	12000	XR 12000	CRS	ASR 9000	ASR 1000	MWR 2941	ISR1900	ISR2900	ISR 3900	UBR7200	UBR10000	Cisco 4700	ASR901	ASR903	ASR 5000
Out Label									Y	Y		Y		Y		Y	Y	Y	Y	Y	Y	Y	Y [31]						Y	Y	Y	
Source address									Y	Y		Y		Y		Y	Y	Y	Y	Y	Y	Y	Y [32]						Y	Y	Y	
Destination address									Y	Y		Y		Y		Y	Y	Y	Y	Y	Y	Y	Y [33]						Y	Y	Y	
TunnelType												Y				Y	Y	Y	Y		Y										Y	

[1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 31, 32, 33] Not Supported in IOS 12.2(33)MRA (CSR3.2)

MPLS-TP

Table 6-134 MPLS-TP Attribute Support on Cisco Routers—Cisco Prime Network 3.9

Attribute	800	1000	1600	1700	1800	2500	2600	2800	3600	3700	3800	7200	7300	7400	7500	7600	10000	12000	XR 12000	CRS	ASR 9000	ASR 1000	MWR 2941	ISR1900	ISR2900	ISR 3900	UBR7200	UBR10000	Cisco 4700	ASR901	ASR903
IMO Name—IMPLSTPGlobal																															
icc																Y															Y
globalId																Y					Y										Y
protectionMode																Y					Y										Y
redundancyMode																Y					Y										Y
routerId																Y					Y										Y
tpEnabledLinks																Y					Y										Y
lspEndpoints																Y					Y										Y
lspMidpoints																Y					Y										Y
mplsTpTunnelEps																Y					Y										Y
IMO Name—IMPLSTPTunnelEP																															
tunnelId																Y					Y										Y
remoteTunnelId																Y					Y										Y
globalId																Y					Y										Y
destGlobalId																Y					Y										Y
localInfo																Y					Y										Y
peerInfo																Y					Y										Y
adminStatus																Y					Y										Y

Table 6-134 MPLS-TP Attribute Support on Cisco Routers—Cisco Prime Network 3.9 (continued)

Attribute	800	1000	1600	1700	1800	2500	2600	2800	3600	3700	3800	7200	7300	7400	7500	7600	10000	12000	XR 12000	CRS	ASR 9000	ASR 1000	MWR 2941	ISR1900	ISR2900	ISR 3900	UBR7200	UBR10000	Cisco 4700	ASR901	ASR903
operStatus																Y					Y										Y
bandwidthTransmit																Y					Y										Y
bfdTemplate																Y															Y
workingLspNum																Y					Y										Y
protectLspNum																Y					Y										Y
wlBfdState																Y					Y										Y
plBfdState																Y					Y										Y
wlFaultOAM																Y					Y										Y
plFaultOAM																Y					Y										Y
pseudowireList																Y					Y										Y
direction																Y					Y										Y
lspEndPoints																Y					Y										Y
lspMidPoints																Y					Y										Y
internalId																Y					Y										Y
tpDescription																Y					Y										Y
PeerTunnelId																Y					Y										Y
PeerGlobalId																Y					Y										Y
MPLSTPDirection																Y					Y										Y
IMO Name—ILSPEntry																															
lspId																Y					Y										Y
internalId																Y					Y										Y
umc																Y					Y										Y
lspType																Y					Y										Y
IMO Name—ILSPMPEntry																															
fwdInLabel																Y					Y										Y
fwdOutLabel																Y					Y										Y
fwdBandwidth																Y					Y										Y
fwdOutInterface																Y					Y										Y
revInLabel																Y					Y										Y
revOutLabel																Y					Y										Y
revOutLinkId																Y					Y										Y
revBandwidth																Y					Y										Y
revOutInterface																Y					Y										Y
bandwidthDiff																Y					Y										Y

Table 6-134 MPLS-TP Attribute Support on Cisco Routers—Cisco Prime Network 3.9 (continued)

Attribute	800	1000	1600	1700	1800	2500	2600	2800	3600	3700	3800	7200	7300	7400	7500	7600	10000	12000	XR 12000	CRS	ASR 9000	ASR 1000	MWR 2941	ISR1900	ISR2900	ISR 3900	UBR7200	UBR10000	Cisco 4700	ASR901	ASR903
IMO Name—ILSPEPEntry																															
inLabel																Y					Y										Y
outLabel																Y					Y										Y
outLinkId																Y					Y										Y
bandwidth																Y					Y										Y
outInterface																Y					Y										Y
state																Y					Y										Y
IMO Name—ITPEnabledLink																															
linkId																Y					Y										Y
interfaceAddress																Y					Y										Y
nextHop																Y					Y										Y
IMO Name—IMPLSTPBfdSession																															
lspType																Y					Y										Y

VPN (VRF)

Table 6-135 VPN (VRF) Attribute Support on Cisco Routers—Cisco Prime Network 3.9

Attribute	800	1000	1600	1700	1800	2500	2600	2800	3600	3700	3800	7200	7300	7400	7500	7600	10000	12000	XR 12000	CRS	ASR 9000	ASR 1000	MWR 2941	ISR1900	ISR2900	ISR 3900	UBR7200	UBR10000	Cisco 4700	ASR901	ASR903	ASR 5000
IMO Name—IVrf																																
Virtual Routing Table												Y		Y		Y	Y		Y	Y [1]	Y [2]	Y	Y				Y	Y	Y	Y	Y	Y
Exported Route Targets											Y	Y		Y		Y	Y		Y	Y	Y	Y	Y				Y	Y	Y	Y	Y	Y
Imported Route Targets											Y	Y		Y		Y	Y		Y	Y	Y	Y	Y				Y	Y	Y	Y	Y	Y
Route Distinguisher									Y	Y	Y	Y		Y		Y	Y	Y	Y	Y	Y	Y	Y				Y	Y	Y	Y	Y	Y
ARP Entity								Y		Y	Y	Y		Y		Y	Y	Y	Y	Y	Y	Y	Y				Y	Y	Y	Y	Y	Y
Name									Y	Y	Y	Y		Y		Y	Y	Y	Y	Y	Y	Y	Y				Y	Y	Y	Y	Y	Y
Logical Sons							Y		Y	Y	Y	Y		Y		Y	Y	Y				Y	Y				Y	Y	Y	Y	Y	Y
Description										Y	Y	Y		Y		Y	Y	Y	Y	Y [3]	Y [4]	Y	Y				Y	Y	Y	Y	Y	

Table 6-135 VPN (VRF) Attribute Support on Cisco Routers—Cisco Prime Network 3.9 (continued)

Attribute	800	1000	1600	1700	1800	2500	2600	2800	3600	3700	3800	7200	7300	7400	7500	7600	10000	12000	XR 12000	CRS	ASR 9000	ASR 1000	MWR 2941	ISR1900	ISR2900	ISR 3900	UBR7200	UBR10000	Cisco 4700	ASR901	ASR903	ASR 5000
Import Route-Map										Y	Y	Y		Y		Y	Y	Y	Y	Y[5]	Y[6]	Y	Y				Y	Y	Y	Y	Y	
Export Route-Map										Y	Y	Y		Y		Y	Y	Y	Y	Y[7]	Y[8]	Y	Y				Y	Y	Y	Y	Y	
IMO Name—IVrfEntry																																
Next Hop BGP Address									Y	Y	Y	Y		Y		Y	Y	Y	Y	Y[9]	Y[10]	Y	Y				Y	Y	Y	Y	Y	
Incoming and Outgoing Inner Label									Y	Y	Y	Y		Y		Y	Y	Y	Y	Y[11]	Y[12]	Y	Y				Y	Y	Y	Y	Y	
Outer Label									Y	Y	Y	Y		Y		Y	Y	Y	Y	Y[13]	Y[14]	Y	Y				Y	Y	Y	Y	Y	
Destination IP Subnet									Y	Y	Y	Y		Y		Y	Y	Y	Y	Y[15]	Y[16]	Y	Y				Y	Y	Y	Y	Y	Y
Next Hop IP Address									Y	Y	Y	Y		Y		Y	Y	Y	Y	Y[17]	Y[18]	Y	Y				Y	Y	Y	Y	Y	Y
Type									Y	Y	Y	Y		Y		Y	Y	Y	Y	Y[19]	Y[20]	Y	Y				Y	Y	Y	Y	Y	Y
Routing Protocol Type									Y	Y	Y	Y		Y		Y	Y	Y	Y	Y[21]	Y[22]	Y	Y				Y	Y	Y	Y	Y	Y
Outgoing Interface Name									Y	Y	Y	Y		Y		Y	Y	Y	Y	Y[23]	Y[24]	Y	Y				Y	Y	Y	Y	Y	Y
IMO Name—IMpBgp																																
BGP Identifier	Y				Y		Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y				Y	Y	Y	Y	Y	Y
Local Autonomous System					Y		Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y				Y	Y	Y	Y	Y	Y
Cross Virtual Routing Table						Y	Y		Y	Y	Y	Y		Y		Y	Y	Y				Y	Y				Y	Y	Y	Y	Y	
BGP Neighbors					Y	Y	Y	Y	Y	Y	Y	Y		Y		Y	Y	Y	Y	Y	Y	Y	Y				Y	Y	Y	Y	Y	Y
Logical Sons							Y		Y	Y		Y		Y		Y	Y	Y	Y			Y	Y				Y	Y	Y	Y	Y	

Table 6-135 VPN (VRF) Attribute Support on Cisco Routers—Cisco Prime Network 3.9 (continued)

Attribute	800	1000	1600	1700	1800	2500	2600	2800	3600	3700	3800	7200	7300	7400	7500	7600	10000	12000	XR 12000	CRS	ASR 9000	ASR 1000	MWR 2941	ISR1900	ISR2900	ISR 3900	UBR7200	UBR10000	Cisco 4700	ASR901	ASR903	ASR 5000
IMO Name—ICrossVrf																																
Virtual Routing Entries												Y		Y		Y	Y	Y	Y	Y [25]	Y [26]	Y	Y				Y		Y	Y	Y	
Virtual Routing Entity Name												Y		Y		Y	Y	Y	Y	Y [27]	Y [28]	Y	Y				Y		Y	Y	Y	
IMO Name—ICrossVrfRoutingEntry																																
Outgoing Virtual Routing Entity Identifier																												Y				
Incoming and Outgoing Virtual Routing Tags																												Y				
Destination IP Subnet									Y	Y		Y		Y		Y	Y	Y				Y	Y				Y	Y		Y	Y	
Next Hop IP Address									Y	Y		Y		Y		Y	Y	Y				Y	Y				Y	Y		Y	Y	
Type									Y	Y		Y		Y		Y	Y	Y				Y	Y				Y	Y		Y	Y	
Routing Protocol Type									Y	Y		Y		Y		Y	Y	Y				Y	Y				Y	Y		Y	Y	
Outgoing Interface Name																															Y	

[1, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28] In ANA 372 Feb DP and earlier - show route vrf $vrfName$ afi-all From ANA372 March DP - show route vrf all afi-all

[2, 3, 4, 16, 17, 18] In ANA 372 Feb DP and earlier - show vrf $vrfName$ ipv4 detail From ANA372 March DP - show vrf all ipv4 detail; In ANA 372 Feb DP and earlier - show vrf $vrfName$ ipv6 detail From ANA372 March DP - show vrf all ipv6 detail

PWE3

Table 6-136 PWE3 Attribute Support on Cisco Routers—Cisco Prime Network 3.9

Attribute	800	1000	1600	1700	1800	2500	2600	2800	3600	3700	3800	7200	7300	7400	7500	7600	10000	12000	XR 12000	CRS	ASR 9000	ASR 1000	MWR 2941	ISR1900	ISR2900	ISR 3900	UBR7200	UBR10000	Cisco 4700	ASR901	ASR903	ASR 5000
IMO Name—IPTPLayer2MplsTunnel																																
Local and Remote Router Addresses									Y	Y	Y	Y		Y		Y	Y	Y	Y [1]	Y [2]	Y	Y	Y [3]						Y	Y	Y	

Table 6-136 PWE3 Attribute Support on Cisco Routers—Cisco Prime Network 3.9 (continued)

Attribute	800	1000	1600	1700	1800	2500	2600	2800	3600	3700	3800	7200	7300	7400	7500	7600	10000	12000	XR 12000	CRS	ASR 9000	ASR 1000	MWR 2941	ISR1900	ISR2900	ISR 3900	UBR7200	UBR10000	Cisco 4700	ASR901	ASR903	ASR 5000
Local and Remote Virtual Connection Labels									Y	Y		Y		Y		Y	Y	Y	Y[4]	Y[5]	Y	Y	Y[6]						Y	Y	Y	
Tunnel Identification									Y	Y	Y	Y		Y		Y	Y	Y	Y[7]	Y[8]	Y	Y	Y[9]						Y	Y	Y	
Tunnel Status									Y	Y	Y	Y		Y		Y	Y	Y	Y[10]	Y[11]	Y	Y	Y[12]						Y	Y	Y	
Local and Remote Tunnel Interface											Y								Y[13]													
IANA Type									Y	Y		Y		Y		Y	Y	Y	Y[14]	Y	Y	Y	Y[15]						Y	Y	Y	
Containing CTPs																																
Contained CTPs																																
PsuedowireType												Y				Y		Y	Y	Y	Y	Y	Y[16]						Y	Y	Y	
PreferredPathTunnel												Y				Y		Y	Y	Y	Y	Y	Y[17]						Y	Y	Y	
LocalMTU												Y				Y		Y	Y	Y	Y	Y	Y[18]						Y	Y	Y	
RemoteMTU												Y				Y		Y	Y	Y	Y	Y	Y[19]						Y	Y	Y	
PeerStatus												Y				Y		Y	Y	Y	Y	Y	Y[20]						Y	Y	Y	
SignalingProtocol												Y				Y		Y	Y	Y	Y	Y	Y[21]						Y	Y	Y	
VFIName												Y				Y		Y	Y	Y	Y	Y	Y[22]						Y	Y	Y	
psuedowireRole									Y	Y		Y		Y		Y		Y	Y	Y	Y		Y[23]						Y	Y	Y	
PeerRouterIp																																

Table 6-136 PWE3 Attribute Support on Cisco Routers—Cisco Prime Network 3.9 (continued)

Attribute	800	1000	1600	1700	1800	2500	2600	2800	3600	3700	3800	7200	7300	7400	7500	7600	10000	12000	XR 12000	CRS	ASR 9000	ASR 1000	MWR 2941	ISR1900	ISR2900	ISR 3900	UBR7200	UBR10000	Cisco 4700	ASR901	ASR903	ASR 5000
LocalRouterIp																																
LocalVcLabel																																
PeerVcLabel																																

[1], 2, 3, 4, 5, 6, 7, 8, 9, 10Till ANA 3.6.2 show l2vpn xconnect detail | include (Group | AC: | PW:) show l2vpn xconnect group $groupName$ xc-name $xcname$ detail show l2vpn xconnect group $groupName$ detail From ANA 3.6.3 - show l2vpn xconnect detail

11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23Supported only on IOS 12.2(33)MRA (CSR3.2)

Security

Table 6-137 Security Attribute Support on Cisco Routers—Cisco Prime Network 3.9

Attribute	800	1000	1600	1700	1800	2500	2600	2800	3600	3700	3800	7200	7300	7400	7500	7600	10000	12000	XR 12000	CRS	ASR 9000	ASR 1000	MWR 2941	ISR1900	ISR2900	ISR 3900	UBR7200	UBR10000	Cisco 4700	ASR901	ASR903	ASR 5000
IMO Name—IAccessList																																
Type	Y						Y	Y	Y	Y		Y	Y	Y	Y	Y	Y	Y	Y[1]	Y[2]	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y
Access List Entries	Y	Y	Y	Y	Y		Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y[3]	Y[4]	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y
Name or Id	Y						Y	Y	Y	Y		Y	Y	Y	Y	Y	Y	Y	Y[5]	Y[6]	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y
Index	Y						Y	Y	Y	Y		Y	Y	Y	Y	Y	Y	Y	Y[7]	Y[8]	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y
IMO Name—IAccessListEntry																																
Entry Identification	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y[9]	Y[10]	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y
Action Logic	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y[11]	Y[12]	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y
Source and Destination Address	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y[13]	Y[14]	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y
Source and Destination Wildcard	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y[15]	Y[16]	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y

Table 6-137 Security Attribute Support on Cisco Routers—Cisco Prime Network 3.9 (continued)

Attribute	800	1000	1600	1700	1800	2500	2600	2800	3600	3700	3800	7200	7300	7400	7500	7600	10000	12000	XR 12000	CRS	ASR 9000	ASR 1000	MWR 2941	ISR1900	ISR2900	ISR 3900	UBR7200	UBR10000	Cisco 4700	ASR901	ASR903	ASR 5000
Protocol Type	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y[17]	Y[18]	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y
Source and Destination Port Ranges	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y[19]	Y[20]	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y
Source and Destination Port Action	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y[21]	Y[22]	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y
Protocol Specific Info	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y[23]	Y[24]	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	
Differential Services Code Points	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y[25]	Y[26]	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	
Type of Service	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y[27]	Y[28]	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	
Precedence	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y[29]	Y[30]	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	
Matches	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y[31]	Y[32]	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	

[1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 31, 3]2ANA 3.6.0 and earlier: show access-lists ipv4. ANA 3.6.1 and later: show running-config ipv4 access-list.

Hardware

Table 6-138 Hardware Attribute Support on Cisco Routers—Cisco Prime Network 3.9

Attribute	800	1000	1600	1700	1800	2500	2600	2800	3600	3700	3800	7200	7300	7400	7500	7600	10000	12000	XR 12000	CRS	ASR 9000	ASR 1000	MWR 2941	ISR1900	ISR2900	ISR 3900	UBR7200	UBR10000	Cisco 4700	ASR901	ASR903	ASR 5000
IMO Name—IChassis																																
Description	Y		Y		Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y
Equipment Holder Type		Y	Y	Y	Y				Y	Y	Y	Y		Y		Y	Y					Y	Y	Y	Y		Y	Y	Y	Y	Y	Y

Table 6-138 Hardware Attribute Support on Cisco Routers—Cisco Prime Network 3.9 (continued)

Attribute	800	1000	1600	1700	1800	2500	2600	2800	3600	3700	3800	7200	7300	7400	7500	7600	10000	12000	XR 12000	CRS	ASR 9000	ASR 1000	MWR 2941	ISR1900	ISR2900	ISR 3900	UBR7200	UBR10000	Cisco 4700	ASR901	ASR903	ASR 5000
Contained Equipment Holders																																
Contained Equipments																						Y										Y
Serial Number	Y		Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y
IMO Name—IShelf																																
Description																				Y												
Status																				Y												
Equipment Holder Type																																
Contained Equipment Holders																																
Contained Equipments																																
Serial Number																				Y												
IMO Name—IModule																																
Module Name	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y [1]	Y	Y	Y	Y	Y	Y		Y	Y	Y	Y	Y	Y
Module Description	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y
Software Version	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y		Y	Y	Y
Operational Status	Y	Y	Y	Y	Y	Y		Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y		Y	
Hardware Type + Version	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y		Y	Y	Y
Managed IP Address																																
Redundant Equipment																		Y	Y													
Configured Redundancy																Y		Y	Y	Y	Y	Y									Y	Y
Redundancy Status	Y		Y	Y		Y	Y				Y	Y				Y		Y	Y	Y	Y	Y	Y				Y			Y	Y	Y
Operational Status Last Changed	Y	Y	Y	Y	Y	Y	Y		Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y			Y	Y	Y	Y		Y	Y	Y	Y	Y	Y
Supported Physical Termination Points		Y	Y						Y	Y		Y		Y		Y	Y	Y	Y			Y	Y				Y	Y		Y	Y	
Serial Number (soft property)	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y
Slots Number								Y					Y		Y											Y			Y			Y

Table 6-138 Hardware Attribute Support on Cisco Routers—Cisco Prime Network 3.9 (continued)

Attribute	800	1000	1600	1700	1800	2500	2600	2800	3600	3700	3800	7200	7300	7400	7500	7600	10000	12000	XR 12000	CRS	ASR 9000	ASR 1000	MWR 2941	ISR1900	ISR2900	ISR 3900	UBR7200	UBR10000	Cisco 4700	ASR901	ASR903	ASR 5000
IMO Name—IPowerSupply																																
Same as IModule		Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y		Y	Y				Y	Y	Y	Y	Y	Y	Y	Y	Y		Y			
IMO Name—IFanTray																																
Same as IModule		Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y		Y	Y				Y	Y	Y	Y	Y	Y	Y	Y	Y		Y			
IMO Name—IPluggableTransceiver																																
ConnectorDescription		Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y		Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y
PID		Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y		Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y
ConnectorSerialNumber		Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y		Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y
ConnectorType		Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y		Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y
PluggablePortState		Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y		Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y
PluggableType		Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y		Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y
IMO Name—IManagedElement																																
IP Address	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y		Y	Y	Y	Y	Y	
Communication State	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y		Y	Y	Y	Y	Y	
Investigation State	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y		Y	Y	Y	Y	Y	
Element Category	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y		Y	Y	Y	Y	Y	
Element Type and Key	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y		Y	Y	Y	Y	Y	
Device Name	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y[2]		Y	Y	Y	Y	Y	
System Name	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	
System Description	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	
Up Time	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	
Software Version	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	
Vendor Identity	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y		Y	Y	Y	Y	Y	
Memory and CPU Usage	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y
DRAM Free	Y	Y	Y	Y	Y	Y	Y		Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y		Y	Y	Y	Y	Y	
DRAM Used	Y	Y	Y	Y	Y	Y	Y		Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	
DRAM Usage	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y																	Y	
Flash Device Size	Y	Y	Y	Y	Y	Y	Y		Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y		Y	Y	Y	Y	Y	
NVRAM Size	Y	Y	Y	Y	Y	Y	Y		Y	Y	Y	Y	Y	Y	Y	Y	Y	Y		Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	
Processor DRAM	Y	Y	Y	Y	Y	Y	Y		Y	Y	Y	Y	Y	Y	Y	Y	Y	Y		Y	Y	Y	Y	Y	Y		Y	Y	Y	Y	Y	

Table 6-138 Hardware Attribute Support on Cisco Routers—Cisco Prime Network 3.9 (continued)

Attribute	800	1000	1600	1700	1800	2500	2600	2800	3600	3700	3800	7200	7300	7400	7500	7600	10000	12000	XR 12000	CRS	ASR 9000	ASR 1000	MWR 2941	ISR1900	ISR2900	ISR 3900	UBR7200	UBR10000	Cisco 4700	ASR901	ASR903	ASR 5000
Sys Contact	Y	Y	Y	Y	Y	Y	Y		Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y
Sys Location	Y	Y	Y	Y	Y	Y	Y		Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y
Serial Number	Y	Y	Y	Y	Y	Y	Y		Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y
File Systems																			Y	Y	Y											
IMO Name—IContext																																
Name						Y	Y	Y	Y	Y		Y		Y		Y	Y	Y				Y	Y				Y			Y		Y
Bounded Connections																																
IP Address Pools																																
Forwarding Components List																																
Traffic Descriptors List																																
Tunnel Containers List																																
Data Link Aggregation Containers List																																
IMO Name—ISystemService																																
Type																																
Status																																
Up Time	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y				Y			Y		Y	
IMO Name—IBridge																																
Bridge Table	Y								Y					Y		Y	Y		Y	Y	Y		Y			Y				Y	Y	
Type	Y													Y		Y	Y		Y	Y	Y		Y			Y				Y	Y	
MAC Address	Y													Y		Y	Y				Y		Y			Y				Y	Y	
IP Interface	Y													Y		Y	Y		Y	Y	Y		Y			Y				Y	Y	Y
Name	Y						Y		Y					Y		Y	Y	Y	Y	Y	Y		Y			Y				Y	Y	Y
Logical Sons	Y						Y		Y					Y		Y	Y	Y	Y	Y	Y		Y			Y				Y	Y	
Vlan Type																			Y	Y										Y		
IMO Name—IBridgeEntry																																
Destination MAC	Y					Y	Y		Y					Y		Y	Y		Y		Y		Y			Y				Y	Y	
Outgoing Interface	Y					Y	Y		Y					Y		Y	Y		Y		Y		Y			Y				Y	Y	
IMO Name—Imodule																																
Operational Status	Y																															

[1]Blower modules are supported in XR versions 3.7.1 and above. PEM Modules are supported in XR versions Prime Network 3.8.1 and above. Pluggable modules are supported in XR versions 3.8.1 and above. Pluggable modules present under sub-modules are only supported. All ports in OCx modules will be modeled as SONET.The actual encapsulation is shown in the port properties.

[2]Device Name is Mapped to Element Name in GUI

Serial

Table 6-139 Serial Attribute Support on Cisco Routers—Cisco Prime Network 3.9

Attribute	800	1000	1600	1700	1800	2500	2600	2800	3600	3700	3800	7200	7300	7400	7500	7600	10000	12000	XR 12000	CRS	ASR 9000	ASR 1000	MWR 2941	ISR1900	ISR2900	ISR 3900	UBR7200	UBR10000	Cisco 4700	ASR901	ASR903	ASR 5000
IMO Name—IPhysicalLayer																																
Media Type		Y	Y	Y	Y	Y	Y			Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y				Y	Y	Y	Y	Y	Y
Clocking Source	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y			Y	Y	Y	Y	Y	Y	Y
Maximum Speed	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y			Y	Y	Y	Y	Y	Y	Y
Is Internal Port	Y	Y	Y	Y	Y	Y		Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y		Y	Y				Y	Y	Y	Y	Y	Y
Discarded Bandwidth																														Y		
Dropped Bandwidth																														Y		
Input Bandwidth			Y	Y		Y	Y	Y		Y																				Y		
Output Bandwidth			Y	Y		Y	Y	Y		Y																				Y		
Discarded and Received Input Data Counters	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y			Y	Y	Y	Y	Y	Y	Y
Dropped and Forward Output Data Counters	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y			Y	Y	Y	Y	Y	Y	Y
Administrative Status	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y			Y	Y	Y	Y	Y	Y	Y
Operational Status	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y			Y	Y	Y	Y	Y	Y	Y
Last Changed	Y	Y	Y		Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y		Y			Y	Y			Y	Y	Y	Y	Y	Y	Y
IANA Type	Y	Y			Y	Y	Y		Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y				Y	Y	Y	Y	Y	Y
Containing CTPs																														Y		
Contained CTPs																														Y		
Port Alias	Y	Y	Y	Y	Y	Y	Y		Y	Y	Y	Y	Y	Y	Y	Y	Y	Y		Y	Y	Y	Y			Y	Y	Y	Y	Y	Y	Y
Location	Y	Y	Y	Y	Y	Y	Y		Y	Y	Y	Y	Y	Y	Y	Y	Y	Y		Y	Y	Y	Y			Y	Y	Y		Y	Y	Y
Sending Alarms	Y	Y	Y	Y	Y	Y	Y		Y	Y	Y	Y	Y	Y	Y	Y	Y	Y		Y	Y	Y	Y			Y	Y	Y	Y	Y	Y	Y
Connector Description	Y	Y	Y	Y	Y	Y	Y		Y	Y	Y	Y		Y		Y	Y	Y	Y	Y	Y	Y	Y			Y	Y	Y	Y	Y	Y	Y

Table 6-139 Serial Attribute Support on Cisco Routers—Cisco Prime Network 3.9 (continued)

Attribute	800	1000	1600	1700	1800	2500	2600	2800	3600	3700	3800	7200	7300	7400	7500	7600	10000	12000	XR 12000	CRS	ASR 9000	ASR 1000	MWR 2941	ISR1900	ISR2900	ISR 3900	UBR7200	UBR10000	Cisco 4700	ASR901	ASR903	ASR 5000
Part ID	Y	Y	Y	Y	Y	Y	Y		Y	Y	Y	Y		Y		Y	Y	Y	Y	Y	Y	Y	Y			Y	Y	Y	Y	Y	Y	Y
Connector Serial Num	Y	Y	Y	Y	Y	Y	Y		Y	Y	Y	Y		Y		Y	Y	Y	Y	Y	Y	Y	Y			Y	Y	Y	Y	Y	Y	Y
Product	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y		Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y			Y	Y	Y	Y	Y		Y	
Status	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y		Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y			Y	Y	Y	Y	Y	Y	Y
Managed	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y		Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y			Y	Y	Y	Y	Y	Y	Y
Ipcore	Y																															

Additional Technologies

Table 6-140 Additional Technologies Attribute Support on Cisco Routers—Cisco Prime Network 3.9

Attribute	800	1000	1600	1700	1800	2500	2600	2800	3600	3700	3800	7200	7300	7400	7500	7600	10000	12000	XR 12000	CRS	ASR 9000	ASR 1000	MWR 2941	ISR1900	ISR2900	ISR 3900	UBR7200	UBR10000	Cisco 4700	ASR901	ASR903	ASR 5000
IMO Name—POS																																
POS	Y	Y		Y	Y	Y	Y	Y	Y	Y		Y		Y		Y	Y	Y	Y	Y		Y									Y	

IPoDWDM

Table 6-141 IPoDWDM Attribute Support on Cisco Routers—Cisco Prime Network 3.9

Attribute	800	1000	1600	1700	1800	2500	2600	2800	3600	3700	3800	7200	7300	7400	7500	7600	10000	12000	XR 12000	CRS	ASR 9000	ASR 1000	MWR 2941	ISR1900	ISR2900	ISR 3900	UBR7200	UBR10000	Cisco 4700	ASR901	ASR903	ASR 5000
IMO Name—IDWDM																																
laserStatus																																
txPower																			Y	Y												
rxPower																			Y	Y												
loopback																			Y	Y												
controllerStatus																			Y	Y												
wavelengthBand																			Y	Y												
msaItuChannel																			Y	Y												
frequency																			Y	Y												
wavelength																			Y	Y												

Table 6-141 IPoDWDM Attribute Support on Cisco Routers—Cisco Prime Network 3.9 (continued)

Attribute	800	1000	1600	1700	1800	2500	2600	2800	3600	3700	3800	7200	7300	7400	7500	7600	10000	12000	XR 12000	CRS	ASR 9000	ASR 1000	MWR 2941	ISR1900	ISR2900	ISR 3900	UBR7200	UBR10000	Cisco 4700	ASR901	ASR903	ASR 5000
g709Status																			Y	Y												
detectedAlarms																			Y	Y												
assertedAlarms																			Y	Y												
opticsType																			Y	Y												
rxLosThreshold																			Y	Y												
location																Y			Y	Y									Y		Y	
Transport Admin Status							Y	Y																								
IMO Name—IDwdmG709Info																																
Location																Y			Y	Y									Y		Y	
Status																Y			Y	Y									Y		Y	
OtuAlarmCounters																Y			Y	Y									Y		Y	
OduAlarmCounters																Y			Y	Y									Y		Y	
OtuAlarmReporting																Y			Y	Y									Y		Y	
OduAlarmReporting																Y			Y	Y									Y		Y	
OtuAssertedAlarms																Y			Y	Y									Y		Y	
OduAssertedAlarms																Y			Y	Y									Y		Y	
OtuDetectedAlarms																Y			Y	Y									Y		Y	
OduDetectedAlarms																Y			Y	Y									Y		Y	
OtuBerCounters																Y			Y	Y									Y		Y	
OtuBerReporting																Y			Y	Y									Y		Y	
OtuAssertedBers																Y			Y	Y									Y		Y	
OtuDetectedBers																Y			Y	Y									Y		Y	
OtuBerThreshold																			Y	Y												
OtuTTI																			Y	Y												
OduTTI																Y			Y	Y									Y		Y	
FecInfo																Y			Y	Y									Y		Y	
FecMode																Y			Y	Y									Y		Y	

Table 6-141 IPoDWDM Attribute Support on Cisco Routers—Cisco Prime Network 3.9 (continued)

Attribute	800	1000	1600	1700	1800	2500	2600	2800	3600	3700	3800	7200	7300	7400	7500	7600	10000	12000	XR 12000	CRS	ASR 9000	ASR 1000	MWR 2941	ISR1900	ISR2900	ISR 3900	UBR7200	UBR10000	Cisco 4700	ASR901	ASR903	ASR 5000
IMO Name—IDwdmPmSettings																																
Location																			Y	Y												
IntervalType																			Y	Y												
FecPmSettings																			Y	Y												
OpticsPmSettings																			Y	Y												
OtnPmSettings																			Y	Y												

LocalSwitching

Table 6-142 LocalSwitching Attribute Support on Cisco Routers—Cisco Prime Network 3.9

Attribute	800	1000	1600	1700	1800	2500	2600	2800	3600	3700	3800	7200	7300	7400	7500	7600	10000	12000	XR 12000	CRS	ASR 9000	ASR 1000	MWR 2941	ISR1900	ISR2900	ISR 3900	UBR7200	UBR10000	Cisco 4700	ASR901	ASR903	ASR 5000
IMO Name—ILocalSwitchingEntity																																
LocalSwitchingTable	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y		Y		Y		Y	Y	Y	Y	Y	Y	Y	Y			Y			Y		Y	
PWSwitchingTable																Y					Y										Y	
IMO Name—ILocalSwitchingEntry																																
Local Switching Entry Key	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y		Y		Y		Y	Y	Y	Y	Y	Y	Y	Y			Y			Y		Y	
Local Switching Entry Status	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y		Y		Y		Y	Y	Y	Y	Y	Y	Y	Y			Y			Y		Y	
Segment 1	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y		Y		Y		Y	Y	Y	Y	Y	Y	Y	Y			Y			Y		Y	
Segment 1 Port Name	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y		Y		Y		Y	Y	Y	Y	Y	Y	Y	Y			Y			Y		Y	
Segment 1 Status	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y		Y		Y		Y	Y	Y	Y	Y	Y	Y	Y			Y			Y		Y	
Segment 2	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y		Y		Y		Y	Y	Y	Y	Y	Y	Y	Y			Y			Y		Y	
Segment 2 Port Name	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y		Y		Y		Y	Y	Y	Y	Y	Y	Y	Y			Y			Y		Y	
Segment 2 Status	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y		Y		Y		Y	Y	Y	Y	Y	Y	Y	Y			Y			Y		Y	

BFD

Table 6-143 BFD Attribute Support on Cisco Routers—Cisco Prime Network 3.9

Attribute	800	1000	1600	1700	1800	2500	2600	2800	3600	3700	3800	7200	7300	7400	7500	7600	10000	12000	XR 12000	CRS	ASR 9000	ASR 1000	MWR 2941	ISR1900	ISR2900	ISR 3900	UBR7200	UBR10000	Cisco 4700	ASR901	ASR903	ASR 5000
IMO Name—IBfdService																																
Status				Y								Y							Y	Y	Y	Y	Y	Y	Y	Y			Y	Y	Y	
IMO Name—IBfdCommon																																
RegisteredProtocols												Y				Y		Y				Y		Y	Y	Y					Y	
InterfaceName												Y				Y		Y				Y		Y	Y	Y					Y	
IMO Name—IBfdSession																																
SourceIp				Y								Y				Y			Y	Y [1]	Y	Y	Y	Y	Y	Y			Y	Y	Y	
DestinationIp				Y								Y				Y			Y	Y [2]	Y	Y	Y	Y	Y	Y			Y	Y	Y	
Interval				Y								Y				Y			Y	Y [3]	Y	Y	Y	Y	Y	Y			Y	Y	Y	
Multiplier				Y								Y				Y			Y	Y [4]	Y	Y	Y	Y	Y	Y			Y	Y	Y	
Protocol				Y								Y				Y			Y	Y [5]	Y	Y	Y	Y	Y	Y			Y	Y	Y	
State				Y								Y				Y			Y	Y [6]	Y	Y	Y	Y	Y	Y			Y	Y	Y	
Interface				Y								Y				Y			Y	Y [7]	Y	Y	Y	Y	Y	Y			Y	Y	Y	
Process				Y								Y				Y			Y	Y [8]	Y	Y	Y	Y	Y	Y			Y	Y	Y	

[1, 2, 3, 4, 5, 6, 7, 8] BFD Support on IPv6 is available only on CRS-1 devices.

Carrier Ethernet

Table 6-144 Carrier Ethernet Attribute Support on Cisco Routers—Cisco Prime Network 3.9

Attribute	800	1000	1600	1700	1800	2500	2600	2800	3600	3700	3800	7200	7300	7400	7500	7600	10000	12000	XR 12000	CRS	ASR 9000	ASR 1000	MWR 2941	ISR1900	ISR2900	ISR 3900	UBR7200	UBR10000	Cisco 4700	ASR901	ASR903	ASR 5000
IMO Name—IVsi																																
vsiInstanceName																Y			Y	Y	Y	Y	Y [1]			Y					Y	
vpnId																Y			Y	Y	Y	Y	Y [2]			Y					Y	
discoveryMode																Y			Y	Y	Y	Y	Y [3]			Y					Y	
vsiMode																Y			Y	Y	Y	Y	Y [4]			Y					Y	
Operational state																Y			Y	Y	Y	Y	Y [5]			Y					Y	
Administrative state																Y			Y	Y	Y	Y	Y [6]			Y					Y	
IMO Name—IPseudowireProperties																																
isSplitHorizonEnabled																Y			Y		Y	Y									Y	
isAutoDiscovered																Y			Y		Y	Y									Y	
IMO Name—IVLANTaggedInterface																																
InterfaceName												Y [7]	Y [8]			Y	Y [9]	Y [10]	Y [11]	Y	Y	Y	Y [12]	Y	Y	Y			Y	Y	Y	
Inner Vlan Id												Y [13]	Y [14]			Y	Y [15]	Y [16]	Y [17]	Y	Y	Y	Y [18]	Y	Y	Y			Y	Y	Y	
Outer Vlan Id												Y [19]	Y [20]			Y	Y [21]	Y [22]	Y [23]	Y	Y	Y	Y [24]	Y	Y	Y			Y	Y	Y	
Encap Type												Y [25]	Y [26]			Y	Y [27]	Y [28]	Y [29]	Y	Y	Y	Y [30]	Y	Y	Y			Y	Y	Y	
Operational state												Y [31]	Y [32]			Y	Y [33]	Y [34]	Y [35]	Y	Y	Y	Y [36]	Y	Y	Y			Y	Y	Y	
Administrative state												Y [37]	Y [38]			Y	Y [39]	Y [40]	Y [41]	Y	Y	Y	Y [42]	Y	Y	Y			Y	Y	Y	

Table 6-144 Carrier Ethernet Attribute Support on Cisco Routers—Cisco Prime Network 3.9 (continued)

Attribute	800	1000	1600	1700	1800	2500	2600	2800	3600	3700	3800	7200	7300	7400	7500	7600	10000	12000	XR 12000	CRS	ASR 9000	ASR 1000	MWR 2941	ISR1900	ISR2900	ISR 3900	UBR7200	UBR10000	Cisco 4700	ASR901	ASR903	ASR 5000
ConfiguredDescription												Y [43] [44]	Y [44]			Y	Y [45]	Y [46]	Y	Y	Y	Y	Y [47]	Y	Y	Y				Y	Y	
IMO Name—IEfp																																
EfpId																Y [48]					Y									Y	Y [49]	
RewriteParams																Y [50]					Y									Y	Y [51]	
EncapsParams																Y [52]					Y									Y	Y [53]	
AdminStatus																Y [54]					Y									Y	Y [55]	
OperStatus																Y [56]					Y									Y	Y [57]	
SplitHorizonGroup																Y [58]														Y	Y [59]	
MatchCriteria																Y [60]					Y									Y	Y [61]	
ConfiguredDescription																Y					Y									Y	Y	
GetServiceInstanceId																Y [62]					Y									Y	Y [63]	
SetServiceInstanceId																Y [64]					Y									Y	Y [65]	

[1, 2, 3, 4, 5, 6, 7] Supported for the below software versions 12.2(27)SBC2 12.2(31)SBX 12.0(33)S1 gt 12.0(32)S gt 12.2(28)SB gt 12.2(33)SRC gt 12.2(33)SRD gt 12.2(33)SRE gt 12.4(20)T gt 12.4(24)T

[8, 9, 10, 11, 12, 13, 14] Supported for the below software versions 12.2(31)SBX gt 12.2(28)SB gt 12.2(33)SRC gt 12.2(33)SRD gt 12.2(33)SRE gt 12.4(20)T gt 12.4(24)T

[15, 16, 17, 18, 19, 20, 21, 22, 23, 57, 58, 59, 60, 61, 62, 63, 64, 65] SNMP is used for versions greater than SRD.

[24, 25, 26, 27, 28, 29, 30] Supported in IOS versions 12.2(28)SB1 and above.

[31, 32, 33, 34, 35, 36, 37]Supported in IOS versions 12.0(31)S and above only.

[38, 39, 40, 41, 42, 43]Supported for versions greater than IOX 3.8

[44, 45, 46, 47, 48, 49]Supported only on IOS 12.2(33)MRA (CSR3.2)

[50, 51, 52, 53, 54, 55, 56]Not Supported in IOS 12.2(33)MRA (CSR3.2)

CDP

Table 6-145 CDP Attribute Support on Cisco Routers—Cisco Prime Network 3.9

Attribute	800	1000	1600	1700	1800	2500	2600	2800	3600	3700	3800	7200	7300	7400	7500	7600	10000	12000	XR 12000	CRS	ASR 9000	ASR 1000	MWR 2941	ISR1900	ISR2900	ISR 3900	UBR7200	UBR10000	Cisco 4700	ASR901	ASR903	ASR 5000
IMO Name—ICdpService																																
cdpHoldtime	Y	Y	Y	Y	Y	Y	Y		Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	
cdpMessageInterval	Y	Y	Y	Y	Y	Y	Y		Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	
cdpDeviceId	Y	Y	Y	Y	Y	Y	Y		Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	
cdpState	Y	Y	Y	Y	Y	Y	Y		Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	
cdpVersion	Y	Y	Y	Y	Y	Y	Y		Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	
IMO Name—ICdpNeighbor																																
remoteDeviceId	Y	Y	Y	Y	Y	Y	Y		Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	
remotePortId	Y	Y	Y	Y	Y	Y	Y		Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	
remoteIPAddress	Y	Y	Y	Y	Y	Y	Y		Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	
localPortId	Y	Y	Y	Y	Y	Y	Y		Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	

Discovery Protocol

Table 6-146 Discovery Protocol Attribute Support on Cisco Routers—Cisco Prime Network 3.9

Attribute	800	1000	1600	1700	1800	2500	2600	2800	3600	3700	3800	7200	7300	7400	7500	7600	10000	12000	XR 12000	CRS	ASR 9000	ASR 1000	MWR 2941	ISR1900	ISR2900	ISR 3900	UBR7200	UBR10000	Cisco 4700	ASR901	ASR903	ASR 5000
IMO Name—IDiscoveryProtocol																																
DiscoveryProtocol Type	Y	Y	Y	Y	Y	Y	Y		Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y			Y	Y	Y	Y	Y	Y	
Info	Y	Y	Y	Y	Y	Y	Y		Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	

Ethernet OAM

Table 6-147 Ethernet OAM Attribute Support on Cisco Routers—Cisco Prime Network 3.9

Attribute	800	1000	1600	1700	1800	2500	2600	2800	3600	3700	3800	7200	7300	7400	7500	7600	10000	12000	XR 12000	CRS	ASR 9000	ASR 1000	MWR 2941	ISR1900	ISR2900	ISR 3900	UBR7200	UBR10000	Cisco 4700	ASR901	ASR903	ASR 5000
IMO Name—ICfmService																																
cacheSize																Y			Y	Y	Y		Y [1]			Y				Y	Y	
maximumCacheSize																Y							Y [2]			Y				Y	Y	
holdTime																Y			Y	Y	Y		Y [3]			Y				Y	Y	
version																Y			Y	Y	Y		Y [4]			Y				Y	Y	
maintenanceIntermedatePointsTable																Y			Y	Y	Y		Y [5]			Y				Y	Y	
maintenanceDomain																Y			Y	Y	Y		Y [6]			Y				Y	Y	
IMO Name—IMaintenanceDomain																																
name																Y			Y	Y	Y		Y [7]			Y				Y	Y	
level																Y			Y	Y	Y		Y [8]			Y				Y	Y	
Id																Y			Y	Y	Y		Y [9]			Y				Y	Y	
maintenanceAssociation																Y			Y	Y	Y		Y [10]			Y				Y	Y	
IMO Name—IMaintenanceEndPoint																																
macAddress																Y			Y	Y	Y		Y [11]			Y				Y	Y	
Interface																Y			Y	Y	Y		Y [12]			Y				Y	Y	
continuityCheckStatus																Y			Y	Y	Y		Y [13]			Y				Y	Y	
direction																Y			Y	Y	Y		Y [14]			Y				Y	Y	

Table 6-147 Ethernet OAM Attribute Support on Cisco Routers—Cisco Prime Network 3.9 (continued)

Attribute	800	1000	1600	1700	1800	2500	2600	2800	3600	3700	3800	7200	7300	7400	7500	7600	10000	12000	XR 12000	CRS	ASR 9000	ASR 1000	MWR 2941	ISR1900	ISR2900	ISR 3900	UBR7200	UBR10000	Cisco 4700	ASR901	ASR903	ASR 5000
IMO Name—IMaintenanceAssociation																																
name																Y			Y	Y	Y		Y [15]			Y				Y	Y	
associationType																Y			Y	Y	Y		Y [16]			Y				Y	Y	
maximalMeps																Y			Y	Y	Y		Y [17]			Y				Y	Y	
continuityCheckInterval																Y			Y	Y	Y		Y [18]			Y				Y	Y	
continuityCheckEnable																Y			Y	Y	Y		Y [19]			Y				Y	Y	
crossCheckEnable																Y			Y	Y	Y		Y [20]			Y				Y	Y	
direction																Y			Y	Y	Y		Y [21]			Y				Y	Y	
bridge																Y			Y	Y	Y		Y [22]			Y				Y	Y	
maintenanceEndPoints																Y			Y	Y	Y		Y [23]			Y				Y	Y	
cfmRemoteMaintenanceEndPoints																Y			Y	Y	Y		Y [24]			Y				Y	Y	
IMO Name—IMaintenanceIntermediatePoint																																
level																Y			Y	Y	Y		Y [25]							Y	Y	
cfmInterface																Y			Y	Y	Y		Y [26]							Y	Y	
isAutocreated																Y			Y	Y	Y		Y [27]							Y	Y	

Table 6-147 Ethernet OAM Attribute Support on Cisco Routers—Cisco Prime Network 3.9 (continued)

Attribute	800	1000	1600	1700	1800	2500	2600	2800	3600	3700	3800	7200	7300	7400	7500	7600	10000	12000	XR 12000	CRS	ASR 9000	ASR 1000	MWR 2941	ISR1900	ISR2900	ISR 3900	UBR7200	UBR10000	Cisco 4700	ASR901	ASR903	ASR 5000
Vlans																Y			Y	Y	Y		Y [28]							Y	Y	
macAddress																Y			Y	Y	Y		Y [29]							Y	Y	
IMO Name—IRemoteMaintenanceEndPoint																																
mepId																Y			Y	Y	Y		Y [30]			Y				Y	Y	
macAddress																Y			Y	Y	Y		Y [31]			Y				Y	Y	
level																Y			Y	Y	Y		Y [32]			Y				Y	Y	
maintenanceEndPointStatus																Y			Y	Y	Y		Y [33]			Y				Y	Y	
maintenanceEndPointOid																Y			Y	Y	Y		Y [34]			Y				Y	Y	
IMO Name—IOAMData																																
adminState																Y					Y		Y	Y	Y	Y				Y	Y	
pduMaxRate																Y							Y	Y	Y	Y				Y	Y	
pduMinRate																Y					Y		Y	Y	Y	Y				Y	Y	
linkTimeout																Y					Y		Y	Y	Y	Y				Y	Y	
highThresholdAction																Y					Y		Y	Y	Y	Y				Y	Y	
linkFaultAction																Y					Y		Y	Y	Y	Y				Y	Y	
dyingGaspAction																Y					Y		Y	Y	Y	Y				Y	Y	
criticalEventAction																Y					Y		Y	Y	Y	Y				Y	Y	
mode																Y					Y		Y	Y	Y	Y				Y	Y	
unidirectional																Y					Y		Y	Y	Y	Y				Y	Y	
linkMonitor																Y					Y		Y	Y	Y	Y				Y	Y	
remoteLoopback																Y					Y		Y	Y	Y	Y				Y	Y	
portStatus																Y					Y		Y	Y	Y	Y				Y	Y	
loopbackStatus																Y					Y		Y	Y	Y	Y				Y	Y	

Table 6-147 Ethernet OAM Attribute Support on Cisco Routers—Cisco Prime Network 3.9 (continued)

Attribute	800	1000	1600	1700	1800	2500	2600	2800	3600	3700	3800	7200	7300	7400	7500	7600	10000	12000	XR 12000	CRS	ASR 9000	ASR 1000	MWR 2941	ISR1900	ISR2900	ISR 3900	UBR7200	UBR10000	Cisco 4700	ASR901	ASR903	ASR 5000
remoteData																Y					Y		Y	Y	Y	Y				Y	Y	
name																Y					Y		Y	Y	Y	Y				Y	Y	
ethernetPort																Y					Y		Y	Y	Y	Y				Y	Y	
IMO Name—IOAMRemoteData																																
macAddress																Y					Y		Y	Y	Y	Y				Y	Y	
vendor																Y					Y		Y	Y	Y	Y				Y	Y	
mode																Y					Y		Y	Y	Y	Y				Y	Y	
unidirection																Y					Y		Y	Y	Y	Y				Y	Y	
linkMonitor																Y					Y		Y	Y	Y	Y				Y	Y	
remoteLoopback																Y					Y		Y	Y	Y	Y				Y	Y	
IMO Name—IUNIProperties																																
UNIId																Y					Y		Y							Y	Y	
isServiceMultiplexing																Y					Y		Y							Y	Y	
isBundlingEnabled																Y					Y		Y							Y	Y	
bundlingType																Y					Y		Y							Y	Y	
IMO Name—IEthernetLMI																																
isGlobalEnabled																							Y							Y		
mode																							Y							Y		
ELMIInterfaces																Y					Y		Y							Y		
deviceEVCs																Y					Y		Y							Y		
IMO Name—IDeviceEVC																																
EVCName																Y					Y		Y							Y	Y	
EVCStatus																Y					Y		Y							Y	Y	
EVCType																Y					Y		Y							Y	Y	
cfmMaName																Y					Y		Y							Y	Y	
configuredRemoteUNICount																Y					Y		Y							Y	Y	
activeRemoteUNICount																Y					Y		Y							Y	Y	
UNIInterfaces																Y					Y		Y							Y	Y	
IMO Name—IUNIInterfaces																																
UNIStatus																Y					Y		Y							Y	Y	
UNIId																Y					Y		Y							Y	Y	
interfaceName																Y					Y		Y							Y	Y	

Table 6-147 Ethernet OAM Attribute Support on Cisco Routers—Cisco Prime Network 3.9 (continued)

Attribute	800	1000	1600	1700	1800	2500	2600	2800	3600	3700	3800	7200	7300	7400	7500	7600	10000	12000	XR 12000	CRS	ASR 9000	ASR 1000	MWR 2941	ISR1900	ISR2900	ISR 3900	UBR7200	UBR10000	Cisco 4700	ASR901	ASR903	ASR 5000
vlanList																Y					Y		Y							Y	Y	
lmiLinkStatus																Y					Y		Y							Y	Y	
IMO Name—IELMIInterfaces																																
interfaceName																Y					Y		Y							Y	Y	
T391																Y					Y		Y							Y	Y	
T392																Y					Y		Y							Y	Y	
N391																Y					Y		Y							Y	Y	
N393																Y					Y		Y							Y	Y	

[1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 31, 32, 33, 34]CFM is supported on IOS 12.2(33) MRA (CSR 3.2) and higher versions

CGN

Table 6-148 CGN Attribute Support on Cisco Routers—Cisco Prime Network 3.9

Attribute	800	1000	1600	1700	1800	2500	2600	2800	3600	3700	3800	7200	7300	7400	7500	7600	10000	12000	XR 12000	CRS	ASR 9000	ASR 1000	MWR 2941	ISR1900	ISR2900	ISR 3900	UBR7200	UBR10000	Cisco 4700	ASR901	ASR903	ASR 5000
IMO Name—ICgnService																																
cgnName																				Y [1]												
Locations																				Y [2]												
ServiceInterfaces																				Y [3]												
statistics																																
addressPools																																
prefferedLocations																																
associatedInterfaces																																
IMO Name—ICgnStatsEntry																																
StatName																				Y												
StatValue																				Y												
statisticsName																																
statisticsValue																																

Table 6-148 CGN Attribute Support on Cisco Routers—Cisco Prime Network 3.9 (continued)

Attribute	800	1000	1600	1700	1800	2500	2600	2800	3600	3700	3800	7200	7300	7400	7500	7600	10000	12000	XR 12000	CRS	ASR 9000	ASR 1000	MWR 2941	ISR1900	ISR2900	ISR 3900	UBR7200	UBR10000	Cisco 4700	ASR901	ASR903	ASR 5000
IMO Name—ICgnServiceAddressPool																																
outsideVrf																				Y [4]												
addressPool																				Y [5]												
insideVrf																				Y [6]												
addressFamily																				Y [7]												
IMO Name—ICgnServiceLocation																																
instanceName																				Y [8]												
location																				Y [9]												
infraInterface																				Y [10]												
locationType																				Y [11]												
redundancyStatus																																
IMO Name—ICgnServiceType																																
Name																				Y												
serviceType																				Y												
cgnStats																				Y												
IMO Name—ICgnServiceType Nat44																																
addressPools																				Y												
IMO Name—ICgnServiceTypeNat64																																
addressFamilies																				Y												
ipv6Prefix																				Y												
IMO Name—ICgnServiceTypeTunnel																																
addressFamilies																				Y												
ipv6Prefix																				Y												
sourceAddress																				Y												
tunnelSubMode																				Y												
Ipv6Address																				Y												
Prefix																				Y												

Table 6-148 CGN Attribute Support on Cisco Routers—Cisco Prime Network 3.9 (continued)

Attribute	800	1000	1600	1700	1800	2500	2600	2800	3600	3700	3800	7200	7300	7400	7500	7600	10000	12000	XR 12000	CRS	ASR 9000	ASR 1000	MWR 2941	ISR1900	ISR2900	ISR 3900	UBR7200	UBR10000	Cisco 4700	ASR901	ASR903	ASR 5000
Suffix																				Y												
Mtu																																
IMO Name—ICgnServiceAddressFamily																																
ServiceAppInterface																																
address Family																																
IMO Name—ICgnIPInterface																																
interface																																

[1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11] show running-config interface ServiceApp* | include "interface|serviceaddress",show running-config interface ServiceInfra* | include "interface|serviceaddress" was supported only in CRS XR 3.9.2

SBC

Table 6-149 SBC Attribute Support on Cisco Routers—Cisco Prime Network 3.9

Attribute	800	1000	1600	1700	1800	2500	2600	2800	3600	3700	3800	7200	7300	7400	7500	7600	10000	12000	XR 12000	CRS	ASR 9000	ASR 1000	MWR 2941	ISR1900	ISR2900	ISR 3900	UBR7200	UBR10000	Cisco 4700	ASR901	ASR903	ASR 5000
IMO Name—ISbcService																																
sbcMode																						Y										
releaseVersion																						Y										
applicationVersion																						Y										
haStatus																						Y										
IMO Name—ISBE																																
callRedirectLimit																						Y										
onholdTimeout																						Y										
IMO Name—IDBE																																
dbeLocationID																						Y										
dbeType																						Y										
IMO Name—IDbeMediaInterface																																
addressRange																						Y										
vrfName																						Y										
managedBy																						Y										
portRange																						Y										

Table 6-149 SBC Attribute Support on Cisco Routers—Cisco Prime Network 3.9 (continued)

Attribute	800	1000	1600	1700	1800	2500	2600	2800	3600	3700	3800	7200	7300	7400	7500	7600	10000	12000	XR 12000	CRS	ASR 9000	ASR 1000	MWR 2941	ISR1900	ISR2900	ISR 3900	UBR7200	UBR10000	Cisco 4700	ASR901	ASR903	ASR 5000
serviceClass																						Y										
status																						Y										
natMode																						Y										
termination																						Y										
IMO Name—ISbcAccount																																
name																						Y										
adjacencyList																						Y										
IMO Name—ISbeAaaInterface																																
networkId																						Y										
vrf																						Y										
IMO Name—ISbeBillingProperties																																
ldrCheckTime																						Y										
adminStatus																						Y										
operationStatus																						Y										
billingMethod																						Y										
localBillingAddress																						Y										
cachePath																						Y										
cacheMaxSize																						Y										
cacheMinorAlarm																						Y										
cacheMajorAlarm																						Y										
cacheCriticalAlarm																						Y										
retryInterval																						Y										
IMO Name—ISbeBillingInstanceProperties																																
instanceNr																						Y										
batchSize																						Y										
batchTime																						Y										
deactMode																						Y										
transportStatus																						Y										
adminStatus																						Y										
IMO Name—ISbeRadiusClientProperty																																
sbeRetryInterval																						Y										
clientType																						Y										
sbeConcurrentRequestsLimit																						Y										
sbeRetryLimit																						Y										

Table 6-149 SBC Attribute Support on Cisco Routers—Cisco Prime Network 3.9 (continued)

Attribute	800	1000	1600	1700	1800	2500	2600	2800	3600	3700	3800	7200	7300	7400	7500	7600	10000	12000	XR 12000	CRS	ASR 9000	ASR 1000	MWR 2941	ISR1900	ISR2900	ISR 3900	UBR7200	UBR10000	Cisco 4700	ASR901	ASR903	ASR 5000
radiusMode																						Y										
IMO Name—ISbeRadiusServerProperties																																
serverPriority																						Y										
serverKey																						Y										
portNumber																						Y										
IMO Name—ISbcAdjacencyEnd																																
peerSubnetRestrication																						Y										
isMediaPassthrough																						Y										
isHuntingTriggerDisabled																						Y										
huntingTriggers																						Y										
vrf																						Y										
localSignalingAddress																						Y										
remoteSignalingAddress																						Y										
localSignalingPort																						Y										
remoteSignalingPort																						Y										
operationStatus																						Y										
instanceName																						Y										
transportProtocol																						Y										
IMO Name—ISbcAdjacencyGroup																																
name																						Y										
adjacencyList																						Y										
IMO Name—ISbcSipAdjacencyEnd																																
preferredTransport																						Y										
registrationTargetAddress																						Y										
registrationTargetPor																						Y										
IMO Name—ISbcSipAdjacencyEndAuthRealm																																
domain																						Y										
username																						Y										
password																						Y										
IMO Name—ISbeConfiguredBlackList																																
blacklistType																						Y										

Table 6-149 SBC Attribute Support on Cisco Routers—Cisco Prime Network 3.9 (continued)

Attribute	800	1000	1600	1700	1800	2500	2600	2800	3600	3700	3800	7200	7300	7400	7500	7600	10000	12000	XR 12000	CRS	ASR 9000	ASR 1000	MWR 2941	ISR1900	ISR2900	ISR 3900	UBR7200	UBR10000	Cisco 4700	ASR901	ASR903	ASR 5000
instancename																						Y										
IMO Name—ISbeConfiguredBlackListEntry																																
eventType																						Y										
triggerSize																						Y										
triggerPeriod																						Y										
blackListingPeriod																						Y										
isDefaultTriggerSize																						Y										
isDefaultTriggerPeriod																						Y										
IMO Name—ISbeCurrentBlacklisting																																
sourceAddress																						Y										
isAllSourceAddresses																						Y										
sourcePortType																						Y										
sourcePortNumber																						Y										
timeRemaining																						Y										
IMO Name—ISbeCodecList																																
name																						Y										
IMO Name—ISbeCodecListEntry																																
minPacketizationPeriod																						Y										
codecName																						Y										
IMO Name—IDbeH248Profile																																
profileVersion																						Y										
packages																						Y										
IMO Name—ISbeMediaGateway																																
codecList																						Y										
ipAddress																						Y										
IMO Name—IDbeMGC																																
remoteIP																						Y										
remotePort																						Y										
transport																						Y										
IMO Name—ISbcH248ControlInterface																																
ipAddress																						Y										
transport																						Y										

Table 6-149 SBC Attribute Support on Cisco Routers—Cisco Prime Network 3.9 (continued)

Attribute	800	1000	1600	1700	1800	2500	2600	2800	3600	3700	3800	7200	7300	7400	7500	7600	10000	12000	XR 12000	CRS	ASR 9000	ASR 1000	MWR 2941	ISR1900	ISR2900	ISR 3900	UBR7200	UBR10000	Cisco 4700	ASR901	ASR903	ASR 5000
port																						Y										
IMO Name—ISbeGlobalHuntingTriggerList																																
huntingMode																						Y										
huntingTriggers																						Y										
IMO Name—ISbeCacPolicySet																																
firstScope																						Y										
IMO Name—ISbeCacPolicyTable																																
instanceName																						Y										
instanceDescription																						Y										
matchType																						Y										
IMO Name—ISbeCacRuleEntry																																
scope																						Y										
IMO Name—ISbeCallPolicySet																																
isActive																						Y										
policySetNumber																						Y										
name																						Y										
description																						Y										
IMO Name—ISbeCallPolicyTable																																
instanceName																						Y										
instanceDescription																						Y										
matchType																						Y										
IMO Name—ISbeCallRuleEntry																																
entryNumber																						Y										
action																						Y										
matchValue																						Y										
entryCategory																						Y										
IMO Name—ISbePolicySet																																
isActive																						Y										
policySetNumber																						Y										
name																						Y										
description																						Y										
IMO Name—ISbePolicyTable																																
matchType																						Y										
name																						Y										
description																						Y										

Table 6-149 SBC Attribute Support on Cisco Routers—Cisco Prime Network 3.9 (continued)

Attribute	800	1000	1600	1700	1800	2500	2600	2800	3600	3700	3800	7200	7300	7400	7500	7600	10000	12000	XR 12000	CRS	ASR 9000	ASR 1000	MWR 2941	ISR1900	ISR2900	ISR 3900	UBR7200	UBR10000	Cisco 4700	ASR901	ASR903	ASR 5000
IMO Name—ISbeRuleEntry																																
entryNumber																						Y										
action																						Y										
matchValue																						Y										
entryCategory																						Y										
IMO Name—ISbeSdpMatchTable																																
tableType																						Y										
matchStrings																						Y										
IMO Name—ISbeSdpPolicyTable																																
name																						Y										
IMO Name—ISbeQosProfile																																
classOfService																						Y										
markingType																						Y										
dscp																						Y										
ipPrecedence																						Y										
tos																						Y										
IMO Name—ISbeSipHeaderProfile																																
instanceName																						Y										
isInUse																						Y										
profileType																						Y										
description																						Y										
IMO Name—ISbeSipHeaderProfileEntry																																
entryNr																						Y										
action																						Y										
value																						Y										
conditions																						Y										
parameterProfile																						Y										
IMO Name—ISbeSipHeaderProfileHeader																																
name																						Y										
IMO Name—ISbeSipMethodProfile																																
isPassthrough																						Y										
IMO Name—ISbeSipMethodProfileMethod																																
instanceName																						Y										
action																						Y										
mapStatusCode																						Y										

Table 6-149 SBC Attribute Support on Cisco Routers—Cisco Prime Network 3.9 (continued)

Attribute	800	1000	1600	1700	1800	2500	2600	2800	3600	3700	3800	7200	7300	7400	7500	7600	10000	12000	XR 12000	CRS	ASR 9000	ASR 1000	MWR 2941	ISR1900	ISR2900	ISR 3900	UBR7200	UBR10000	Cisco 4700	ASR901	ASR903	ASR 5000
headerProfile																						Y										
IMO Name—ISbeSipOptionProfile																																
options																						Y										
IMO Name—ISbeSipParameterProfile																																
parameters																						Y										
IMO Name—ISbeSipProfile																																
instanceName																						Y										
isInUse																						Y										
profileType																						Y										
description																						Y										
IMO Name—ISbeSipTimerProperties																																
tcpConnectTimeout																						Y										
tcpIdleTimeout																						Y										
tlsIdleTimeout																						Y										
inviteTimeout																						Y										
udpFirstRetransmitInterval																						Y										
udpMaxRetransmitInterval																						Y										

AccessGatewayService

Table 6-150 AccessGatewayService Attribute Support on Cisco Routers—Cisco Prime Network 3.9

Attribute	800	1000	1600	1700	1800	2500	2600	2800	3600	3700	3800	7200	7300	7400	7500	7600	10000	12000	XR 12000	CRS	ASR 9000	ASR 1000	MWR 2941	ISR1900	ISR2900	ISR 3900	UBR7200	UBR10000	Cisco 4700	ASR901
IMO Name—IAccessGatewayService																														
AccessGWGroups																Y					Y									
IMO Name—IAccessGatewayGroup																														
AccessGWGroupName																Y					Y									
AccessGWGroupType																Y					Y									
AccessGWInterfacePropertiesTable																Y					Y									

Table 6-150 AccessGatewayService Attribute Support on Cisco Routers—Cisco Prime Network 3.9 (continued)

Attribute	800	1000	1600	1700	1800	2500	2600	2800	3600	3700	3800	7200	7300	7400	7500	7600	10000	12000	XR 12000	CRS	ASR 9000	ASR 1000	MWR 2941	ISR1900	ISR2900	ISR 3900	UBR7200	UBR10000	Cisco 4700	ASR901
IMO Name—IAccessGatewayInterfaceProperties																														
accessGWinterfaceKey																Y					Y									
interface																Y					Y									
accessGWConfigName																Y					Y									
accessGWConfigRevision																Y					Y									
accessGWMaxAge																Y					Y									
accessGWProviderBridge																					Y									
accessGWBridgeAddress																Y					Y									
accessGWPortIdentifier																Y					Y									
accessGWExternalCost																Y					Y									
accessGWHelloTime																Y					Y									
accessGWPortActive																Y					Y									
accessGWBPDUsSent																Y					Y									
accessGWReversionControlEnabled																					Y									
accessGWInstanceTable																Y					Y									
IMO Name—IAccessGatewayInstance																														
accessGWInstanceId																Y					Y									
accessGWVlanIds																Y					Y									
accessGWBridgePriority																Y					Y									
accessGWPortPriority																Y					Y									
accessGWCost																Y					Y									
accessGWRootBridgePriority																Y					Y									
accessGWRootBridgeAddress																Y					Y									
accessGWTopologyChanges																Y					Y									

Table 6-150 AccessGatewayService Attribute Support on Cisco Routers—Cisco Prime Network 3.9 (continued)

Attribute	800	1000	1600	1700	1800	2500	2600	2800	3600	3700	3800	7200	7300	7400	7500	7600	10000	12000	XR 12000	CRS	ASR 9000	ASR 1000	MWR 2941	ISR1900	ISR2900	ISR 3900	UBR7200	UBR10000	Cisco 4700	ASR901
accessGWExternalCost																Y					Y									

6PE

Table 6-151 6PE Attribute Support on Cisco Routers—Cisco Prime Network 3.9

Attribute	800	1000	1600	1700	1800	2500	2600	2800	3600	3700	3800	7200	7300	7400	7500	7600	10000	12000	XR 12000	CRS	ASR 9000	ASR 1000	MWR 2941	ISR1900	ISR2900	ISR 3900	UBR7200	UBR10000	Cisco 4700	ASR901
IMO Name—IBGPLabelRoutingEntry																														
label												Y				Y	Y	Y	Y	Y	Y	Y								

6rd

Table 6-152 6rd Attribute Support on Cisco Routers—Cisco Prime Network 3.9

Attribute	800	1000	1600	1700	1800	2500	2600	2800	3600	3700	3800	7200	7300	7400	7500	7600	10000	12000	XR 12000	CRS	ASR 9000	ASR 1000	MWR 2941	ISR1900	ISR2900	ISR 3900	UBR7200	UBR10000	Cisco 4700	ASR901
IMO Name—ITunnel6rd																														
ipv6Prefix																Y						Y								
sourceAddress																Y						Y								
tunnelSubMode																Y						Y								
prefix																Y						Y								
suffix																Y						Y								
mtu																Y						Y								

MLACP

Table 6-153 MLACP Attribute Support on Cisco Routers—Cisco Prime Network 3.9

Attribute	800	1000	1600	1700	1800	2500	2600	2800	3600	3700	3800	7200	7300	7400	7500	7600	10000	12000	XR 12000	CRS	ASR 9000	ASR 1000	MWR 2941	ISR1900	ISR2900	ISR 3900	UBR7200	UBR10000	Cisco 4700	ASR901	ASR903
IMO Name—IIccpRedundacyGroup																															
GroupNumber																Y					Y										Y
PeerMonitoringOption																Y					Y										Y
MemberIpAddres																Y					Y										Y
MemberDeviceName																Y					Y										Y
MLacpNodeId																Y					Y										Y
MLacpSystemMACAddress																Y					Y										Y
MLacpSystemPriority																Y					Y										Y
LinkAggregations																Y					Y										Y
BackboneInterfaces																Y					Y										Y
IMO Name—IIccpRedundacyContainer																															
IccpRedundancyGroups																Y					Y										Y
IMO Name—IMLacpProperties																															
IccpRedundancyGroup																Y					Y										Y
MLacpFailoverOption																					Y										
MLacpOperationalSystemMAC																Y					Y										Y
MLacpOperationalSystemPriority																Y					Y										Y
MLacpMaxBundle																Y					Y										Y
MLacpRole																Y					Y										Y

IPSec

Table 6-154 IPSec Attribute Support on Cisco Routers—Cisco Prime Network 3.9

Attribute	800	1000	1600	1700	1800	2500	2600	2800	3600	3700	3800	7200	7300	7400	7500	7600	10000	XR 12000	CRS	ASR 1000	MWR 2941	ISR1900	ISR2900	ISR 3900	UBR7200	UBR10000	Cisco 4700	ASR901	ASR903
IMO Name—IIPSecTunnel																													
ipsecName																		Y		Y									
vrf																		Y		Y									
ipAddress																		Y		Y									
tunnelSource																		Y		Y									
tunnelDestination																		Y		Y									
serviceLocation																		Y											
standbyInterface																		Y											
profile																		Y		Y									

Mobile

Table 6-155 Mobile Attribute Support on Cisco Routers—Cisco Prime Network 3.9

Attribute	800	1000	1600	1700	1800	2500	2600	2800	3600	3700	3800	7200	7300	7400	7500	7600	10000	XR 12000	CRS	ASR 9000	ASR 1000	MWR 2941	ISR1900	ISR2900	ISR 3900	UBR7200	UBR10000	Cisco 4700	ASR901	ASR903	ASR 5000
IMO Name—IAPN																															
apnName																															Y
accountingMode																															Y
apnSelectionMode																															Y
addressAllocationValidationPolicy																															Y
apnAllocationType																															Y
ipHeaderCompression																															Y
newcallPolicy																															Y
IMO Name—IPDPContextsParameters																															
pdpTContextType																															Y
primaryContexts																															Y
totalContexts																															Y
IMO Name—IAPNIPParameters																															
ipInputAccessGroup																															Y

Table 6-155 Mobile Attribute Support on Cisco Routers—Cisco Prime Network 3.9 (continued)

Attribute	800	1000	1600	1700	1800	2500	2600	2800	3600	3700	3800	7200	7300	7400	7500	7600	10000	XR 12000	CRS	ASR 9000	ASR 1000	MWR 2941	ISR1900	ISR2900	ISR 3900	UBR7200	UBR10000	Cisco 4700	ASR901	ASR903	ASR 5000
ipOutputAccessGroup																															Y
localIPGatewayAddr																															Y
nextHopGatewayAddr																															Y
isDiscardEnabled																															Y
IMO Name—IAPNChargingCharacteristics																															
homeBitBehavior																															Y
homeProfile																															Y
visitingBitBehavior																															Y
visitingProfile																															Y
roamingBitBehavior																															Y
roamingProfile																															Y
allBitBehavior																															Y
allBitProfile																															Y
radiusReturned																															Y
useGgsn																															Y
IMO Name—IRadiusServerConfiguration																															
radiusGroup																															Y
radiusSecondaryGroup																															Y
returnedFramedIpAddressPolicy																															Y
returnedUserNamePolicy																															Y
IMO Name—IMobileIP																															
mnHomeAgent																															Y
mnAlternateHomeAgent																															Y
mnAAARemovalIndication																															Y
mnHaSpi																															Y
mnHaSharedKey																															Y
mnHaHashAlgorithm																															Y
IMO Name—IAPNTunnel																															
tunnelType																															Y

Table 6-155 Mobile Attribute Support on Cisco Routers—Cisco Prime Network 3.9 (continued)

Attribute	800	1000	1600	1700	1800	2500	2600	2800	3600	3700	3800	7200	7300	7400	7500	7600	10000	XR 12000	CRS	ASR 9000	ASR 1000	MWR 2941	ISR1900	ISR2900	ISR 3900	UBR7200	UBR10000	Cisco 4700	ASR901	ASR903	ASR 5000
addressAllocationValidationPolicy																															Y
tunnelPeerLoadBalancing																															Y
IMO Name—IGSMQos																															
sduErrorRatio																															Y
residualBER																															Y
IMO Name—IAPNIPv6																															
addressPrefixPool																															Y
dnsPrimaryAddress																															Y
dnsSecondaryAddress																															Y
egressAddressFiltering																															Y
IMO Name—IQCIEntry																															
qci																															Y
dscp																															Y
IMO Name—IQCIARPEntry																															
qci																															Y
dscp																															Y
qciAllocationRetentionPriority																															Y
IMO Name—IVirtualAPN																															
preference																															Y
apnOid																															Y
abstractVirtualAPNRuleDefinition																															Y
IMO Name—IGGSNService																															
serviceName																															Y
status																															Y
authenticationServerTimeout																															Y
accountingServerTimeout																															Y
GTPU																															Y
PLMN Policy																															Y
AccountingContext																															Y

Table 6-155 Mobile Attribute Support on Cisco Routers—Cisco Prime Network 3.9 (continued)

Attribute	800	1000	1600	1700	1800	2500	2600	2800	3600	3700	3800	7200	7300	7400	7500	7600	10000	XR 12000	CRS	ASR 9000	ASR 1000	MWR 2941	ISR1900	ISR2900	ISR 3900	UBR7200	UBR10000	Cisco 4700	ASR901	ASR903	ASR 5000
LocalIPAddress																															Y
IMO Name—ISGSNEntry																															
IpAddress																															Y
SubnetMask																															Y
PLMNID																															Y
PLMN Foreign																															Y
Reject Foreign Subscriber																															Y
RAT Type																															Y
Description																															Y
IMO Name—IPLMNEntry																															
PLMN ID																															Y
Primary																															Y
IMO Name—IGTPUService																															
ServiceName																															Y
State																															Y
EchoInterval																															Y
MaxRetransmissions																															Y
RetransmissionTimeout																															Y
IPSECTunnelIdleTimeout																															Y
AllowErrorIndication																															Y
IncludeUDPPortExtHdr																															Y
ScriptMetadataOids																															Y



CHAPTER 7

Support Information for Cisco Switches

This chapter contains support information for Virtual Network Elements (VNEs) that manage Cisco switches in Cisco Prime Network 3.9.

This chapter contains the following topics:

- Cisco Catalyst 1900 Series Switches, page 7-2
- Cisco Catalyst 2900 Series Switches, page 7-3
- Cisco ME 3400 Series Ethernet Access Switches, page 7-6
- Cisco Catalyst 3500 XL Series Switches, page 7-9
- Cisco Catalyst 3550 Series Switches, page 7-12
- Cisco Catalyst 3560 Series Switches, page 7-14
- Cisco Catalyst 3750 Series Switches, page 7-17
- Cisco Catalyst 3750 Metro Series Switches, page 7-19
- Cisco Catalyst 4000 Series Switches, page 7-22
- Cisco Catalyst 4500 Series Switches, page 7-26
- Cisco Catalyst 4900 Series Switches, page 7-34
- Cisco ME 4900 Series Ethernet Switch, page 7-43
- Cisco Catalyst 5000 Series Switches, page 7-49
- Cisco Catalyst 6500 Series (CatOS) Switches, page 7-51
- Cisco Catalyst 6500 Series (IOS) Switches, page 7-56
- Cisco ME 6500 Series Ethernet Switches (6524), page 7-69
- Cisco ME 3600X Ethernet Access Switch, page 7-72
- Cisco ME 3800X Carrier Ethernet Switches, page 7-75
- Cisco Nexus 7000 Series Switches, page 7-78
- Cisco Nexus 5000 Series Switches, page 7-81
- Cisco Nexus 1000 Series Switches, page 7-84
- Cisco ACE 4700 Series Access Control Engine, page 7-85
- Cisco Service Control Engines, page 7-90
- Supported Technologies on Cisco Switches, page 7-92

Note For more information about the technologies described in this chapter , see Part 2 Technology Support.

Cisco Catalyst 1900 Series Switches

This section includes the following information about Catalyst 1900 switches (for information on the NE types supported in Cisco Prime Network 3.9, see Cisco Catalyst 1900 Series Switches):

- Catalyst 1900—Supported Software Versions, page 7-2
- Catalyst 1900—Supported Topologies, page 7-2
- Catalyst 1900—Supported Technologies, page 7-2
- Catalyst 1900—Supported Service Events, page 7-3

Catalyst 1900—Supported Software Versions

Table 7-1 Supported Software Versions for Catalyst 1900—Cisco Prime Network 3.9

Software Version	Product_Version
CatOS 9.00.04	3.7
CatOS 9.00.06	3.7

Catalyst 1900—Supported Topologies

Table 7-2 Supported Topologies for Catalyst 1900—Cisco Prime Network 3.9

Topology Type	Link Type	Product_Version
Ethernet	Ethernet	3.7
Physical Layer	Physical Layer	3.7
LAG	LAG	3.7

Catalyst 1900—Supported Technologies

The following technologies are supported by the Catalyst 1900 in Cisco Prime Network 3.9:

- IP, page 7-92
- Ethernet, page 7-99
- Hardware, page 7-124
- Serial, page 7-127
- CDP, page 7-132
- Discovery Protocol, page 7-132

Catalyst 1900—Supported Service Events

Table 7-3 Supported Service Events for Catalyst 1900—Cisco Prime Network 3.9

Event Name	Product_Version	Expedited
Active IP Interfaces Found	3.7	Y
All IP Interfaces Down	3.7	Y
BGP process up	3.7	N
Card Down	3.7	Y
Card Up	3.7	Y
CPU utilization exceeded upper threshold	3.7	N
Device Unsupported	3.7	N
Layer 2 Tunnel Down	3.7	N
Link up	3.7	N
Memory utilization exceeded upper threshold	3.7	N
Module Unsupported	3.7	N
MPLS Black Hole found	3.7	N
fan-tray down	Prime Network 3.8	N
fan-tray out	Prime Network 3.8	N
power-supply down	Prime Network 3.8	N

Cisco Catalyst 2900 Series Switches

This section includes the following information about Cisco Catalyst 2900 Series switches (for information on the NE types supported in Cisco Prime Network 3.9, see Cisco Catalyst 2900 Series Switches):

- Cisco Catalyst 2900 Series—Supported Software Versions, page 7-4
- Cisco Catalyst 2900 Series—Supported Topologies, page 7-4
- Cisco Catalyst 2900 Series—Supported Modules, page 7-4
- Cisco Catalyst 2900 Series—Supported Technologies, page 7-5
- Cisco Catalyst 2900 Series—Supported Service Events, page 7-5

Cisco Catalyst 2900 Series—Supported Software Versions

Table 7-4 Supported Software Versions for Cisco Catalyst 2900 Series—Cisco Prime Network 3.9

Software Version	Product_Version
12.0(5)WC17	3.6.2
12.1(22)EA8	3.6.2
12.1(22)EA8a	3.6.2
12.2(25)FX	3.6.0
12.2(25)SEE2	3.7.1
12.2(25)SEE3	3.7.1
CatOS 9.00.04	3.6.0

Cisco Catalyst 2900 Series—Supported Topologies

Table 7-5 Supported Topologies for Cisco Catalyst 2900 Series—Cisco Prime Network 3.9

Topology Type	Link Type	Product_Version
Ethernet	Ethernet	3.6.0
Physical Layer	Physical Layer	3.6.0
LAG	LAG	3.6.0

Cisco Catalyst 2900 Series—Supported Modules

Table 7-6 Supported Modules for Cisco Catalyst 2900 Series—Cisco Prime Network 3.9

Module Name	Product_Version	Module Description
WS-C2912-XL	3.6.0	12 fixed autosensing 10/100 ports
WS-C2924M-XL	3.6.0	24 fixed autosensing 10/100 ports 2 expansion slots
WS-C2948G	3.6.0	48 10/100 ports and 2 fixed, gigabit interface converter (GBIC)-based 1000BASE-X uplink ports 1.5 RU switch Catalyst OS installed
WS-X2948	3.6.0	Switching Supervisor

Cisco Catalyst 2900 Series—Supported Technologies

The following technologies are supported by the Cisco Catalyst 2900 Series in Cisco Prime Network 3.9:

- IP, page 7-92
- Ethernet, page 7-99
- Security, page 7-122
- Hardware, page 7-124
- Serial, page 7-127
- LLDP, page 7-131
- CDP, page 7-132
- Discovery Protocol, page 7-132

Cisco Catalyst 2900 Series—Supported Service Events

Table 7-7 Supported Service Events for Cisco Catalyst 2900 Series—Cisco Prime Network 3.9

Event Name	Product_Version	Expedited
Active IP Interfaces Found	3.6.0	Y
All IP Interfaces Down	3.6.0	Y
BGP process up	3.6.0	N
Card Down	3.6.0	Y
Card Up	3.6.0	Y
CPU utilization exceeded upper threshold	3.6.0	N
Device Unsupported	3.6.0	N
Layer 2 Tunnel Down	3.6.0	N
Link up	3.6.0	N
Memory utilization exceeded upper threshold	3.6.0	N
Module Unsupported	3.6.0	N
MPLS Black Hole found	3.6.0	N
rep port role change	Prime Network 3.8	Y
fan-tray down	Prime Network 3.8	N
fan-tray out	Prime Network 3.8	N

Table 7-7 Supported Service Events for Cisco Catalyst 2900 Series—Cisco Prime Network 3.9

Event Name	Product_Version	Expedited
power-supply down	Prime Network 3.8	N

Cisco ME 3400 Series Ethernet Access Switches

This section includes the following information about Cisco ME 3400 Series switches (for information on the NE types supported in Cisco Prime Network 3.9, see Cisco ME 3400 Series Ethernet Access Switches):

- Cisco ME 3400 Series—Supported Software Versions, page 7-6
- Cisco ME 3400 Series—Supported Topologies, page 7-7
- Cisco ME 3400 Series—Supported Modules, page 7-7
- Cisco ME 3400 Series—Supported Technologies, page 7-8
- Cisco ME 3400 Series—Supported Service Events, page 7-9

Cisco ME 3400 Series—Supported Software Versions

Table 7-8 Supported Software Versions for Cisco ME 3400 Series—Cisco Prime Network 3.9

Software Version	Product_Version
12.2(0.0.48)EY	3.6.5[1]
12.2(25)SEG	3.6.1
12.2(35)SE	3.6.1[2]
12.2(35)SE1	3.6.1[3]
12.2(35)SE3	3.6.1[4]
12.2(35)SE4	3.6.4[5]
12.2(37)SE	3.6.3[6]
12.2(37)SE1	3.6.4[7]
12.2(44)EY	3.6.5[8]
12.2(44)EY4	3.6.5[9]
12.2(44)SE	3.6.3[10]
12.2(44)SE1	3.6.4[11]
12.2(46)SE	3.6.4[12]
12.2(50)SE	3.6.6[13]
12.2(50)SE1	3.7[14]
12.2(52)SE	3.6.7[15]

Table 7-8 Supported Software Versions for Cisco ME 3400 Series—Cisco Prime Network 3.9

Software Version	Product_Version
12.2(53)SE	3.7[16]
12.3(22)S	3.6.1[17]
12.3(23)	3.6.1[18]
12.3(23)S1	3.6.1[19]
12.3(23)S2	3.6.1[20]
12.3(23)S3	3.6.1[21]
12.2(54)SE	3.7.1
12.2(55)SE	3.7.1.0.4[22]
12.2(58)SE	3.7.2-DP-3.0
12.2(58)SE1	3.7.X-DP-6.0
12.2(58)SE2	3.7.X-DP-7.0
12.2(58)EX	Cisco-ANA-3.7.x-DP15, Cisco-ANA-3.8-DP6

[1, 2, 3, 4, 5, 6, 7, 8, 10, 11, 12, 13, 17, 18, 19, 20, 21, 22]ANA models pluggable ports for this IOS version.

[9]Tested with modified version of 12.2(44)EY ANA models pluggable ports for this IOS version.

[14, 15, 16]ANA recognizes all maintenance builds in this IOS release train.ANA models pluggable ports for this IOS version.

Cisco ME 3400 Series—Supported Topologies

Table 7-9 Supported Topologies for Cisco ME 3400 Series—Cisco Prime Network 3.9

Topology Type	Link Type	Product_Version
Ethernet	Ethernet	3.6.5
Physical Layer	Physical Layer	3.6.5

Cisco ME 3400 Series—Supported Modules

Table 7-10 Supported Modules for Cisco ME 3400 Series—Cisco Prime Network 3.9

Module Name	Product_Version	Module Description
GLC-EX-SMD	3.6.7	1000BASE-EX extended SFP transceiver module

Table 7-10 Supported Modules for Cisco ME 3400 Series—Cisco Prime Network 3.9 (continued)

Module Name	Product_Version	Module Description
GLC-FE-100FX	3.6.7	100BaseFX-SFP module for 100 MB ports,1310 -nm wavelenght ,2 Km over MMF
GLC-FE-100LX	3.6.7	100BaseLX10-SFP module for 100 MB ports,1310 -nm wavelenght ,10 Km over SMF
GLC-LH-SM	3.6.4	1000BASE-LX/LH SFP transceiver module for MMF and SMF, 1300-nm wavelength
GLC-ZX-SM	3.7	Contains a Class 1 laser of 1550 nm for 1000BASE-ZX (extended wavelength) applications
ME340X-PWR-AC	3.6.7	AC power supply and fan module for ME-3400E-24TS-M and ME-3400EG-12CS-M
SFP-GE-L	3.6.4	1000BASE-LX/LH SFP transceiver module for MMF and SMF, 1300-nm wavelength, extended operating temperature range and DOM support
SFP-GE-S	3.6.7	1000BASE-Sx Short wavelength gigabit ethernet SFP.
SFP-GE-Z	3.6.7	1000BASE-Zx Extended reach gigabit ethernet SFP.
GLC-BX-D	3.7.1	1000BASE-BX10 SFP module for single-strand SMF, 1490-nm TX/1310-nm RX wavelength
GLC-BX-U	3.7.1	1000BASE-BX10 SFP module for single-strand SMF, 1310-nm TX/1490-nm RX wavelength

Cisco ME 3400 Series—Supported Technologies

The following technologies are supported by the Cisco ME 3400 Series in Cisco Prime Network 3.9:

- IP, page 7-92
- Routing Protocols, page 7-96
- Ethernet, page 7-99
- Security, page 7-122
- Hardware, page 7-124
- Serial, page 7-127
- Additional Technologies, page 7-128
- LLDP, page 7-131
- CDP, page 7-132
- Discovery Protocol, page 7-132
- Ethernet OAM, page 7-133

Cisco ME 3400 Series—Supported Service Events

Table 7-11 Supported Service Events for Cisco ME 3400 Series—Cisco Prime Network 3.9

Event Name	Product_Version	Expedited
Active IP Interfaces Found	3.6.1	Y
All IP Interfaces Down	3.6.1	Y
Card Down	3.6.1	Y
Card Up	3.6.1	Y
CPU utilization exceeded upper threshold	3.6.1	N
Device Unsupported	3.6.1	Y
Link down due to admin down	3.6.1	N
Link down due to oper down	3.6.1	N
Link up	3.6.1	N
Memory utilization exceeded upper threshold	3.6.1	N
Module Unsupported	3.6.1	Y
MPLS Black Hole found	3.6.1	N
Pluggable transceiver out	Prime Network 3.8	N
Rep port role change	Prime Network 3.8	Y

Cisco Catalyst 3500 XL Series Switches

This section includes the following information about Cisco Catalyst 3500 XL Series switches (for information on the NE types supported in Cisco Prime Network 3.9, see Cisco Catalyst 3500 XL Series Switches):

- Cisco Catalyst 3500 XL Series—Supported Software Versions, page 7-10
- Cisco Catalyst 3500 XL Series—Supported Topologies, page 7-10
- Cisco Catalyst 3500 XL Series—Supported Modules, page 7-10
- Cisco Catalyst 3500 XL Series—Supported Technologies, page 7-10
- Cisco Catalyst 3500 XL Series—Supported Service Events, page 7-11

Cisco Catalyst 3500 XL Series—Supported Software Versions

Table 7-12 Supported Software Versions for Cisco Catalyst 3500 XL Series—Cisco Prime Network 3.9

Software Version	Product_Version
Cat IOS 12.0(5)WC9a	3.6.0

Cisco Catalyst 3500 XL Series—Supported Topologies

Table 7-13 Supported Topologies for Cisco Catalyst 3500 XL Series—Cisco Prime Network 3.9

Topology Type	Link Type	Product_Version
Ethernet	Ethernet	3.6.0
Physical Layer	Physical Layer	3.6.0
LAG	LAG	3.6.2

Cisco Catalyst 3500 XL Series—Supported Modules

Table 7-14 Supported Modules for Cisco Catalyst 3500 XL Series—Cisco Prime Network 3.9

Module Name	Product_Version	Module Description
C3K-BLWR-60CFM	3.6.4	Fan Module for the Catalyst 3750-E and 3560-E Series

Cisco Catalyst 3500 XL Series—Supported Technologies

The following technologies are supported by the Cisco Catalyst 3500 XL Series in Cisco Prime Network 3.9:

- IP, page 7-92
- Ethernet, page 7-99
- Hardware, page 7-124
- Serial, page 7-127
- CDP, page 7-132
- Discovery Protocol, page 7-132

Cisco Catalyst 3500 XL Series—Supported Service Events

Table 7-15 Supported Service Events for Cisco Catalyst 3500 XL Series—Cisco Prime Network 3.9

Event Name	Product_Version	Expedited
Active IP Interfaces Found	3.6.0	Y
All IP Interfaces Down	3.6.0	Y
BGP process up	3.6.0	N
Card Down	3.6.0	Y
Card Up	3.6.0	Y
CPU utilization exceeded upper threshold	3.6.0	N
Device Unsupported	3.6.0	N
Layer 2 Tunnel Down	3.6.0	N
Link up	3.6.0	N
Memory utilization exceeded upper threshold	3.6.0	N
Module Unsupported	3.6.0	N
MPLS Black Hole found	3.6.0	N
Rx utilization exceeded upper threshold	3.6.0	N
Tx utilization exceeded upper threshold	3.6.0	N
rep port role change	Prime Network 3.8	Y
fan-tray down	Prime Network 3.8	N
fan-tray out	Prime Network 3.8	N
power-supply down	Prime Network 3.8	N

Cisco Catalyst 3550 Series Switches

This section includes the following information about Cisco Catalyst 3550 Series switches (for information on the NE types supported in Cisco Prime Network 3.9, see Cisco Catalyst 3550 Series Switches):

- Cisco Catalyst 3550 Series—Supported Software Versions, page 7-12
- Cisco Catalyst 3550 Series—Supported Topologies, page 7-12
- Cisco Catalyst 3550 Series—Supported Technologies, page 7-13
- Cisco Catalyst 3550 Series—Supported Service Events, page 7-13

Cisco Catalyst 3550 Series—Supported Software Versions

Table 7-16 Supported Software Versions for Cisco Catalyst 3550 Series—Cisco Prime Network 3.9

Software Version	Product_Version
12.1(11)EA	3.6.1
12.1(12c)EA1	3.6.1
12.1(13)EA	3.6.1
12.1(14)AX3	3.6.1
12.1(14)EA1	3.6.1
12.1(19)EA	3.6.1
12.1(20)EA	3.6.1
12.1(22)EA	3.6.1
12.1(22)EA6	3.6.1
12.1(22)EA8a	3.6.1

Cisco Catalyst 3550 Series—Supported Topologies

Table 7-17 Supported Topologies for Cisco Catalyst 3550 Series—Cisco Prime Network 3.9

Topology Type	Link Type	Product_Version
Ethernet	Ethernet	3.6.0
Physical Layer	Physical Layer	3.6.0
LAG	LAG	3.6.0

Cisco Catalyst 3550 Series—Supported Technologies

The following technologies are supported by the Cisco Catalyst 3550 Series in Cisco Prime Network 3.9:

- IP, page 7-92
- Ethernet, page 7-99
- Hardware, page 7-124
- Serial, page 7-127
- Additional Technologies, page 7-128
- CDP, page 7-132
- Discovery Protocol, page 7-132

Cisco Catalyst 3550 Series—Supported Service Events

Table 7-18 Supported Service Events for Cisco Catalyst 3550 Series—Cisco Prime Network 3.9

Event Name	Product_Version	Expedited
Active IP Interfaces Found	3.6.0	Y
All IP Interfaces Down	3.6.0	Y
Card Down	3.6.0	Y
Card Up	3.6.0	Y
CPU utilization exceeded upper threshold	3.6.0	N
Device Unsupported	3.6.0	N
IMA Operationally down	3.6.0	N
Link down due to admin down	3.6.0	N
Link down due to oper down	3.6.0	N
Link up	3.6.0	N
Memory utilization exceeded upper threshold	3.6.0	N
MLPPP Up	3.6.0	N
Module Unsupported	3.6.0	N
MPLS Black Hole found	3.6.0	N
rep port role change	Prime Network 3.8	Y
fan-tray down	Prime Network 3.8	N

Table 7-18 Supported Service Events for Cisco Catalyst 3550 Series—Cisco Prime Network 3.9

Event Name	Product_Version	Expedited
fan-tray out	Prime Network 3.8	N
power-supply down	Prime Network 3.8	N

Cisco Catalyst 3560 Series Switches

This section includes the following information about Cisco Catalyst 3560 Series switches (for information on the NE types supported in Cisco Prime Network 3.9, see Cisco Catalyst 3560 Series Switches):

- Cisco Catalyst 3560 Series—Supported Software Versions, page 7-14
- Cisco Catalyst 3560 Series—Supported Topologies, page 7-15
- Cisco Catalyst 3560 Series—Supported Modules, page 7-15
- Cisco Catalyst 3560 Series—Supported Technologies, page 7-16
- Cisco Catalyst 3560 Series—Supported Service Events, page 7-16

Cisco Catalyst 3560 Series—Supported Software Versions

Table 7-19 Supported Software Versions for Cisco Catalyst 3560 Series—Cisco Prime Network 3.9

Software Version	Product_Version
12.1(13)EA1a	3.6.0
12.1(14)EA1a	3.6.0
12.1(22)EA1	3.6.2
12.1(22)EA5	3.6.1
12.1(22)EA8a	3.6.1
12.1(25)EW	3.6.0
12.1(6)EA1a	3.6.0
12.2(25)SEC	3.6.2
12.2(25)SEC2	3.6.2
12.2(25)SED	3.6.0
12.2(25)SEE2	3.6.1

Table 7-19 Supported Software Versions for Cisco Catalyst 3560 Series—Cisco Prime Network 3.9 (continued)

Software Version	Product_Version
12.2(53)SE2	ANA3.8.X-DP6, ANA3.7.X-DP15

Cisco Catalyst 3560 Series—Supported Topologies

Table 7-20 Supported Topologies for Cisco Catalyst 3560 Series—Cisco Prime Network 3.9

Topology Type	Link Type	Product_Version
Ethernet	Ethernet	3.6.0
Physical Layer	Physical Layer	3.6.0
LAG	LAG	3.6.0

Cisco Catalyst 3560 Series—Supported Modules

Table 7-21 Supported Modules for Cisco Catalyst 3560 Series—Cisco Prime Network 3.9

Module Name	Product_Version	Module Description
C3K-BLWR-60CFM	3.6.4	Fan Module for the Catalyst 3750-E and 3560-E Series
WS-C3560-24PS	3.6.1	24 Ethernet 10/100 ports and 2 SFP-based Gigabit Ethernet ports
WS-C3560-48PS	3.6.0	48 Ethernet 10/100 ports and 4 SFP-based Gigabit Ethernet ports
WS-C3560-48TS	3.6.2	48 Ethernet 10/100 ports and 4 SFP-based Gigabit Ethernet ports
WS-C3560G-24PS	3.6.1	24 Ethernet 10/100/1000 ports and 4 SFP-based Gigabit Ethernet ports
WS-C3560G-24TS	3.6.1	24 Ethernet 10/100/1000 ports and 4 SFP-based Gigabit Ethernet ports
WS-C3560G-48PS	3.6.1	48 Ethernet 10/100/1000 ports and 4 SFP-based Gigabit Ethernet ports
WS-C3560G-48TS	3.6.0	48 Ethernet 10/100/1000 ports and 4 SFP-based Gigabit Ethernet ports

Cisco Catalyst 3560 Series—Supported Technologies

The following technologies are supported by the Cisco Catalyst 3560 Series in Cisco Prime Network 3.9:

- IP, page 7-92
- Routing Protocols, page 7-96
- Ethernet, page 7-99
- VPN (VRF), page 7-120
- Hardware, page 7-124
- Serial, page 7-127
- Additional Technologies, page 7-128
- CDP, page 7-132
- Discovery Protocol, page 7-132

Cisco Catalyst 3560 Series—Supported Service Events

Table 7-22 Supported Service Events for Cisco Catalyst 3560 Series—Cisco Prime Network 3.9

Event Name	Product_Version	Expedited
Active IP Interfaces Found	3.6.0	Y
All IP Interfaces Down	3.6.0	Y
BGP process up	3.6.0	N
Card Down	3.6.0	Y
Card Up	3.6.0	Y
CPU utilization exceeded upper threshold	3.6.0	N
Device Unsupported	3.6.0	N
Keepalive configured	3.6.0	N
Keepalive not configured	3.6.0	N
Layer 2 Tunnel Down	3.6.0	N
Link up	3.6.0	N
Memory utilization exceeded upper threshold	3.6.0	N
Module Unsupported	3.6.0	N
MPLS Black Hole found	3.6.0	N
Rx utilization exceeded upper threshold	3.6.0	N
Tx utilization exceeded upper threshold	3.6.0	N

Table 7-22 Supported Service Events for Cisco Catalyst 3560 Series—Cisco Prime Network 3.9

Event Name	Product_Version	Expedited
rep port role change	Prime Network 3.8	Y
pluggable transceiver out	Prime Network 3.8	N
fan-tray down	Prime Network 3.8	N
fan-tray out	Prime Network 3.8	N
power-supply down	Prime Network 3.8	N

Cisco Catalyst 3750 Series Switches

This section includes the following information about Cisco 3750 Series switches (for information on the NE types supported in Cisco Prime Network 3.9, see Cisco Catalyst 3750 Series Switches):

- Cisco 3750 Series—Supported Software Versions, page 7-17
- Cisco 3750 Series—Supported Topologies, page 7-18
- Cisco 3750 Series—Supported Modules, page 7-18
- Cisco 3750 Series—Supported Technologies, page 7-18
- Cisco 3750 Series—Supported Service Events, page 7-19

Cisco 3750 Series—Supported Software Versions

Table 7-23 Supported Software Versions for Cisco 3750 Series—Cisco Prime Network 3.9

Software Version	Product_Version
12.2(25)EY3	3.6.0
12.2(25)SEC2	3.6.2
12.2(52)SE	3.6.7
12.2(50)SE	3.6.7
12.2(53)SE2	ANA3.8.X-DP6, ANA3.7.X-DP15

Cisco 3750 Series—Supported Topologies

Table 7-24 Supported Topologies for Cisco 3750 Series—Cisco Prime Network 3.9

Topology Type	Link Type	Product_Version
Ethernet	Ethernet	3.6.0
Physical Layer	Physical Layer	3.6.0
LAG	LAG	3.6.2

Cisco 3750 Series—Supported Modules

Table 7-25 Supported Modules for Cisco 3750 Series—Cisco Prime Network 3.9

Module Name	Product_Version	Module Description
C3KX-NM-10G	ANA3.8.X-DP6, ANA3.7.X-DP15	Two 10GbE SFP+ ports network module with four physical ports with two SFP+ and two regular SFP ports
C3KX-PWR-350WAC	ANA3.8.X-DP6, ANA3.7.X-DP15	350W AC power supply

Cisco 3750 Series—Supported Technologies

The following technologies are supported by the Cisco 3750 Series in Cisco Prime Network 3.9:

- IP, page 7-92
- Ethernet, page 7-99
- Hardware, page 7-124
- Serial, page 7-127
- LLDP, page 7-131
- CDP, page 7-132
- Discovery Protocol, page 7-132

Cisco 3750 Series—Supported Service Events

Table 7-26 Supported Service Events for Cisco 3750 Series—Cisco Prime Network 3.9

Event Name	Product_Version	Expedited
Active IP Interfaces Found	3.6.0	Y
All IP Interfaces Down	3.6.0	Y
BGP process up	3.6.0	N
Card Down	3.6.0	Y
Card Up	3.6.0	Y
CPU utilization exceeded upper threshold	3.6.0	N
Device Unsupported	3.6.0	N
Layer 2 Tunnel Down	3.6.0	N
Link up	3.6.0	N
Memory utilization exceeded upper threshold	3.6.0	N
Module Unsupported	3.6.0	N
MPLS Black Hole found	3.6.0	N
Rx utilization exceeded upper threshold	3.6.0	N
Tx utilization exceeded upper threshold	3.6.0	N
rep port role change	Prime Network 3.8	Y

Cisco Catalyst 3750 Metro Series Switches

This section includes the following information about Cisco Catalyst 3750 Metro Series switches (for information on the NE types supported in Cisco Prime Network 3.9, see Cisco Catalyst 3750 Metro Series Switches):

- Cisco Catalyst 3750 Metro Series—Supported Software Versions, page 7-20
- Cisco Catalyst 3750 Metro Series—Supported Topologies, page 7-20
- Cisco Catalyst 3750 Metro Series—Supported Modules, page 7-21
- Cisco Catalyst 3750 Metro Series—Supported Technologies, page 7-21
- Cisco Catalyst 3750 Metro Series—Supported Service Events, page 7-22

Cisco Catalyst 3750 Metro Series—Supported Software Versions

Table 7-27 Supported Software Versions for Cisco Catalyst 3750 Metro Series—Cisco Prime Network 3.9

Software Version	Product_Version
12.2(25)EY*	3.6.3[1]
12.2(25)EY3	3.6.3[2]
12.2(25)SEB4	3.6.3[3]
12.2(25)SEG1	3.6.3[4]
12.2(35)SE	3.6.3[5]
12.2(37)SE*	3.6.3[6]
12.2(37)SE1	3.6.3[7]
12.2(40)SE	3.6.3[8]
12.2(44)SE1	3.6.3[9]
12.2(46)SE	3.6.4[10]
12.2(50)SE	3.6.6[11]
12.2(52)SE	3.6.7[12]
12.2(53)SE	3.7[13]
12.2(54)SE	3.7.1[14]
12.2(55)SE	3.7.1.0.4[15]
12.2(58)SE	3.7.2-DP-3.0
12.2(58)SE1	3.7.X-DP-6.0

[1, 2, 3, 4, 5, 6, 7, 8, 9, 10] ANA models pluggable ports for this IOS version.

[11, 12, 13, 14, 15] ANA recognizes all maintenance builds in this IOS release train.ANA models pluggable ports for this IOS version.

Cisco Catalyst 3750 Metro Series—Supported Topologies

Table 7-28 Supported Topologies for Cisco Catalyst 3750 Metro Series—Cisco Prime Network 3.9

Topology Type	Link Type	Product_Version
BGP	BGP	3.6.0
Ethernet	Ethernet	3.6.5
MPLS	MPLS	3.6.0
PPP/HDLC	PPP or HDLC	3.6.0
Physical Layer	Physical Layer	3.6.5

Cisco Catalyst 3750 Metro Series—Supported Modules

Table 7-29 Supported Modules for Cisco Catalyst 3750 Metro Series—Cisco Prime Network 3.9

Module Name	Product_Version	Module Description
CATALYST375024ME	3.6.0	Metro Ethernet Catalyst 3750 Module. 24-10/100 + 2 SFP (Small Formfactor Pluggable) ports for downlinks
GLC-EX-SMD	3.6.7	1000BASE-EX extended SFP transceiver module
GLC-LH-SM	3.6.5	1000BASE-LX/LH SFP transceiver module for MMF and SMF, 1300-nm wavelength
ME-C3750-24TE-FAN 0	3.7[1]	Fan Module for ME-C3750-24TE
PWR-ME3750-AC	3.7	Primary AC power supply
PWR-ME3750-DC	3.7	Primary DC power supply
SFP-GE-L	3.6.5	1000BASE-LX/LH SFP transceiver module for MMF and SMF, 1300-nm wavelength, extended operating temperature range and DOM support

[1]Tested by John C (Refer bug CSCtg86953)

Cisco Catalyst 3750 Metro Series—Supported Technologies

The following technologies are supported by the Cisco Catalyst 3750 Metro Series in Cisco Prime Network 3.9:

- IP, page 7-92
- Routing Protocols, page 7-96
- Ethernet, page 7-99
- MPLS, page 7-116
- MPLS-TE, page 7-118
- VPN (VRF), page 7-120
- PWE3, page 7-121
- Security, page 7-122
- Hardware, page 7-124
- Serial, page 7-127
- Additional Technologies, page 7-128
- LocalSwitching, page 7-128
- BFD, page 7-129
- LLDP, page 7-131
- CDP, page 7-132
- Discovery Protocol, page 7-132

- Ethernet OAM, page 7-133

Cisco Catalyst 3750 Metro Series—Supported Service Events

Table 7-30 Supported Service Events for Cisco Catalyst 3750 Metro Series—Cisco Prime Network 3.9

Event Name	Product_Version	Expedited
Active IP Interfaces Found	3.6.0	Y
All IP Interfaces Down	3.6.0	Y
BGP process up	3.6.0	N
Card Down	3.6.0	Y
Card Up	3.6.0	Y
CPU utilization exceeded upper threshold	3.6.0	N
Device Unsupported	3.6.0	Y
Keepalive configured	3.7	N
Keepalive not configured	3.7	N
Layer 2 Tunnel Down	3.6.0	N
Link up	3.6.0	N
Memory utilization exceeded upper threshold	3.6.0	N
Module Unsupported	3.6.0	Y
MPLS Black Hole found	3.6.0	N
Pluggable transceiver out	Prime Network 3.8	N
Rep port role change	Prime Network 3.8	Y
Rx utilization exceeded upper threshold	3.6.0	N
Tx utilization exceeded upper threshold	3.6.0	N

Cisco Catalyst 4000 Series Switches

This section includes the following information about Cisco Catalyst 4000 Series switches (for information on the NE types supported in Cisco Prime Network 3.9, see Cisco Catalyst 4000 Series Switches):

- Cisco Catalyst 4000 Series—Supported Software Versions, page 7-23

- Cisco Catalyst 4000 Series—Supported Topologies, page 7-23
- Cisco Catalyst 4000 Series—Supported Modules, page 7-23
- Cisco Catalyst 4000 Series—Supported Technologies, page 7-25
- Cisco Catalyst 4000 Series—Supported Service Events, page 7-25

Cisco Catalyst 4000 Series—Supported Software Versions

Table 7-31 Supported Software Versions for Cisco Catalyst 4000 Series—Cisco Prime Network 3.9

Software Version	Product_Version
IOS 12.1(12c)EW1	3.6.0[1]
IOS 12.2(20)EWA1	3.6.0[2]
IOS 12.2(25)SG	3.6.0[3]
IOS 12.2(31)SGA2	3.6.2[4]
IOS 12.2(50)SG1	3.6.7[5]
IOS 12.2(52)SG	3.6.7[6]
IOS 12.2(53)SG	3.7[7]

[1, 2, 3, 4]ANA models pluggable ports for this IOS version.

[5, 6, 7]ANA recognizes all maintenance builds in this IOS release train.ANA models pluggable ports for this IOS version.

Cisco Catalyst 4000 Series—Supported Topologies

Table 7-32 Supported Topologies for Cisco Catalyst 4000 Series—Cisco Prime Network 3.9

Topology Type	Link Type	Product_Version
Ethernet	Ethernet	3.6.0
Physical Layer	Physical Layer	3.6.0
LAG	LAG	3.6.2

Cisco Catalyst 4000 Series—Supported Modules

Table 7-33 Supported Modules for Cisco Catalyst 4000 Series—Cisco Prime Network 3.9

Module Name	Product_Version	Module Description
CWDM-SFP-1470	3.6.0	CWDM SFP 1470 nm, Gigabit Ethernet and 1G/2G FC

Table 7-33 Supported Modules for Cisco Catalyst 4000 Series—Cisco Prime Network 3.9

Module Name	Product_Version	Module Description
CWDM-SFP-1490	3.6.0	CWDM SFP 1490 nm, Gigabit Ethernet and 1G/2G FC
CWDM-SFP-1510	3.6.0	CWDM SFP 1510 nm, Gigabit Ethernet and 1G/2G FC
CWDM-SFP-1530	3.6.0	CWDM SFP 1530 nm, Gigabit Ethernet and 1G/2G FC
CWDM-SFP-1550	3.6.0	CWDM SFP 1550 nm, Gigabit Ethernet and 1G/2G FC
CWDM-SFP-1570	3.6.0	CWDM SFP 1570 nm, Gigabit Ethernet and 1G/2G FC
CWDM-SFP-1590	3.6.0	CWDM SFP 1590 nm, Gigabit Ethernet and 1G/2G FC
CWDM-SFP-1610	3.6.0	CWDM SFP 1610 nm, Gigabit Ethernet and 1G/2G FC
WS-U4504-FX-MT	3.6.0	FE Uplink Daughter Card, 4-port 100FX (MTRJ)
WS-X4014	3.6.0	Catalyst 4006 Supervisor 3, Spare
WS-X4124-FX-MT	3.6.0	FE Switching Module, 24-port 100FX (MTRJ)
WS-X4148-FX-MT	3.6.0	FE Switching Module, 48-100FX MMF (MTRJ)
WS-X4148-RJ	3.6.0	10/100 Fast Ethernet Module, 48 Ports (RJ-45)
WS-X4148-RJ21	3.6.0	Telco switch module, 48-port 10/100 (4xRJ21)
WS-X4148-RJ45V	3.6.0	Inline Power 10/100, 48-port (RJ45)
WS-X4232-GB-RJ	3.6.0	E/FE/GE Module, 2-GE (GBIC), 32-10/100 FE (RJ-45)
WS-X4232-RJ-XX	3.6.0	FE Base Module, 32-10/100(RJ45)+ Modular Uplink slot
WS-X4248-RJ21V	3.6.0	48-port PoE 10/100 BASE-TX switching module
WS-X4248-RJ45V	3.6.0	48-port PoE 10/100BASE-TX switching module
WS-X4302-GB	3.6.0	2-port 1000BASE-X (GBIC) Gigabit Ethernet
WS-X4306-GB	3.6.0	Gigabit Ethernet Module, 6 Ports (GBIC)
WS-X4412-2GB-T	3.6.0	GE Module, 12-1000T (RJ45)+2-1000X (GBIC Slot)
WS-X4418-GB	3.6.0	GE Module, Server Switching 18 Ports (GBIC)
WS-X4424-GB-RJ45	3.6.0	24-port 10/100/1000BASE-T Gigabit Ethernet switching module
WS-X4424-GB-RJ-45	3.6.0	24 port 10/100/1000 Auto-Sensing Module (RJ45)
WS-X4448-GB-LX	3.6.0	48-port 1000BASE-LX (SFP included) Gigabit Ethernet switching module
WS-X4448-GB-RJ45	3.6.0	48 port 10/100/1000 Auto-Sensing Module (RJ45)
WS-X4548-GB-RJ45	3.6.0	48-port Gigabit Ethernet 10/100/1000BASE-T switching module

Table 7-33 Supported Modules for Cisco Catalyst 4000 Series—Cisco Prime Network 3.9

Module Name	Product_Version	Module Description
WS-X4548-GB-RJ45V	3.6.0	48-port PoE 10/100/1000BASE-T switching module

Cisco Catalyst 4000 Series—Supported Technologies

The following technologies are supported by the Cisco Catalyst 4000 Series in Cisco Prime Network 3.9:

- IP, page 7-92
- Ethernet, page 7-99
- Hardware, page 7-124
- Serial, page 7-127
- CDP, page 7-132
- Discovery Protocol, page 7-132

Cisco Catalyst 4000 Series—Supported Service Events

Table 7-34 Supported Service Events for Cisco Catalyst 4000 Series—Cisco Prime Network 3.9

Event Name	Product_Version	Expedited
Active IP Interfaces Found	3.6.0	Y
All IP Interfaces Down	3.6.0	Y
BGP process up	3.6.0	N
Card Down	3.6.0	Y
Card In	3.6.0	Y
Card Out	3.6.0	Y
Card Up	3.6.0	Y
CPU utilization exceeded upper threshold	3.6.0	N
Device Unsupported	3.6.0	N
Keepalive configured	3.6.0	N
Keepalive not configured	3.6.0	N
Layer 2 Tunnel Down	3.6.0	N
Link up	3.6.0	N
Memory utilization exceeded upper threshold	3.6.0	N
Module Unsupported	3.6.0	N
MPLS Black Hole found	3.6.0	N

Table 7-34 Supported Service Events for Cisco Catalyst 4000 Series—Cisco Prime Network 3.9

Event Name	Product_Version	Expedited
Rx utilization exceeded upper threshold	3.6.0	N
Tx utilization exceeded upper threshold	3.6.0	N
rep port role change	Prime Network 3.8	Y
fan-tray down	Prime Network 3.8	N
fan-tray out	Prime Network 3.8	N
power-supply down	Prime Network 3.8	N

Cisco Catalyst 4500 Series Switches

This section includes the following information about Cisco Catalyst 4500 Series switches (for information on the NE types supported in Cisco Prime Network 3.9, see Cisco Catalyst 4500 Series Switches):

- Cisco Catalyst 4500 Series—Supported Software Versions, page 7-26
- Cisco Catalyst 4500 Series—Supported Topologies, page 7-27
- Cisco Catalyst 4500 Series—Supported Modules, page 7-28
- Cisco Catalyst 4500 Series—Supported Technologies, page 7-32
- Cisco Catalyst 4500 Series—Supported Service Events, page 7-33

Cisco Catalyst 4500 Series—Supported Software Versions

Table 7-35 Supported Software Versions for Cisco Catalyst 4500 Series—Cisco Prime Network 3.9

Software Version	Product_Version
12.1(13)EW	3.6.0
12.2(20)EWA	3.6.0[1]
12.2(25)EWA14	3.6.6[2]
12.2(31)SGA2	3.6.2[3]

Table 7-35 Supported Software Versions for Cisco Catalyst 4500 Series—Cisco Prime Network 3.9 (continued)

Software Version	Product_Version
12.2(50)SG1	3.6.7[4]
12.2(52)SG	3.6.6[5]
12.2(52)XO	3.6.7[6]
12.2(53)SG	3.7[7]
12.1(12c)EW1	3.6.0[8]
12.2(20)EWA1	3.6.0[9]
12.2(25)SG	3.6.0[10]
12.2(54)SG	3.7.1
12.2(53)SG1	3.7.1
12.2(53)SG2	3.7.1
12.2(53)SG3	ANA-3.7.2-DP1
12.2(53)SG4	ANA-3.7.2-DP2
15.0(2)SG	ANA-3.7.2-DP4
3.2.0SG	ANA-3.7.2-DP4

[1, 2, 3, 6, 8, 9, 10]ANA models pluggable ports for this IOS version.

[4, 5, 7]ANA recognizes all maintenance builds in this IOS release train.ANA models pluggable ports for this IOS version.

Cisco Catalyst 4500 Series—Supported Topologies

Table 7-36 Supported Topologies for Cisco Catalyst 4500 Series—Cisco Prime Network 3.9

Topology Type	Link Type	Product_Version
Ethernet	Ethernet	3.6.0
Framerelay	Framerelay	3.6.0
Physical Layer	Physical Layer	3.6.0
LAG	LAG	3.6.2

Cisco Catalyst 4500 Series—Supported Modules

Table 7-37 Supported Modules for Cisco Catalyst 4500 Series—Cisco Prime Network 3.9

Module Name	Product_Version	Module Description
CWDM-SFP-1550	3.7	CWDM 1550 NM SFP Gigabit Ethernet and 1G/2G FC
DWDM-X2-30.33=	3.7	10GBASE-DWDM 1530.33 nm X2 (100-GHz ITU grid)
DWDM-X2-31.12=	3.7	10GBASE-DWDM 1531.12 nm X2 (100-GHz ITU grid)
DWDM-X2-31.90=	3.7	10GBASE-DWDM 1531.90 nm X2 (100-GHz ITU grid)
DWDM-X2-32.68=	3.7	10GBASE-DWDM 1532.68 nm X2 (100-GHz ITU grid)
DWDM-X2-34.25=	3.7	10GBASE-DWDM 1534.25 nm X2 (100-GHz ITU grid)
DWDM-X2-35.04=	3.7	10GBASE-DWDM 1535.04 nm X2 (100-GHz ITU grid)
DWDM-X2-35.82=	3.7	10GBASE-DWDM 1535.82 nm X2 (100-GHz ITU grid)
DWDM-X2-36.61=	3.7	10GBASE-DWDM 1536.61 nm X2 (100-GHz ITU grid)
DWDM-X2-38.19=	3.7	10GBASE-DWDM 1538.19 nm X2 (100-GHz ITU grid)
DWDM-X2-38.98=	3.7	10GBASE-DWDM 1538.98 nm X2 (100-GHz ITU grid)
DWDM-X2-39.77=	3.7	10GBASE-DWDM 1539.77 nm X2 (100-GHz ITU grid)
DWDM-X2-40.56=	3.7	10GBASE-DWDM 1540.56 nm X2 (100-GHz ITU grid)
DWDM-X2-42.14=	3.7	10GBASE-DWDM 1542.14 nm X2 (100-GHz ITU grid)
DWDM-X2-42.94=	3.7	10GBASE-DWDM 1542.94 nm X2 (100-GHz ITU grid)
DWDM-X2-43.73=	3.7	10GBASE-DWDM 1543.73 nm X2 (100-GHz ITU grid)
DWDM-X2-44.53=	3.7	10GBASE-DWDM 1544.53 nm X2 (100-GHz ITU grid)
DWDM-X2-46.12=	3.7	10GBASE-DWDM 1546.12 nm X2 (100-GHz ITU grid)
DWDM-X2-46.92=	3.7	10GBASE-DWDM 1546.92 nm X2 (100-GHz ITU grid)

Table 7-37 Supported Modules for Cisco Catalyst 4500 Series—Cisco Prime Network 3.9

Module Name	Product_Version	Module Description
DWDM-X2-47.72=	3.7	10GBASE-DWDM 1547.72 nm X2 (100-GHz ITU grid)
DWDM-X2-48.51=	3.7	10GBASE-DWDM 1548.51 nm X2 (100-GHz ITU grid)
DWDM-X2-50.12=	3.7	10GBASE-DWDM 1550.12 nm X2 (100-GHz ITU grid)
DWDM-X2-50.92=	3.7	10GBASE-DWDM 1550.92 nm X2 (100-GHz ITU grid)
DWDM-X2-51.72=	3.7	10GBASE-DWDM 1551.72 nm X2 (100-GHz ITU grid)
DWDM-X2-52.52=	3.7	10GBASE-DWDM 1552.52 nm X2 (100-GHz ITU grid)
DWDM-X2-54.13=	3.7	10GBASE-DWDM 1554.13 nm X2 (100-GHz ITU grid)
DWDM-X2-54.94=	3.7	10GBASE-DWDM 1554.94 nm X2 (100-GHz ITU grid)
DWDM-X2-55.75=	3.7	10GBASE-DWDM 1555.75 nm X2 (100-GHz ITU grid)
DWDM-X2-56.55=	3.7	10GBASE-DWDM 1556.55 nm X2 (100-GHz ITU grid)
DWDM-X2-58.17=	3.7	10GBASE-DWDM 1558.17 nm X2 (100-GHz ITU grid)
DWDM-X2-58.98=	3.7	10GBASE-DWDM 1558.98 nm X2 (100-GHz ITU grid)
DWDM-X2-59.79=	3.7	10GBASE-DWDM 1559.79 nm X2 (100-GHz ITU grid)
DWDM-X2-60.61=	3.7	10GBASE-DWDM 1560.61 nm X2 (100-GHz ITU grid)
GLC-BX-D	3.7	1000BASE-BX10 SFP module for single-strand SMF, 1490-nm TX/1310-nm RX wavelength.
GLC-BX-U	3.7	1000BASE-BX10 SFP module for single-strand SMF, 1310-nm TX/1490-nm RX wavelength, single LC/PC connector
GLC-FE-100BX-D	3.7	1000BASE-BX10 SFP module for single-strand SMF, 1490-nm TX/1310-nm RX wavelength, single LC/PC connector
GLC-FE-100BX-U	3.7	100BASE-BX10-U SFP
GLC-FE-100FX	3.7	100BASE-FX SFP for FE port
GLC-FE-100LX	3.7	100BASE-LX SFP for FE port
GLC-FE-100ZX	3.7	100BASE-ZX SFP module for 100-MB ports, and 1550 nm wavelength, 80 km over SMF.

Table 7-37 Supported Modules for Cisco Catalyst 4500 Series—Cisco Prime Network 3.9

Module Name	Product_Version	Module Description
GLC-LH-SM	3.6.7	Transceiver module - SFP - Gigabit EN - 1000Base-LX, 1000Base-LH - 1300 nm
GLC-SX-MM	3.7	Transceiver module - SFP - Gigabit EN - 1000Base-SX - 850 nm
GLC-ZX-SM	3.6.7	1000BASE-ZX SFP
PWR-C45-1300ACV	3.6.4	Cisco Catalyst 4500 Series 1300W AC power supply (with integrated PoE)
PWR-C45-1400DC	3.6.7	Cisco Catalyst 4500 Series triple input 1400W DC power supply (data only)
PWR-C45-1400DC-P	3.7	Cisco Catalyst 4500 Series 1400W DC power supply with integrated power entry module (PEM)
PWR-C45-2800ACV	3.6.7	Cisco Catalyst 4500 Series 2800W AC power supply (with integrated PoE)
WS-G5483	3.7	Cisco Catalyst 4500 1400 WDC Power Supply with PEM (PoE)
WS-U4504-FX-MT	3.6.0	FE Uplink Daughter Card, 4-port 100FX (MTRJ)
WS-X4013+	3.6.0	Cisco Catalyst 4500 Series Supervisor Engine II-Plus
WS-X4013+10GE	3.7	Cisco Catalyst 4500 Series Supervisor Engine II-Plus-10GE
WS-X4013+TS	3.6.0	Cisco Catalyst 4500 Series Supervisor Engine II-Plus-TS, twelve 10/100/1000 PoE (RJ-45) and eight 1000-X SFP ports included on supervisor-engine faceplate
WS-X4014	3.6.0	Catalyst 4500 Supervisor II-Plus (IOS), 2GE,Console(RJ-45)
WS-X4124-FX-MT	3.6.0	FE Switching Module, 24-port 100FX (MTRJ)
WS-X4124-RJ45	3.6.0	Supervisor Engine III
WS-X4148-FE-BD-LC	3.6.0	24-Port 100BASE-FX Fast Ethernet Switching Module
WS-X4148-FE-LX-MT	3.6.0	24-Port 10/100BASE-TX Fast Ethernet Switching Module
WS-X4148-FX-MT	3.6.0	FE Switching Module, 48-100FX MMF (MTRJ)
WS-X4148-RJ	3.6.0	Cisco Catalyst 4500 10/100 Auto Module, 48-Port (RJ-45)
WS-X4148-RJ21	3.6.0	Telco switch module, 48-port 10/100 (4xRJ21)
WS-X4148-RJ45V	3.6.0	Inline Power 10/100, 48-port (RJ45)
WS-X4224-RJ45V	3.6.0	Catalyst 4500 10/100 Module, 48-Ports Telco (4xRJ21)
WS-X4232-GB-RJ	3.6.0	10/100BASE-TX Fast Ethernet switching module with Cisco pre-standard PoE

Table 7-37 Supported Modules for Cisco Catalyst 4500 Series—Cisco Prime Network 3.9

Module Name	Product_Version	Module Description
WS-X4232-L3	3.6.0	Catalyst 4500 10/100 PoE 802.3af 24-ports (RJ45)
WS-X4232-RJ-XX	3.6.0	Catalyst 4500 32-10/100 (RJ-45),2-GE(GBIC)
WS-X4248-FE-SFP	3.6.0	Layer 3 Services Module
WS-X4248-RJ21V	3.6.0	Catalyst 4500 10/100 Module,32-ports(RJ45)+Modular uplinks
WS-X4248-RJ45V	3.6.0	Catalyst 4500 48-Port 100BASE-X (SFPs Optional)
WS-X4302-GB	3.6.0	Catalyst 4500 PoE 802.3af 10/100, 48-Ports (RJ21)
WS-X4306-GB	3.6.0	Catalyst 4500 PoE 802.3af 10/100, 48-Ports (RJ45)
WS-X4412-2GB-T	3.6.0	Catalyst 4500 Gigabit Ethernet Module, 2-Ports (GBIC)
WS-X4418-GB	3.6.0	Catalyst 4500 Gigabit Ethernet Module, 6-Ports (GBIC)
WS-X4424-GB-RJ45	3.6.0	1000BASE-T plus 1000BASE-X Gigabit Ethernet switching module
WS-X4448-GB-LX	3.6.0	Catalyst 4500 GE Module, Server Switching 18-Ports (GBIC)
WS-X4448-GB-RJ45	3.6.0	Catalyst 4500 24-port 10/100/1000 Module (RJ45)
WS-X4448-GB-SFP	3.6.0	1000BASE-X Gigabit Ethernet switching module
WS-X4506-GB-T	3.6.0	Catalyst 4500 48-Port 10/100/1000 Module (RJ45)
WS-X4515	3.6.0	Catalyst 4500 48-Port 1000Base-X (SFPs Optional)
WS-X4516	3.6.0	Catalyst 4500 6-Port 10/100/1000 PoE or SFP (Optional)
WS-X4516-10GE	3.6.0	Catalyst 4500 Supervisor IV (2 GE),Console(RJ-45)
WS-X4524-GB-RJ45V	3.6.0	Catalyst 4500 Supervisor V (2 GE),Console(RJ-45)
WS-X4548-GB-RJ45	3.6.0	Catalyst 4500 Supervisor V-10GE, 2x10GE (X2) and 4x1GE (SFP)
WS-X4548-GB-RJ45V	3.6.0	Catalyst 4500 PoE 802.3af 10/ 100/1000 24-ports (RJ45)
WS-X45-SUP6-E	3.6.7	Catalyst 4500 Enhanced 48-Port 10/100/1000 Base-T (RJ-45)
WS-X45-SUP6L-E	3.6.7	Catalyst 4500 PoE 802.3af 10/100/1000, 48-Ports (RJ45)
WS-X4604-GWY	3.6.0	Catalyst 4000 Access Gateway Module
WS-X4606-X2-E	3.6.7	Cisco 4506 Power supply module
WS-X4624-SFP-E	3.6.7	1000BASE-LX/LH SFP transceiver module for MMF and SMF, 1300-nm wavelength
WS-X4648-RJ45V+E	3.7	Cisco Catalyst 4500 E-Series 48-Port 802.3af PoE and PoEP-ready 10/100/1000 (RJ-45)

Table 7-37 Supported Modules for Cisco Catalyst 4500 Series—Cisco Prime Network 3.9

Module Name	Product_Version	Module Description
WS-X4648-RJ45V-E	3.7	Cisco Catalyst 4500 E-Series 48-port 802.3af PoE 10/100/1000 (RJ-45)
X2-10GB-CX4	3.7	10 Gigabit Ethernet X2 with Copper Wire (Data and PoE)
X2-10GB-ER	3.6.7	Catalyst 4500 E-Series Sup 6-E, 2x10GE(X2) w/Twin Gig
X2-10GB-LR	3.6.7	Catalyst 4500 E-Series Sup 6L-E, 2x10GE(X2) w/Twin Gig
X2-10GB-LRM	3.7	10GBASE-LRM X2 transceiver module for MMF, 1310-nm wavelength, SC duplex connector
X2-10GB-LX4	3.7	10GBASE-LX4 X2 transceiver module for MMF, 1310-nm wavelength, SC duplex connector
X2-10GB-SR	3.7	10GBASE-ER X2 transceiver module for SMF, 1550-nm wavelength, SC duplex connector
X2-10GB-ZR	3.7	10GBASE-LR Serial 1310-nm long-reach, single-mode fiber (SMF), dispersion-shifted fiber (DSF)
WS-X4597-E	3.7[1]	Catalyst 4507R-E Fan Tray
WS-X45-SUP7-E	ANA-3.7.2-DP4	Sup 7-E 10GE (SFP+), 1000BaseX (SFP) with 4 SFP+ Ports
WS-X4712-SFP+E	ANA-3.7.2-DP4	10GE SFP+ with 12 SFP+ ports
WS-X4612-SFP-E	ANA-3.7.2-DP4	1000BaseX (SFP) with 12 SFP Ports Jumbo Frame Support
WS-X4640-CSFP-E	ANA-3.7.2-DP4	1000BaseX with 40-port SFP/80-port C-SFP Jumbo Frame Support

[1]Tested by John C(PLM).Refer bug-CSCtg86953

Cisco Catalyst 4500 Series—Supported Technologies

The following technologies are supported by the Cisco Catalyst 4500 Series in Cisco Prime Network 3.9:

- IP, page 7-92
- Routing Protocols, page 7-96
- Ethernet, page 7-99
- VPN (VRF), page 7-120
- Security, page 7-122
- Hardware, page 7-124

- Serial, page 7-127
- LLDP, page 7-131
- CDP, page 7-132
- Discovery Protocol, page 7-132

Cisco Catalyst 4500 Series—Supported Service Events

Table 7-38 Supported Service Events for Cisco Catalyst 4500 Series—Cisco Prime Network 3.9

Event Name	Product_Version	Expedited
Active IP Interfaces Found	3.6.0	Y
All IP Interfaces Down	3.6.0	Y
BGP process up	3.6.0	N
Card Down	3.6.0	Y
Card In	3.6.0	Y
Card Out	3.6.0	Y
Card Up	3.6.0	Y
CPU utilization exceeded upper threshold	3.6.0	N
Device Unsupported	3.6.0	N
Dropped packet rate exceeded upper threshold	3.6.0	N
Link up	3.6.0	N
Memory utilization exceeded upper threshold	3.6.0	N
Module Unsupported	3.6.0	N
rep port role change	Prime Network 3.8	Y
pluggable transceiver out	Prime Network 3.8	N
fan-tray down	Prime Network 3.8	N
fan-tray out	Prime Network 3.8	N
power-supply down	Prime Network 3.8	N

Cisco Catalyst 4900 Series Switches

This section includes the following information about Cisco Catalyst 4900 Series switches (for information on the NE types supported in Cisco Prime Network 3.9, see Cisco Catalyst 4900 Series Switches):

- Cisco Catalyst 4900 Series—Supported Software Versions, page 7-34
- Cisco Catalyst 4900 Series—Supported Topologies, page 7-35
- Cisco Catalyst 4900 Series—Supported Modules, page 7-35
- Cisco Catalyst 4900 Series—Supported Technologies, page 7-40
- Cisco Catalyst 4900 Series—Supported Service Events, page 7-41

Cisco Catalyst 4900 Series—Supported Software Versions

Table 7-39 Supported Software Versions for Cisco Catalyst 4900 Series—Cisco Prime Network 3.9

Software Version	Product_Version
IOS 12.2(25)EWA	3.6.3[1]
IOS 12.2(25)EWA2	3.6.3[2]
IOS 12.2(25)EWA4	3.6.2[3]
IOS 12.2(25)EWA6	3.6.2[4]
IOS 12.2(31)SG	3.6.1[5]
IOS 12.2(31)SGA1	3.6.1[6]
IOS 12.2(50)SG	3.7[7]
IOS 12.2(52)SG	3.6.6[8]
IOS 12.2(53)SG	3.7[9]
IOS 12.2(54)SG	3.7.1
IOS 12.2(53)SG1	3.7.1
IOS 12.2(53)SG4	ANA-3.7.2-DP2
IOS 15.0(2)SG	ANA-3.7.2-DP4

[1, 2, 3, 4, 5, 6] ANA models pluggable ports for this IOS version.

[7, 8, 9] ANA recognizes all maintenance builds in this IOS release train.ANA models pluggable ports for this IOS version.

Cisco Catalyst 4900 Series—Supported Topologies

Table 7-40 Supported Topologies for Cisco Catalyst 4900 Series—Cisco Prime Network 3.9

Topology Type	Link Type	Product_Version
Ethernet	Ethernet	3.6.1
Physical Layer	Physical Layer	3.6.1
LAG	LAG	3.6.1

Cisco Catalyst 4900 Series—Supported Modules

Table 7-41 Supported Modules for Cisco Catalyst 4900 Series—Cisco Prime Network 3.9

Module Name	Product_Version	Module Description
CAB-SM-LCSC-1M	3.6.1	1m fiber single-mode LC-to-SC connectors
CAB-SM-LCSC-5M	3.6.1	5m fiber single-mode LC-to-SC connectors
CSS5-CABLX-LCSC	3.6.1	Cisco CSS 11500 10m fiber single-mode LX LC-to-SC connectors
CSS5-CABSX-LC	3.6.1	Cisco CSS 11500 10m fiber multimode SX LC connectors
CSS5-CABSX-LCSC	3.6.1	Cisco CSS 11500 10m fiber multimode SX LC-to-SC connectors
CWDM-SFP-1470	3.6.1	Longwave 1470 nm laser single-mode
CWDM-SFP-1490	3.6.1	Longwave 1490 nm laser single-mode
CWDM-SFP-1510	3.6.1	Longwave 1510 nm laser single-mode
CWDM-SFP-1530	3.6.1	Longwave 1530 nm laser single-mode
CWDM-SFP-1550	3.6.1	Longwave 1550 nm laser single-mode
CWDM-SFP-1570	3.6.1	Longwave 1570 nm laser single-mode
CWDM-SFP-1590	3.6.1	Longwave 1590 nm laser single-mode
CWDM-SFP-1610	3.6.1	Longwave 1610 nm laser single-mode
CWDM-SFP-XXXX	3.6.1	CWDM small form-factor pluggable module
DWDM-X2-30.33=	3.7	10GBASE-DWDM 1530.33 nm X2 (100-GHz ITU grid)
DWDM-X2-31.12=	3.7	10GBASE-DWDM 1531.12 nm X2 (100-GHz ITU grid)
DWDM-X2-31.90=	3.7	10GBASE-DWDM 1531.90 nm X2 (100-GHz ITU grid)
DWDM-X2-32.68=	3.7	10GBASE-DWDM 1532.68 nm X2 (100-GHz ITU grid)

Table 7-41 Supported Modules for Cisco Catalyst 4900 Series—Cisco Prime Network 3.9

Module Name	Product_Version	Module Description
DWDM-X2-34.25=	3.7	10GBASE-DWDM 1534.25 nm X2 (100-GHz ITU grid)
DWDM-X2-35.04=	3.7	10GBASE-DWDM 1535.04 nm X2 (100-GHz ITU grid)
DWDM-X2-35.82=	3.7	10GBASE-DWDM 1535.82 nm X2 (100-GHz ITU grid)
DWDM-X2-36.61=	3.7	10GBASE-DWDM 1536.61 nm X2 (100-GHz ITU grid)
DWDM-X2-38.19=	3.7	10GBASE-DWDM 1538.19 nm X2 (100-GHz ITU grid
DWDM-X2-38.98=	3.7	10GBASE-DWDM 1538.98 nm X2 (100-GHz ITU grid)
DWDM-X2-39.77=	3.7	10GBASE-DWDM 1539.77 nm X2 (100-GHz ITU grid)
DWDM-X2-40.56=	3.7	10GBASE-DWDM 1540.56 nm X2 (100-GHz ITU grid)
DWDM-X2-42.14=	3.7	10GBASE-DWDM 1542.14 nm X2 (100-GHz ITU grid)
DWDM-X2-42.94=	3.7	10GBASE-DWDM 1542.94 nm X2 (100-GHz ITU grid)
DWDM-X2-43.73=	3.7	10GBASE-DWDM 1543.73 nm X2 (100-GHz ITU grid)
DWDM-X2-44.53=	3.7	10GBASE-DWDM 1544.53 nm X2 (100-GHz ITU grid)
DWDM-X2-46.12=	3.7	10GBASE-DWDM 1546.12 nm X2 (100-GHz ITU grid)
DWDM-X2-46.92=	3.7	10GBASE-DWDM 1546.92 nm X2 (100-GHz ITU grid)
DWDM-X2-47.72=	3.7	10GBASE-DWDM 1547.72 nm X2 (100-GHz ITU grid)
DWDM-X2-48.51=	3.7	10GBASE-DWDM 1548.51 nm X2 (100-GHz ITU grid)
DWDM-X2-50.12=	3.7	10GBASE-DWDM 1550.12 nm X2 (100-GHz ITU grid)
DWDM-X2-50.92=	3.7	10GBASE-DWDM 1550.92 nm X2 (100-GHz ITU grid)
DWDM-X2-51.72=	3.7	10GBASE-DWDM 1551.72 nm X2 (100-GHz ITU grid)
DWDM-X2-52.52=	3.7	10GBASE-DWDM 1552.52 nm X2 (100-GHz ITU grid)

Table 7-41 Supported Modules for Cisco Catalyst 4900 Series—Cisco Prime Network 3.9

Module Name	Product_Version	Module Description
DWDM-X2-54.13=	3.7	10GBASE-DWDM 1554.13 nm X2 (100-GHz ITU grid)
DWDM-X2-54.94=	3.7	10GBASE-DWDM 1554.94 nm X2 (100-GHz ITU grid)
DWDM-X2-55.75=	3.7	10GBASE-DWDM 1555.75 nm X2 (100-GHz ITU grid)
DWDM-X2-56.55=	3.7	10GBASE-DWDM 1556.55 nm X2 (100-GHz ITU grid)
DWDM-X2-58.17=	3.7	10GBASE-DWDM 1558.17 nm X2 (100-GHz ITU grid)
DWDM-X2-58.98=	3.7	10GBASE-DWDM 1558.98 nm X2 (100-GHz ITU grid)
DWDM-X2-59.79=	3.7	10GBASE-DWDM 1559.79 nm X2 (100-GHz ITU grid)
DWDM-X2-60.61=	3.7	10GBASE-DWDM 1560.61 nm X2 (100-GHz ITU grid)
GLC-BX-D	3.6.1[1]	1000BASE-BX10-D downstream bidirectional single fiber; with DOM
GLC-BX-U	3.6.1[2]	1000BASE-BX10-U upstream bidirectional single fiber; with DOM
GLC-LH-SM	3.6.1[3]	Gigabit Ethernet SFP, LC connector LH transceiver
GLC-SX-MM	3.6.1[4]	Gigabit Ethernet SFP, LC connector SX transceiver
GLC-T	3.6.1	Gigabit Ethernet SFP, RJ-45 connector, 1000BASE-T transceiver
GLC-ZX-SM	3.6.1[5]	Gigabit Ethernet SFP, LC connector ZX transceiver
PWR-C49M-1000AC	3.7	Cisco Catalyst 4900M AC Power Supply
PWR-C49M-1000DC	3.7	4900M DC power supply, 1000 watts module
WS-C4948	3.6.1	Catalyst 4000 series fixed configuration switch with 48 10/100/1000BaseT wirespeed ports and 4 1000BaseX SFP ports
WS-C4948-10GE	3.6.1	Catalyst 4000 series fixed configuration switch with 48 10/100/1000BaseT wirespeed ports and 2 10Gbps X2 ports
WS-X4904-10GE	3.7	Catalyst 4000 series fixed configuration switch with 48 10/100/1000BaseT wirespeed ports and 4 1000BaseX SFP ports
WS-X4908-10GE	3.7	Catalyst 4900M series, half height line card with 8 port 2:1 10GE interface
WS-X4908-10G-RJ45	3.7.1	4900M 8 port 10GBase-T (RJ-45) half card
WS-X4920-GB-RJ45	3.7	Catalyst 4900M series, half height line card with 20 port 10/100/1000 RJ45 interface

Table 7-41 Supported Modules for Cisco Catalyst 4900 Series—Cisco Prime Network 3.9

Module Name	Product_Version	Module Description
WS-X4992	3.7	Cisco Catalyst 4900M Spare Fan Tray
X2-10GB-CX4	3.6.1[6]	10GBASE-CX4 single-mode X2 module
X2-10GB-ER	3.6.1[7]	10GBASE-ER single-mode X2 module
X2-10GB-LR	3.6.1[8]	10GBASE-LR single-mode X2 module
X2-10GB-LRM	3.7	10GBASE-LX4 X2 transceiver module for MMF, 1310-nm wavelength, SC duplex connector
X2-10GB-LX4	3.6.1[9]	10GBASE-LX4 single-mode X2 module
X2-10GB-SR	3.6.1[10]	10GBASE-SR single-mode X2 module
X2-10GB-ZR	3.7	10GBASE-ZR X2 transceiver module for SMF, 1550-nm wavelength, SC duplex connector
X2-10GE-CX4	3.6.1	10GBASE-CX4 X2 Module
X2-10GE-ER	3.6.1	10GBASE-ER X2 Module
X2-10GE-LR	3.6.1	10GBASE-LR X2 Module
X2-10GE-LX4	3.6.1	10GBASE-LX4 X2 Module
X2-10GE-SR	3.6.1	10GBASE-SR X2 Module
WS-X4908-10G-RJ45	ANA-3.7.2-DP4[11]	Cisco Catalyst 4900M 8-port 10GBASE-T module (RJ45)
WS-X4612-SFP-E	ANA-3.7.2-DP4	Cisco Catalyst 4500E Series 12-port GE (SFP)
WS-X4712-SFP+E	ANA-3.7.2-DP4	Cisco Catalyst 4500E Series 12-port 10GE (SFP+)
WS-X4640-CSFP-E	ANA-3.7.2-DP4	10GBaseT(RJ45),1000BaseT(RJ45) with 8 10G RJ45 ports
WS-X45-SUP7-E	ANA-3.7.2-DP4	Cisco Catalyst 4500E Series Supervisor Engine 7-E
DWDM-SFP-5655	ANA-3.7.2-DP4	1000BASE-DWDM SFP 1556.55 nm
DWDM-SFP-5575	ANA-3.7.2-DP4	1000BASE-DWDM SFP 1555.75 nm
DWDM-SFP-5494	ANA-3.7.2-DP4	1000BASE-DWDM SFP 1554.94 nm
DWDM-SFP-5413	ANA-3.7.2-DP4	1000BASE-DWDM SFP 1554.13 nm
DWDM-SFP-5252	ANA-3.7.2-DP4	1000BASE-DWDM SFP 1552.52 nm
DWDM-SFP-5172	ANA-3.7.2-DP4	1000BASE-DWDM SFP 1551.72 nm
DWDM-SFP-5092	ANA-3.7.2-DP4	1000BASE-DWDM SFP 1550.92 nm

Table 7-41 Supported Modules for Cisco Catalyst 4900 Series—Cisco Prime Network 3.9

Module Name	Product_Version	Module Description
DWDM-SFP-5012	ANA-3.7.2-DP4	1000BASE-DWDM SFP 1550.12 nm
DWDM-SFP-4851	ANA-3.7.2-DP4	1000BASE-DWDM SFP 1548.51 nm
DWDM-SFP-4772	ANA-3.7.2-DP4	1000BASE-DWDM SFP 1547.72 nm
DWDM-SFP-4692	ANA-3.7.2-DP4	1000BASE-DWDM SFP 1546.92 nm
DWDM-SFP-4612	ANA-3.7.2-DP4	1000BASE-DWDM SFP 1546.12 nm
DWDM-SFP-4453	ANA-3.7.2-DP4	1000BASE-DWDM SFP 1544.53 nm
DWDM-SFP-4373	ANA-3.7.2-DP4	1000BASE-DWDM SFP 1543.73 nm
DWDM-SFP-4294	ANA-3.7.2-DP4	1000BASE-DWDM SFP 1542.94 nm
DWDM-SFP-4214	ANA-3.7.2-DP4	1000BASE-DWDM SFP 1542.14 nm
DWDM-SFP-4056	ANA-3.7.2-DP4	1000BASE-DWDM SFP 1540.56 nm
DWDM-SFP-3977	ANA-3.7.2-DP4	1000BASE-DWDM SFP 1539.77 nm
DWDM-SFP-3898	ANA-3.7.2-DP4	1000BASE-DWDM SFP 1538.98 nm
DWDM-SFP-3819	ANA-3.7.2-DP4	1000BASE-DWDM SFP 1538.19 nm
DWDM-SFP-3661	ANA-3.7.2-DP4	1000BASE-DWDM SFP 1536.61 nm
DWDM-SFP-3582	ANA-3.7.2-DP4	1000BASE-DWDM SFP 1535.82 nm
DWDM-SFP-3504	ANA-3.7.2-DP4	1000BASE-DWDM SFP 1535.04 nm
DWDM-SFP-3425	ANA-3.7.2-DP4	1000BASE-DWDM SFP 1534.25 nm
DWDM-SFP-3268	ANA-3.7.2-DP4	1000BASE-DWDM SFP 1532.68 nm
DWDM-SFP-3190	ANA-3.7.2-DP4	1000BASE-DWDM SFP 1531.90 nm
DWDM-SFP-3112	ANA-3.7.2-DP4	1000BASE-DWDM SFP 1531.12 nm

Table 7-41 Supported Modules for Cisco Catalyst 4900 Series—Cisco Prime Network 3.9

Module Name	Product_Version	Module Description
DWDM-SFP-3033	ANA-3.7.2-DP4	1000BASE-DWDM SFP 1530.33 nm
DWDM-SFP-6141	ANA-3.7.2-DP4	1000BASE-DWDM SFP 1561.41 nm
DWDM-SFP-5736	ANA-3.7.2-DP4	1000BASE-DWDM SFP 1557.36 nm
DWDM-SFP-5332	ANA-3.7.2-DP4	1000BASE-DWDM SFP 1553.32 nm
DWDM-SFP-4931	ANA-3.7.2-DP4	1000BASE-DWDM SFP 1549.31 nm
DWDM-SFP-4532	ANA-3.7.2-DP4	1000BASE-DWDM SFP 1545.32 nm
DWDM-SFP-4134	ANA-3.7.2-DP4	1000BASE-DWDM SFP 1541.34 nm
DWDM-SFP-3739	ANA-3.7.2-DP4	1000BASE-DWDM SFP 1537.39 nm
DWDM-SFP-3346	ANA-3.7.2-DP4	1000BASE-DWDM SFP 1533.46 nm

[1, 2, 3, 4, 5, 6, 7, 8, 9, 10]Support verified in ANA 3.7

[11]Support verified in ANA 3.7.2 DP4

Cisco Catalyst 4900 Series—Supported Technologies

The following technologies are supported by the Cisco Catalyst 4900 Series in Cisco Prime Network 3.9:

- IP, page 7-92
- Routing Protocols, page 7-96
- Ethernet, page 7-99
- VPN (VRF), page 7-120
- Security, page 7-122
- Hardware, page 7-124
- Serial, page 7-127
- Additional Technologies, page 7-128
- LLDP, page 7-131
- CDP, page 7-132
- Discovery Protocol, page 7-132

Cisco Catalyst 4900 Series—Supported Service Events

Table 7-42 Supported Service Events for Cisco Catalyst 4900 Series—Cisco Prime Network 3.9

Event Name	Product_Version	Expedited
Active ip interfaces found	3.6.1	N
All ip interfaces down	3.6.1	N
BGP link down due to admin	3.6.1	N
BGP link down due to oper	3.6.1	N
BGP link down vrf due to admin	3.6.1	N
BGP link down vrf due to oper	3.6.1	N
BGP link up	3.6.1	N
BGP neighbor found	3.6.1	N
BGP neighbor loss due to admin	3.6.1	N
BGP neighbor loss due to oper	3.6.1	N
BGP process down	3.6.1	N
BGP process up	3.6.1	N
Card down	3.6.1	N
Card in	3.6.1	N
Card out	3.6.1	N
Card up	3.6.1	N
Device Managed	3.6.1	N
Device Partially Managed	3.6.1	N
Device Unsupported	3.6.1	N
Discarded packet rate exceeded upper threshold	3.6.1	N
Discarded packet rate is below lower threshold	3.6.1	N
Dropped packet rate exceeded upper threshold	3.6.1	N
Dropped packet rate is below lower threshold	3.6.1	N
GRE tunnel down	3.6.1	N
GRE tunnel up	3.6.1	N
High priority member down	3.6.1	N
High Priority MPLS-TE tunnel down	3.6.1	N
keepalive configured	3.6.1	N
keepalive not configured	3.6.1	N
l2tp peer established	3.6.1	N

Table 7-42 Supported Service Events for Cisco Catalyst 4900 Series—Cisco Prime Network 3.9

Event Name	Product_Version	Expedited
l2tp peer is removed	3.6.1	N
l2tp peer not established	3.6.1	N
LAG down	3.6.1	N
LAG Link down	3.6.1	N
LAG Link up	3.6.1	N
LAG up	3.6.1	N
Layer 2 tunnel up	3.6.1	N
LDP neighbor down	3.6.1	N
LDP neighbor up	3.6.1	N
Link down due to admin down	3.6.1	N
Link down due to Card event	3.6.1	N
Link down due to oper down	3.6.1	N
Link down on unreachable	3.6.1	N
Link over utilized	3.6.1	N
Link up	3.6.1	N
Link utilization normal	3.6.1	N
Logical port down	3.6.1	N
Logical port up	3.6.1	N
Low priority member down	3.6.1	N
Low Priority MPLS-TE tunnel down	3.6.1	N
Management Unreachable	3.6.1	N
Medium priority member down	3.6.1	N
Medium Priority MPLS-TE tunnel down	3.6.1	N
Memory utilization exceeded upper threshold	3.6.1	N
Memory utilization less than lower threshold	3.6.1	N
Module Unsupported	3.6.1	N
MPLS interface added	3.6.1	N
MPLS interface removed	3.6.1	N
MPLS-TE tunnel up	3.6.1	N
OSPF Neighbor Down	3.6.1	N
OSPF Neighbor Up	3.6.1	N
Port down due to admin	3.6.1	N
Port down due to Card down	3.6.1	N

Table 7-42 Supported Service Events for Cisco Catalyst 4900 Series—Cisco Prime Network 3.9

Event Name	Product_Version	Expedited
Port down due to Card out	3.6.1	N
Port down due to oper	3.6.1	N
Port up	3.6.1	N
Primary HSRP interface active	3.6.1	N
Primary HSRP interface not active	3.6.1	N
rx dormant	3.6.1	N
rx dormant normal	3.6.1	N
Rx utilization exceeded upper threshold	3.6.1	N
Rx utilization is below lower threshold	3.6.1	N
Secondary HSRP interface active	3.6.1	N
Secondary HSRP interface not active	3.6.1	N
Service down	3.6.1	N
Service up	3.6.1	N
Shelf in	3.6.1	N
Shelf out	3.6.1	N
tx dormant	3.6.1	N
tx dormant normal	3.6.1	N
Tx utilization exceeded upper threshold	3.6.1	N
Tx utilization is below lower threshold	3.6.1	N
rep port role change	3.8.0	Y
pluggable transceiver out	3.8.0	N
fan-tray down	3.8.0	N
fan-tray out	3.8.0	N
power-supply down	3.8.0	N

Cisco ME 4900 Series Ethernet Switch

This section includes the following information about Cisco 4924 ME switches (for information on the NE types supported in Cisco Prime Network 3.9, see Cisco ME 4900 Series Ethernet Switch):

- Cisco 4924 ME—Supported Software Versions, page 7-44
- Cisco 4924 ME—Supported Topologies, page 7-44
- Cisco 4924 ME—Supported Modules, page 7-44
- Cisco 4924 ME—Supported Technologies, page 7-46

- Cisco 4924 ME—Supported Service Events, page 7-46

Cisco 4924 ME—Supported Software Versions

Table 7-43 Supported Software Versions for Cisco 4924 ME—Cisco Prime Network 3.9

Software Version	Product_Version
12.2(25)EWA	3.6.3[1]
12.2(25)EWA4	3.6.3[2]
12.2(25)EWA6	3.6.3[3]
12.2(31)SG	3.6.3[4]
12.2(31)SGA1	3.6.1[5]
12.2(46)SG	3.6.6[6]
12.2(50)SG	3.6.6[7]
12.2(53)SG	3.7[8]
12.2(53)SG2	3.7.1
12.2(53)SG3	ANA-3.7.2-DP1

[1, 2, 3, 4, 5, 6, 7, 8] ANA models pluggable ports for this IOS version.

Cisco 4924 ME—Supported Topologies

Table 7-44 Supported Topologies for Cisco 4924 ME—Cisco Prime Network 3.9

Topology Type	Link Type	Product_Version
Ethernet	Ethernet	3.6.1
Physical Layer	Physical Layer	3.6.1
LAG	LAG	Prime Network 3.8

Cisco 4924 ME—Supported Modules

Table 7-45 Supported Modules for Cisco 4924 ME—Cisco Prime Network 3.9

Module Name	Product_Version	Module Description
CAB-SM-LCSC-1M	3.6.1	1m fiber single-mode LC-to-SC connectors

Table 7-45 Supported Modules for Cisco 4924 ME—Cisco Prime Network 3.9 (continued)

Module Name	Product_Version	Module Description
CAB-SM-LCSC-5M	3.6.1	5m fiber single-mode LC-to-SC connectors
CSS5-CABLX-LCSC	3.6.1	Cisco CSS 11500 10m fiber single-mode LX LC-to-SC connectors
CSS5-CABSX-LC	3.6.1	Cisco CSS 11500 10m fiber multimode SX LC connectors
CSS5-CABSX-LCSC	3.6.1	Cisco CSS 11500 10m fiber multimode SX LC-to-SC connectors
CWDM-SFP-1470	3.6.1	Cisco CWDM SFP 1470 nm; Gigabit Ethernet and 1G/2G FC (gray)
CWDM-SFP-1490	3.6.1	Cisco CWDM SFP 1490 nm; Gigabit Ethernet and FC (violet)
CWDM-SFP-1510	3.6.1	Cisco CWDM SFP 1510 nm; Gigabit Ethernet and 1G/2G FC (blue)
CWDM-SFP-1530	3.6.1	Cisco CWDM SFP 1530 nm; Gigabit Ethernet and 1G/2G FC (green)
CWDM-SFP-1550	3.6.1	Cisco CWDM SFP 1550 nm; Gigabit Ethernet and 1G/2G FC (yellow)
CWDM-SFP-1570	3.6.1	Cisco CWDM SFP 1570 nm; Gigabit Ethernet and 1G/2G FC (orange)
CWDM-SFP-1590	3.6.1	Cisco CWDM SFP 1590 nm; Gigabit Ethernet and 1G/2G FC (red)
CWDM-SFP-1610	3.6.1	Cisco CWDM SFP 1610 nm; Gigabit Ethernet and 1G/2G FC (brown)
GLC-BX-D	3.6.1	1000BASE-BX10-D downstream bidirectional single fiber; with DOM
GLC-BX-U	3.6.1	1000BASE-BX10-U upstream bidirectional single fiber; with DOM
GLC-LH-SM	3.6.1	Gigabit Ethernet SFP, LC connector LH transceiver
GLC-SX-MM	3.6.1	Gigabit Ethernet SFP, LC connector SX transceiver
GLC-T	3.6.1	Gigabit Ethernet SFP, RJ-45 connector, 1000BASE-T transceiver
GLC-ZX-SM	3.6.1	Gigabit Ethernet SFP, LC connector ZX transceiver
ME-4924-10GE	3.6.1	Cisco ME 4924-10GE, IP Base software image (RIP, static routes), no power supply, fan tray
PWR-C49-300DC	3.6.6	Power Supply (DC 300W)
WS-X4991	3.6.6	Fan Tray
X2-10GE-CX4	3.6.1	10GBASE-CX4 X2 Module
X2-10GE-ER	3.6.1	10GBASE-ER X2 Module
X2-10GE-LR	3.6.1	10GBASE-LR X2 Module

Table 7-45 Supported Modules for Cisco 4924 ME—Cisco Prime Network 3.9 (continued)

Module Name	Product_Version	Module Description
X2-10GE-LX4	3.6.1	10GBASE-LX4 X2 Module
X2-10GE-SR	3.6.1	10GBASE-SR X2 Module

Cisco 4924 ME—Supported Technologies

The following technologies are supported by the Cisco 4924 ME in Cisco Prime Network 3.9:

- IP, page 7-92
- Routing Protocols, page 7-96
- Ethernet, page 7-99
- VPN (VRF), page 7-120
- Security, page 7-122
- Hardware, page 7-124
- Serial, page 7-127
- Additional Technologies, page 7-128
- LLDP, page 7-131
- CDP, page 7-132
- Discovery Protocol, page 7-132

Cisco 4924 ME—Supported Service Events

Table 7-46 Supported Service Events for Cisco 4924 ME—Cisco Prime Network 3.9

Event Name	Product_Version	Expedited
Active ip interfaces found	3.6.1	N
All ip interfaces down	3.6.1	N
BGP link down due to admin	3.6.1	N
BGP link down due to oper	3.6.1	N
BGP link down vrf due to admin	3.6.1	N
BGP link down vrf due to oper	3.6.1	N
BGP link up	3.6.1	N
BGP neighbor found	3.6.1	N
BGP neighbor loss due to admin	3.6.1	N
BGP neighbor loss due to oper	3.6.1	N
BGP process down	3.6.1	N
BGP process up	3.6.1	N

Table 7-46 Supported Service Events for Cisco 4924 ME—Cisco Prime Network 3.9 (continued)

Event Name	Product_Version	Expedited
Card down	3.6.1	N
Card in	3.6.1	N
Card out	3.6.1	N
Card up	3.6.1	N
Device Managed	3.6.1	N
Device Partially Managed	3.6.1	N
Device Unsupported	3.6.1	N
Discarded packet rate exceeded upper threshold	3.6.1	N
Discarded packet rate is below lower threshold	3.6.1	N
Dropped packet rate exceeded upper threshold	3.6.1	N
Dropped packet rate is below lower threshold	3.6.1	N
GRE tunnel down	3.6.1	N
GRE tunnel up	3.6.1	N
High priority member down	3.6.1	N
High Priority MPLS-TE tunnel down	3.6.1	N
keepalive configured	3.6.1	N
keepalive not configured	3.6.1	N
l2tp peer established	3.6.1	N
l2tp peer is removed	3.6.1	N
l2tp peer not established	3.6.1	N
LAG down	3.6.1	N
LAG Link down	3.6.1	N
LAG Link up	3.6.1	N
LAG up	3.6.1	N
Layer 2 tunnel up	3.6.1	N
LDP neighbor down	3.6.1	N
LDP neighbor up	3.6.1	N
Link down due to admin down	3.6.1	N
Link down due to Card event	3.6.1	N
Link down due to oper down	3.6.1	N
Link down on unreachable	3.6.1	N
Link over utilized	3.6.1	N

Table 7-46 Supported Service Events for Cisco 4924 ME—Cisco Prime Network 3.9 (continued)

Event Name	Product_Version	Expedited
Link up	3.6.1	N
Link utilization normal	3.6.1	N
Logical port down	3.6.1	N
Logical port up	3.6.1	N
Low priority member down	3.6.1	N
Low Priority MPLS-TE tunnel down	3.6.1	N
Management Unreachable	3.6.1	N
Medium priority member down	3.6.1	N
Medium Priority MPLS-TE tunnel down	3.6.1	N
Memory utilization exceeded upper threshold	3.6.1	N
Memory utilization less than lower threshold	3.6.1	N
Module Unsupported	3.6.1	N
MPLS interface added	3.6.1	N
MPLS interface removed	3.6.1	N
MPLS-TE tunnel up	3.6.1	N
OSPF Neighbor Down	3.6.1	N
OSPF Neighbor Up	3.6.1	N
Port down due to admin	3.6.1	N
Port down due to Card down	3.6.1	N
Port down due to Card out	3.6.1	N
Port down due to oper	3.6.1	N
Port up	3.6.1	N
Primary HSRP interface active	3.6.1	N
Primary HSRP interface not active	3.6.1	N
rx dormant	3.6.1	N
rx dormant normal	3.6.1	N
Rx utilization exceeded upper threshold	3.6.1	N
Rx utilization is below lower threshold	3.6.1	N
Secondary HSRP interface active	3.6.1	N
Secondary HSRP interface not active	3.6.1	N
Service down	3.6.1	N
Service up	3.6.1	N

Table 7-46 Supported Service Events for Cisco 4924 ME—Cisco Prime Network 3.9 (continued)

Event Name	Product_Version	Expedited
Shelf in	3.6.1	N
Shelf out	3.6.1	N
tx dormant	3.6.1	N
tx dormant normal	3.6.1	N
Tx utilization exceeded upper threshold	3.6.1	N
Tx utilization is below lower threshold	3.6.1	N
rep port role change	Prime Network 3.8	Y
pluggable transceiver out	Prime Network 3.8	N
fan-tray down	Prime Network 3.8	N
fan-tray out	Prime Network 3.8	N
power-supply down	Prime Network 3.8	N

Cisco Catalyst 5000 Series Switches

This section includes the following information about Cisco 5000 Series switches (for information on the NE types supported in Cisco Prime Network 3.9, see Cisco Catalyst 5000 Series Switches):

- Cisco 5000 Series—Supported Software Versions, page 7-50
- Cisco 5000 Series—Supported Topologies, page 7-50
- Cisco 5000 Series—Supported Technologies, page 7-50
- Cisco 5000 Series—Supported Service Events, page 7-50

Cisco 5000 Series—Supported Software Versions

Table 7-47 Supported Software Versions for Cisco 5000 Series—Cisco Prime Network 3.9

Software Version	Product_Version
4.5(15)	3.7

Cisco 5000 Series—Supported Topologies

Table 7-48 Supported Topologies for Cisco 5000 Series—Cisco Prime Network 3.9

Topology Type	Link Type	Product_Version
Business	Business	3.7
Ethernet	Ethernet	3.7
Physical Layer	Physical Layer	3.7

Cisco 5000 Series—Supported Technologies

The following technologies are supported by the Cisco 5000 Series in Cisco Prime Network 3.9:

- IP, page 7-92
- Ethernet, page 7-99
- Hardware, page 7-124
- Serial, page 7-127
- CDP, page 7-132
- Discovery Protocol, page 7-132

Cisco 5000 Series—Supported Service Events

Table 7-49 Supported Service Events for Cisco 5000 Series—Cisco Prime Network 3.9

Event Name	Product_Version	Expedited
Active IP Interfaces Found	3.7	Y
All IP Interfaces Down	3.7	Y
BGP process up	3.7	N
Card Down	3.7	Y
Card In	3.7	Y
Card Out	3.7	Y

Table 7-49 Supported Service Events for Cisco 5000 Series—Cisco Prime Network 3.9

Event Name	Product_Version	Expedited
Card Up	3.7	Y
CPU utilization exceeded upper threshold	3.7	N
Device Unsupported	3.7	N
Link up	3.7	N
Module Unsupported	3.7	N
rep port role change	Prime Network 3.8	Y
fan-tray down	Prime Network 3.8	N
fan-tray out	Prime Network 3.8	N
power-supply down	Prime Network 3.8	N

Cisco Catalyst 6500 Series (CatOS) Switches

This section includes the following information about Cisco Catalyst 6500 Series (CatOS) switches (for information on the NE types supported in Cisco Prime Network 3.9, see Cisco Catalyst 6500 Series (CatOS) Switches):

- Cisco Catalyst 6500 Series (CatOS)—Supported Software Versions, page 7-51
- Cisco Catalyst 6500 Series (CatOS)—Supported Topologies, page 7-52
- Cisco Catalyst 6500 Series (CatOS)—Supported Modules, page 7-52
- Cisco Catalyst 6500 Series (CatOS)—Supported Technologies, page 7-55
- Cisco Catalyst 6500 Series (CatOS)—Supported Service Events, page 7-55

Cisco Catalyst 6500 Series (CatOS)—Supported Software Versions

Table 7-50 Supported Software Versions for Cisco Catalyst 6500 Series (CatOS)—Cisco Prime Network 3.9

Software Version	Product_Version
6.4(10)	3.6.3
7.6(1)	3.6.3

Table 7-50 Supported Software Versions for Cisco Catalyst 6500 Series (CatOS)—Cisco Prime Network 3.9 (continued)

Software Version	Product_Version
7.6(8)	3.6.3
8.3(4)	3.6.3
8.4.1	3.6.3
8.5(1)	3.7[1]
8.5(7)	3.7

[1]ANA recognizes all maintenance builds in this CatOS release train.

Cisco Catalyst 6500 Series (CatOS)—Supported Topologies

Table 7-51 Supported Topologies for Cisco Catalyst 6500 Series (CatOS)—Cisco Prime Network 3.9

Topology Type	Link Type	Product_Version
Ethernet	Ethernet	3.6.0
Physical Layer	Physical Layer	3.6.0
LAG	LAG	3.6.2

Cisco Catalyst 6500 Series (CatOS)—Supported Modules

Table 7-52 Supported Modules for Cisco Catalyst 6500 Series (CatOS)—Cisco Prime Network 3.9

Module Name	Product_Version	Module Description
AIP	3.6.0	ATM Interface Processor
CAT6509	3.6.0	Catalyst 6500 Plus with 9 slots
CAT6K-MSFC	3.6.0	Multilevel Switching Feature Card for the Catalyst 6000 series
CAT6K-MSFC2	3.6.0	Multilevel Switching Feature Card Version 2 for the Catalyst 6000 series
CAT6K-WSF-6700-CFC	3.6.0	Catalyst 6500 centralized Forwarding Card
CAT6K-WSF-6K-DFC3A	3.6.0	Catalyst 6500 Distributed L3 switching engine IIIa
CAT6K-WSF-6K-PFC3A	3.6.0	Catalyst 6500 Centralized L3 switching engine IIIa
CAT6K-WSF-6K-VPWR-GE	3.6.0	Cat6k voice daughter cards
CAT6K-WS-SUP32-GE-3B	3.6.0	cat6k-ws-sup32-ge-3b
CAT6K-WS-SUP720	3.6.0	Catalyst 6500 Supervisor Module 720 CPU board

Table 7-52 Supported Modules for Cisco Catalyst 6500 Series (CatOS)—Cisco Prime Network 3.9

Module Name	Product_Version	Module Description
CAT6K-WS-SUP720-BASE	3.6.0	Catalyst 6500 Supervisor Module 720 base board
CAT6K-WS-SVC-IDSM2	3.6.0	Catalyst 6500 Intrusion Detection Module
CAT6K-WSX-6066-SLB-APC	3.6.0	Content Switching Module
CAT6K-WSX-6148-GE-TX	3.6.0	Catalyst 6000 48 port10/100/1000BaseT(RJ-45) module
CAT6K-WSX-6148-RJ45	3.6.0	48 port10/100BaseTX(RJ-45) module
CAT6K-WSX-6248A-RJ45	3.6.0	Catalyst 6000 48-port 10/100BaseTX RJ-45
CAT6K-WSX-6248-RJ45	3.6.0	Catalyst 6000 Family 48-port 10/100 RJ-45 module
CAT6K-WSX-6348-RJ45	3.6.0	48-port 10/100 ethernet module
CAT6K-WSX-6416-GBIC	3.6.0	16-port GBIC Gigabit ethernet module
CAT6K-WSX-6515-GETX	3.6.0	Catalyst 6500 16 port 10/100/1000BaseT (RJ-45) module
CAT6K-WSX-6516A-GBIC	3.6.0	Catalyst 6500 16 port 1000BaseX (GBIC)
CAT6K-WSX-6516-GBIC	3.6.0	Catalyst 6500 16 port 1000BaseX GBIC
CAT6K-WSX-6524-MMMT	3.6.0	Catalyst 6500 24 port 100BaseX MM (MT-RJ) module
CAT6K-WSX-6548-GETX	3.6.0	Catalyst 6500 48 port 10/100/1000 (RJ-45)
CAT6K-WSX-6548-RJ21	3.6.0	Catalyst 6500 48 port 10/100BaseTX (RJ-21)
CAT6K-WSX-6548-RJ45	3.6.0	48 port 10/100 Hydra2+/Hydra2V+
CAT6K-WSX-6704-10GE	3.6.0	Catalyst 6500 4 port 10 GE
CAT6K-WSX-6724-SFP	3.6.0	Catalyst 6500 24 port 1000Base FX (SFP GBIC)
CAT6K-WSX-6748-GETX	3.6.0	Catalyst 6500 48 port 10/100/1000 (RJ-45)
CAT6K-WSX-SUP1A-2GE	3.6.0	Catalyst 6500 2 port 1000BaseX Supervisor module (GBIC)
CAT6K-WSX-SUP2-2GE	3.6.0	Supervisor 2 with 2 Gigabit Ethernet ports
CATALYST 6500 FIREWALL MODULE	3.6.0	Catalyst 6500 Firewall Module
CEF720 48 PORT 1000MB SFP	3.6.0	Catalyst 6500 48 port 1000Base FX (SFP GBIC)
FSIP	3.6.0	Fast Serial Interface processor
HDV	3.6.0	High Density Voice module
MIP	3.6.0	MultiChanel Interface Processor
MSFC2A ROUTE ENGINE	3.6.0	MSFC2A Route Engine
OC192-POS-RPR1-SM-VSR-SPA	3.6.0	1 port OC-192c/STM-64 POS/RPR single mode very short reach Shared Port Adapter =SPA=
PA-1T3-PLUS	3.6.0	pa-1t3-plus
PA-2FEISL-TX	3.6.0	pa-2feisl-tx
PA-2T3-PLUS	3.6.0	pa-2t3-plus

Table 7-52 Supported Modules for Cisco Catalyst 6500 Series (CatOS)—Cisco Prime Network 3.9

Module Name	Product_Version	Module Description
PA-8CE1	3.6.0	pa-8ce1
PA-A4T	3.6.0	pa-a4t
PA-A8T-V35	3.6.0	pa-a8t-v35
PA-AH1T	3.6.0	pa-ah1t
PA-AH2T	3.6.0	pa-ah2t
PA-ATMDX-DS3	3.6.0	pa-atmdx-ds3
PA-ATMDX-E3	3.6.0	pa-atmdx-e3
PA-ATMDX-MM-OC3	3.6.0	pa-atmdx-mm-oc3
PA-ATMDX-SMI-OC3	3.6.0	pa-atmdx-smi-oc3
PA-ATMDX-SML-OC3	3.6.0	pa-atmdx-sml-oc3
PA-CE3	3.6.0	pa-ce3
PA-POSSW-LR	3.6.0	pa-possw-lr
PA-POSSW-MM	3.6.0	pa-possw-mm
PA-POSSW-SM	3.6.0	pa-possw-sm
PM-1FE-1T1	3.6.0	pm-1fe-1t1
POLICY FEATURE CARD 3	3.6.0	Policy Feature Card 3
POS-OC12-MM	3.6.0	pos-oc12-mm
RP	3.6.0	ROMmon Recovery Procedure
SPA-10X1GE	3.6.1	10-port Gigabit Ethernet SPA, SFP Optics
SPA-1XTENGE-XFP	3.6.1	1-port 10 Gigabit Ethernet SPA, LANPHY XFP Optics
SPA-2XOC3-ATM	3.6.1	2-port OC-3c/STM-1c ATM SPA
SPA-2XOC48POS/RPR	3.6.1	1-port 10 Gigabit Ethernet Shared Port Adapter XFP based
SPA-4XOC3-ATM	3.6.1	4-port OC-3c/STM-1c ATM SPA
TRIP	3.6.0	trip
VPN MODULE	3.6.0	VPN Module
VPN MODULE SUPPORTING 3DES	3.6.0	VPN Module supporting 3DES
WS-C6500-SFM	3.6.0	Switch Fabric Module
WS-C6509-NEB-A	3.6.1	Enhanced 9-slot vertically oriented chassis
WS-F6K-PWR	3.6.0	CATALYST 6000 INLINE POWER CARD, REF
WS-SUP720-3BXL	3.6.0	Catalyst 6500/Cisco 7600 Supervisor 720 Fabric MSFC3 PFC3BXL
WS-SVC-ADM-1-K9=	3.6.0	Catalyst 6500 Cisco Anomaly Detection Module
WS-SVC-AGM-1-K9=	3.6.0	Catalyst 6500 Cisco Anomaly Guard Module

Table 7-52 Supported Modules for Cisco Catalyst 6500 Series (CatOS)—Cisco Prime Network 3.9

Module Name	Product_Version	Module Description
WS-SVC-IDS2-BUN-K9	3.6.1	Cisco Catalyst 6500 Series Intrusion Detection System (IDSM-2) Service Module
WS-SVC-SSL-1-K9=	3.6.0	SSL Module for Catalyst 6500
WS-X6148-FE-SFP	3.6.0	Cisco Catalyst 6500 48-port 100BASE-X SFP Module
WSX-6408A-GBIC	3.6.0	Catalyst 6000 8-port Gigabit Ethernet Module
WSX-6408-GBIC	3.6.0	Card with 8 Gigabit Ethernet ports for the Catalyst 6000 series
WS-X6500-SFM2	3.6.0	Switch Fabric Module 2
WVIC-2DSU-T1(V2)	3.6.0	wvic-2dsu-t1(V2)

Cisco Catalyst 6500 Series (CatOS)—Supported Technologies

The following technologies are supported by the Cisco Catalyst 6500 Series (CatOS) in Cisco Prime Network 3.9:

- IP, page 7-92
- Ethernet, page 7-99
- Frame Relay, page 7-108
- PPP, page 7-110
- Hardware, page 7-124
- Serial, page 7-127
- CDP, page 7-132

Cisco Catalyst 6500 Series (CatOS)—Supported Service Events

Table 7-53 Supported Service Events for Cisco Catalyst 6500 Series (CatOS)—Cisco Prime Network 3.9

Event Name	Product_Version	Expedited
Active IP Interfaces Found	3.6.0	Y
All IP Interfaces Down	3.6.0	Y
BGP process up	3.6.0	N
Card Down	3.6.0	Y
Card In	3.6.0	Y
Card Out	3.6.0	Y
Card Up	3.6.0	Y

Table 7-53 Supported Service Events for Cisco Catalyst 6500 Series (CatOS)—Cisco Prime Network 3.9 (continued)

Event Name	Product_Version	Expedited
CPU utilization exceeded upper threshold	3.6.0	N
Device Unsupported	3.6.0	N
Link up	3.6.0	N
Memory utilization exceeded upper threshold	3.6.0	N
Module Unsupported	3.6.0	N
fan-tray down	Prime Network 3.8	N
fan-tray out	Prime Network 3.8	N
power-supply down	Prime Network 3.8	N

Cisco Catalyst 6500 Series (IOS) Switches

This section includes the following information about Cisco Catalyst 6500 Series (IOS) switches (for information on the NE types supported in Cisco Prime Network 3.9, see Cisco Catalyst 6500 Series (IOS) Switches):

- Cisco Catalyst 6500 Series (IOS)—Supported Software Versions, page 7-56
- Cisco Catalyst 6500 Series (IOS)—Supported Topologies, page 7-57
- Cisco Catalyst 6500 Series (IOS)—Supported Modules, page 7-58
- Cisco Catalyst 6500 Series (IOS)—Supported Technologies, page 7-65
- Cisco Catalyst 6500 Series (IOS)—Supported Service Events, page 7-66

Cisco Catalyst 6500 Series (IOS)—Supported Software Versions

Table 7-54 Supported Software Versions for Cisco Catalyst 6500 Series (IOS)—Cisco Prime Network 3.9

Software Version	Product_Version
IOS 12.1	3.6.1
IOS 12.1(13)E6	3.6.2
IOS 12.1(20)E3	3.6.2

Table 7-54 Supported Software Versions for Cisco Catalyst 6500 Series (IOS)—Cisco Prime Network 3.9 (continued)

Software Version	Product_Version
IOS 12.2	3.6.1[1]
IOS 12.2(17d)SXB	3.6.1
IOS 12.2(18)SXD2	3.6.2
IOS 12.2(18)SXD5	3.6.2
IOS 12.2(18)SXE	3.6.1[2]
IOS 12.2(18)SXF	3.6.1[3]
IOS 12.2(18)SXF7	3.6.2[4]
IOS 12.2(33)	3.6.1[5]
IOS 12.2(33)SRA	3.6.1[6]
IOS 12.2(33)SRA6	3.6.3[7]
IOS 12.2(33)SXH	3.6.3[8]
IOS 12.2(33)SXH1	3.6.3[9]
IOS 12.2(33)SXH2	3.6.6[10]
IOS 12.2(33)SXH2a	3.6.5[11]
IOS 12.2(33)SXI	3.6.4[12]
starts with 12.2(SIERRA)	3.6.1[13]
IOS 12.2(33)SXI5	ANA-3.7.2-DP3
IOS 12.2(33)SXI2a	ANA-3.7.2-DP3
IOS 12.2(33)SXH8	ANA-3.7.2-DP3
IOS 12.2(18)SXF17a	ANA-3.7.2-DP3
IOS 12.2(50)SY	ANA 3.7.x-DP08

[1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13] ANA models pluggable ports for this IOS version.

Cisco Catalyst 6500 Series (IOS)—Supported Topologies

Table 7-55 Supported Topologies for Cisco Catalyst 6500 Series (IOS)—Cisco Prime Network 3.9

Topology Type	Link Type	Product_Version
BGP	BGP	3.6.0
Ethernet	Ethernet	3.6.0

Table 7-55 Supported Topologies for Cisco Catalyst 6500 Series (IOS)—Cisco Prime Network 3.9

Topology Type	Link Type	Product_Version
MPLS	MPLS	3.6.0
PWE3 (Martini)	Tunnel	3.6.0
GRE Tunnel	GRE Tunnel	3.6.0
VPN (VRF)	VPN	3.6.0
Physical Layer	Physical Layer	3.6.0
LAG	LAG	3.6.0

Cisco Catalyst 6500 Series (IOS)—Supported Modules

Table 7-56 Supported Modules for Cisco Catalyst 6500 Series (IOS)—Cisco Prime Network 3.9

Module Name	Product_Version	Module Description
4000W-DC	3.6.2	4000W DC PS for 7609/7613Chassis
6000W-DC	3.6.2	6000W DC PS
7600-ES+40G3C	3.6.7	7600 ES+ Line Card, 40xGE SFP with DFC 3C
7600-ES20	3.6.1	Cisco 7600 Series Ethernet Services Card
7600-ES20-10G3C	3.6.1	Cisco 7600 ES20 line card, 2x10GE XFP with DFC 3C
7600-ES20-10G3CXL	3.6.1	Cisco 7600 ES20 line card, 2x10GE XFP with DFC 3CXL
7600-ES20-GE3C	3.6.1	Cisco 7600 ES20 line card, 20xGE SFP with DFC 3C
7600-ES20-GE3CXL	3.6.1	Cisco 7600 ES20 line card, 20xGE SFP with DFC 3CXL
7600-ES20-PROC	3.6.1	7600 ES20 PROC FRU
7600-ES40-G3CXL	3.6.4	7600 ES+ Line Card, 40xGE SFP with DFC 3CXL
7600-MSFC4	3.6.1	c7600 MSFC4 Daughterboard
7600-SIP-200	3.6.0	SPA Interface Processor-200
7600-SIP-400	3.6.0	SPA Interface Processor-400
7600-SIP-600	3.6.0	SPA Interface Processor-600
7600-SSC-400	3.6.3	Cisco 7600 / Catalyst 6500 Services SPA Carrier Card-400 Rev. 2.0
76-ES+T-20G	3.7.1	7600 ES+T Fixed 20x1G Low Queue Transport 3CXL
76-ES+T-2TG	3.7.1	7600 ES+T Fixed OTN/DWDM+FEC 2x10GE 3C XL Low Queue Transport 3CXL
76-ES+T-40G	3.7.1	7600 ES+T Fixed 40x1G Low Queue Transport 3CXL
76-ES+T-4TG	3.7.1	7600 ES+T Fixed OTN/DWDM+FEC 4x10GE 3C XL Low Queue Transport 3CXL

Table 7-56 Supported Modules for Cisco Catalyst 6500 Series (IOS)—Cisco Prime Network 3.9

Module Name	Product_Version	Module Description
76-ES+XC-20G3C	3.7	7600 ES+XC Combo 10x1GE/ 1x10GE, DFC3CXL
76-ES+XC-20G3CXL	3.7	7600 ES+XC Combo 10x1GE/ 1x10GE, DFC3CXL
76-ES+XC-40G3C	3.7	Combo 20x1GE/2x10GE - 3C
76-ES+XC-40G3CXL	3.7	Combo 20x1GE/2x10GE - 3CXL
ACE20-MOD-K9	3.6.3	Application Control Engine 20 Hardware
CAT6500FIREWALLSM	3.6.2	Cisco Catalyst 6500 Series Firewall Services Module
CAT6500SSLSM	3.6.2	Cisco Catalyst 6500 Series SSL Services Module
CEVFAN	3.6.1	Fan
DFC-3C	3.6.1	Distributed Forwarding Card 3C
FAN-MOD-09	3.6.4	Catalyst 6509-NEB-A Fan Tray
GLC_BX-U	3.6.7	1000BASE-BX10 SFP module for single-strand SMF, 1310-nm TX/1490-nm RX wavelength
GLC-BX-D	3.6.7	1000BASE-BX10 SFP module for single-strand SMF, 1490-nm TX/1310-nm RX wavelength
GLC-LH-SM	3.6.4	Short Wave fiber Gigabit Ethernet
MSFC4	3.6.2	Multilayer Switch Feature Card
OSM-12CT3T1	3.6.0	12-port channelized/unchannelized CT3-T1
OSM-1CHOC12T3-SI	3.6.0	1-port channelized OC-12, SM-IR
OSM-1OC48-POS-SI+	3.6.0	Enhanced 1-port OC-48/STM-16 SONET/SDH OSM, SM-IR
OSM-1OC48-POS-SL+	3.6.0	Enhanced 1-port OC-48/STM-16 SONET/SDH OSM, SM-LR
OSM-1OC48-POS-SS+	3.6.0	Enhanced 1-port OC-48/STM-16 SONET/SDH OSM, SM-SR
OSM-2+4GE-WAN+	3.6.0	4-port Gigabit Ethernet WAN (GBIC) with two Layer 2 LAN ports; CEF256
OSM-2OC12-ATM-MM+	3.6.0	Enhanced 2-port OC-12/STM-4 ATM OSM, MM
OSM-2OC12-ATM-SI+	3.6.0	Enhanced 2-port OC-12/STM-4 ATM OSM, SM-IR
OSM-2OC12-POS-SI+	3.6.0	Enhanced 2-port OC-12c/STM-4c POS, SM-IR; CEF256
OSM-4OC12-POS-SI+	3.6.0	Enhanced 4-port OC-12c/STM-4c POS, SM-IR; CEF256
OSM-4OC3-POS-SI+	3.6.0	Enhanced 4-port OC-3c/STM-1c POS, SM-IR;
PA-1FE-FX	3.6.0	1-port Fast Ethernet port adapter
PA-1FE-TX	3.6.0	1-port Fast Ethernet port adapter
PA-2CE/PRI	3.6.1	Not Found
PA-2FE-TX	3.6.0	2-port Fast Ethernet port adapter
PA-4T+	3.6.0	T1/E1 port adapters

Table 7-56 Supported Modules for Cisco Catalyst 6500 Series (IOS)—Cisco Prime Network 3.9

Module Name	Product_Version	Module Description
PA-A3-E3	3.6.0	ATM with traffic shaping port adapters
PA-A3-T3	3.6.0	ATM with traffic shaping port adapters
PA-MC-2E1/120	3.6.1	2 port multichannel E1 port adapter with G.703 120ohm interf
PA-MC-4T1	3.6.0	T1/E1 port adapters
PA-MC-8T1	3.6.0	T1/E1 port adapters
PA-MC-STM-1	3.6.0	Multichannel STM-1 port adapters
PA-MCX-8TE1	3.6.1	8 port multichannel T1/E1 8PRI port adapter
PA-POS-2OC3	3.6.0	2-port POS OC3c/STM1 port adapter
PFC-3C	3.6.2	Policy Feature Card 3C
PFC-3CXL	3.6.1	Policy Feature Card 3Cxl (PFC3CXL)
PWR-2700-AC/4	3.6.4	2700W AC power supply for Cisco Catalyst 6504-E
PWR-2700-DC/4	3.6.2	2700W DC Power Supply for Cisco 6504-E
PWR-4000-DC	3.6.4	Cisco 4000 Watt DC power supply for Catalyst 6000
RSP720-3C-10GE	3.7	Cisco 7600 Series RSP 720-10GE with 10 Gigabit Ethernet Uplinks that includes PFC-3C and Multilayer Switch Feature Card (MSFC4)
RSP720-3C-GE	3.6.1	Route Switch Processor 720 with PFC3C
RSP720-3CXL	3.6.4	Catalyst 6500 Supervisor Module 720 base board
RSP720-3CXL-10GE	3.7	Cisco 7600 Series RSP 720-10GE with 10 Gigabit Ethernet Uplinks that includes PFC-3CXL and Multilayer Switch Feature Card (MSFC4)
SFP-GE-L	3.6.4	1000BASE-LH/LX pluggable transceiver
SFP-GE-S	3.6.7	1000BASE-Sx Short wavelength gigabit ethernet SFP
SFP-GE-T	3.6.7	1000BASE-T Copper gigabit ethernet SFP
SFP-GE-Z	3.6.7	1000BASE-Zx Extended reach gigabit ethernet SFP
SFP-OC3-IR1	3.6.0	Intermediate range, single-mode fiber
SFP-OC3-LR1	3.6.0	Long range, single-mode fiber
SFP-OC3-MM	3.6.0	Short range, multimode fiber
SFP-OC3-SR	3.6.1	OC3/STM1 SFP, Single-mode fiber, Short Reach
SPA-10X1GE	3.6.0	10-port Gigabit Ethernet SPA, SFP Optics
SPA-10X1GE-V2	3.6.0	10-port Gigabit Ethernet SPA, SFP Optics
SPA-1XCHSTM1/OC3	3.6.0	1-port Channelized STM1/OC3 to DS0 SPA
SPA-1XOC12-ATM	3.6.0	1-Port OC-12c/STM-4c ATM SPA
SPA-1XOC12-POS	3.6.0	1-port OC-12c/STM-4c POS SPA
SPA-1XOC48-ATM	3.6.0	1 port OC-48c/STM-16 ATM SPA

Table 7-56 Supported Modules for Cisco Catalyst 6500 Series (IOS)—Cisco Prime Network 3.9

Module Name	Product_Version	Module Description
SPA-1XTENGE-XFP	3.6.0	1-port 10 Gigabit Ethernet SPA, LANPHY XFP Optics
SPA-24CHT1-CE-ATM	3.6.0	24-Port Channelized T1/E1/J1 ATM CEoP SPA
SPA-2X1GE	3.6.0	2-port Gigabit Ethernet SPA, SFP Optics
SPA-2X1GE-V2	3.6.0	2-port Gigabit Ethernet SPA, SFP Optics
SPA-2XCT3/DS0	3.6.0	2-port Channelized T3 to DS0 SPA
SPA-2XOC3-ATM	3.6.0	2-port OC-3c/STM-1c ATM SPA
SPA-2XOC3-POS	3.6.0	2-port OC-3c/STM-1c POS SPA
SPA-2XOC48POS/RPR	3.6.1	1-port 10 Gigabit Ethernet Shared Port Adapter XFP based
SPA-2XOC48POSRPR	3.6.0	2 port OC-48 POS/RPR SPA with SFP Optics
SPA-2XT3/E3	3.6.0	2-port Clear Channel T3/E3 SPA
SPA-4X1FE-TX-V2	3.6.0	4-port 10/100 Ethernet SPA TX
SPA-4XCT3/DS0	3.6.0	4-port Channelized T3 to DS0 SPA
SPA-4XOC3-ATM	3.6.0	4-port OC-3c/STM-1c ATM SPA
SPA-4XOC3-POS	3.6.0	4-port OC-3c/STM-1c POS SPA
SPA-4XOC48POSRPR	3.6.0	4-port OC-48c/STM-16 POS/DPT/RPR SPA
SPA-4XT3/E3	3.6.0	4-port Clear Channel T3/E3 SPA
SPA-5X1GE	3.6.0	5-port Gigabit Ethernet SPA, SFP Optics
SPA-5X1GE-V2	3.6.2	5-Port Gigabit Ethernet Shared Port Adapter
SPA-8X1FE-TX-V2	3.6.0	8-port 10/100 Ethernet SPA TX
SPA-8XCHT1E1	3.6.0	8-Port Channelized T1/E1 SPA
SPA-CHOC3-CE-ATM	3.6.2	1-port Channelized OC3/STM-1 ATM + Circuit Emulation Shared Port Adapter
SPA-OC192POS-LR	3.6.0	1-port OC-192c/STM-64 POS/RPR SPA, SM-LR
SPA-OC192POS-XFP	3.6.0	1-port OC-192c/STM-64 POS/RPR SPA, XFP Optics
VS-S720-10G-3C	3.6.1	Cisco Catalyst 6500 Series Virtual Switching Supervisor Engine 720 with two 10 Gigabit Ethernet ports and MSFC3 PFC3C
VS-S720-10G-3CXL	3.6.1	Cisco Catalyst 6500 Series Virtual Switching Supervisor Engine 720 with two 10 Gigabit Ethernet ports and MSFC3 PFC3C XL
WS-6700-DFC3B	3.6.1	Catalyst 6500 Distributed forwarding card 3B
WS-6700-DFC3BXL	3.6.1	Catalyst 6500 Distributed forwarding card 3B XL
WS-C6000-CL	3.7	Cisco Catalyst 6000 Clock FRU
WS-C6503-E-FAN	3.6.4	Catalyst 6503-E Chassis Fan Tray
WS-C6506-E-FAN	3.6.4	Catalyst 6506 - E chassis fan Tray

Table 7-56 Supported Modules for Cisco Catalyst 6500 Series (IOS)—Cisco Prime Network 3.9

Module Name	Product_Version	Module Description
WS-C6509-E-FAN	3.6.0	High-capacity fan tray
WS-C6509-NEB-A	3.6.1	Enhanced 9-slot vertically oriented chassis
WS-C6509-NEB-FAN	3.6.4	Catalyst 6509-NEB Fan Tray for 9-Vertical-Slot System
WS-C6509-V-E-FAN	3.6.4	Catalyst 6509-V-E Fan Tray
WS-C6513-CL	3.7	Cisco Clock Module WS-C6513-CL
WS-C6K-13SLT-FAN2	3.6.0	High Speed Fan Tray for Catalyst 6513 / Cisco 7613
WS-C6K-VTT	3.7	Catalyst 6000 VTT Module
WS-CAC-2500W	3.6.4	Catalyst 6500 2500W AC power supply
WS-CAC-3000W	3.6.4	Catalyst 6500 3000W AC power supply
WS-CAC-4000W-INT	3.6.3	4000W AC PowerSupply, International (cable included)
WS-CAC-6000W	3.6.0	6000W AC power supply
WS-CDC-2500W	3.6.4	Cisco 2500 Watt DC power supply for Catalyst 6000 or 8500 series
WS-F6700-DFC3A	3.6.1	Distributed Forwarding Card 3
WS-F6700-DFC3BXL	3.6.0	Distributed Forwarding Card 3BXL (DFC3BXL) for use on CEF720 modules
WS-F6700-DFC3C	3.6.0	Distributed Forwarding Card 3C (DFC3C) for use on CEF720 modules
WS-F6700-DFC3CXL	3.6.0	Distributed Forwarding Card 3CXL (DFC3CXL) for use on CEF720 modules
WS-F6K-FE48X2-AF	3.6.0	IEEE 802.3af PoE daughter card
WS-F6K-GE48-AF	3.6.0	IEEE 802.3af PoE daughter card
WS-F6K-MSFC2	3.6.1	Multilevel Switching Feature Card Version 2 for Catalyst 6000 that is treated as a standalone system by the NMS
WS-F6K-PFC2	3.6.1	Catalyst 6500 L3 switching engine II
WS-F6K-PFC3BXL	3.6.0	Policy Feature Card 3BXL (PFC3BXL)
WS-F6K-PFC3CXL	3.6.0	Policy Feature Card 3CXL (PFC3CXL)
WS-F6K-VPWR	3.6.0	PoE Daughter card
WS-F6K-VPWR-GE	3.6.0	PoE Daughter card
WS-G5486	3.6.4	Long Haul fiber Gigabit Ethernet
WS-G6483	3.6.0	10GBASE-ER serial 1550 nm extended-reach OIM
WS-G6488	3.6.0	10GBASE-LR serial 1310 nm long-reach OIM
WS-SUP32-10GE-3B	3.6.0	Supervisor Engine 32
WS-SUP32-GE-3B	3.6.0	Supervisor Engine 32
WS-SUP720-3B	3.6.0	Supervisor Engine 720 with PFC3B

Table 7-56 Supported Modules for Cisco Catalyst 6500 Series (IOS)—Cisco Prime Network 3.9

Module Name	Product_Version	Module Description
WS-SUP720-3BXL	3.6.0	Supervisor Engine 720 with PFC3BXL
WS-SVC-FWM-1	3.6.0	Catalyst 6500 Firewall Module
WS-SVC-IDS2-BUN-K9	3.6.1	Cisco Catalyst 6500 Series Intrusion Detection System (IDSM-2) Service Module
WS-SVC-IDSM-2	3.6.1	Catalyst 6500 Intrusion Detection Module
WS-SVC-MWAM-1	3.6.0	Multi-Processor WAN Application Module
WS-SVC-NAM-1	3.6.0	Network Analysis module 1
WS-SVC-NAM-2	3.6.0	Network Analysis module 2
WS-X6148A-GE-TX	3.6.0	48 port 10/100/1000 RJ-45 Ethernet Switching Module
WS-X6148A-RJ-45	3.6.0	48 port 10/100TX RJ-45 Ethernet/Fast Ethernet Switching Module
WS-X6148FE-SFP	3.6.1	Catalyst 6500 48 port 100Base-X SFP module
WS-X6148-FE-SFP	3.6.0	48 port 100BASE-FX Fast Ethernet Switching Module
WS-X6148-GE-TX	3.6.0	48 port 10/100/1000 RJ-45 Ethernet Switching Module
WS-X6148-RJ-21	3.6.0	48 port 10/100TX RJ-21 Ethernet/Fast Ethernet Switching Module
WS-X6148-RJ-45	3.6.0	48 port 10/100TX RJ-45 Ethernet/Fast Ethernet Switching Module
WS-X6148X2-RJ-45	3.6.0	96 port 10/100TX RJ-45 Ethernet/Fast Ethernet Switching Module
WS-X6196-RJ-21	3.6.0	96 port 10/100TX RJ-21 Ethernet/Fast Ethernet Switching Module
WS-X6248A-TEL	3.6.0	48 port 10/100TX RJ-21 Enhanced Ethernet/Fast Ethernet Switching Module
WS-X6248-RJ-45	3.6.0	48 port 10/100TX RJ-45 Ethernet/Fast Ethernet Switching Module
WS-X6248-TEL	3.6.0	48 port 10/100TX RJ-21 Ethernet/Fast Ethernet Switching Module
WS-X6316-GE-TX	3.6.0	16-port Gigabit Ethernet RJ-45
WS-X6324-100FX-SM	3.6.0	24 port 100FX Single Mode Fast Ethernet Switching Module
WS-X6348-RJ-21	3.6.0	6500 48 port 10/100BaseTX (RJ-21)
WS-X6348-RJ-45	3.6.0	48 port 10/100TX RJ-45 Ethernet/Fast Ethernet Switching Module
WS-X6408A-GBIC	3.6.0	8-port Gigabit Ethernet GBIC Enhanced QoS Module
WS-X6408-GBIC	3.6.0	8-port Gigabit Ethernet GBIC

Table 7-56 Supported Modules for Cisco Catalyst 6500 Series (IOS)—Cisco Prime Network 3.9

Module Name	Product_Version	Module Description
WS-X6416-GBIC	3.6.0	16-port Gigabit Ethernet GBIC
WS-X6502-10GE	3.6.0	1-port 10-Gigabit Ethernet
WS-X6516A-GBIC	3.6.0	16-port Gigabit Ethernet GBIC
WS-X6516-GBIC	3.6.0	16-port Gigabit Ethernet GBIC
WS-X6516-GE-TX	3.6.0	16 port 10/100/1000 Base-T Ethernet Switching Module
WS-X6548-GE-TX	3.6.0	48 port 10/100/1000 RJ-45 Ethernet Switching Module
WS-X6548-RJ-21	3.6.0	48 port 10/100TX RJ-21 Ethernet/Fast Ethernet Switching Module
WS-X6548-RJ-45	3.6.0	48 port 10/100TX RJ-45 Ethernet/Fast Ethernet Switching Module
WS-X6582-2PA	3.6.0	Enhanced FlexWAN Module;
WS-X6700-CFC	3.6.0	Centralized Forwarding Card
WS-X6704-10GE	3.6.0	4-port 10-Gigabit Ethernet
WS-X6708-10G-3C	3.6.1	C6K 8 port 10 Gigabit Ethernet module with DFC3C (req. X2)
WS-X6708-10GE	3.6.3	C6K 8 port 10 Gigabit Ethernet module with DFC
WS-X6724-SFP	3.6.0	24-port Gigabit Ethernet SFP
WS-X6748-GE-TX	3.6.0	48 port 10/100/1000 RJ-45 Ethernet Switching Module
WS-X6748-SFP	3.6.0	48-port Gigabit Ethernet SFP
WS-X6816-GBIC	3.6.0	16-port Gigabit Ethernet GBIC
WS-X6K-S1A-MSFC2	3.6.1	Catalyst 6000 Supervisor Engine 1A, 2 Gigabit Ethernet, plus MSFC2 and policy feature card (PFC)
WS-X6K-S2-MSFC2	3.6.1	Catalyst 6500 Supervisor Engine-2, 2GE, plus MSFC-2 / PFC-2
WS-X6K-SUP2-2GE	3.6.1	Supervisor 2 with 2 Gigabit Ethernet ports
X2-10GB-SR	3.6.5	10GBASE-SR Serial 850-nm short-reach multimode (MMF)
XENPAK-10GB-ER	3.6.0	10GBASE-ER Serial 1550-nm extended-reach, single-mode fiber (SMF), dispersion-shifted fiber (DSF)
XENPAK-10GB-LR	3.6.4	10 Gigabit Ethernet Serial 1310nm Laser Xenpak Module
XENPAK-10GB-SR	3.6.0	10GBASE-SR Serial 850-nm short-reach multimode fiber (MMF)
XFP-10GLR-OC192SR	3.6.4	OC192 XFP Single Mode Long Reach 2 (80km).

Table 7-56 Supported Modules for Cisco Catalyst 6500 Series (IOS)—Cisco Prime Network 3.9

Module Name	Product_Version	Module Description
WS-SVC-NAM-2-250S	ANA 3.7.x-DP08	WS-SVC-NAM-2-250S 8 ports Network Analysis Module Rev. 0.102
WS-SVC-WISM-1-K9	ANA 3.7.x-DP08	WS-SVC-WISM-1-K9 10 ports WiSM WLAN Service Module Rev. 2.4
WS-X6848-SFP-2T/2TXL	ANA 3.7.x-DP09	WS-X6848-SFP CEF720 48 port 1000mb SFP Rev. 1.0
WS-F6K-DFC4-AXL	ANA 3.7.x-DP09	WS-F6K-DFC4-AXL EARL8 Distributed Forwarding Card Rev. 1.0
WS-X6908-10GE-S	ANA 3.7.x-DP07	WS-X6908-10GE-S CEF720 8 port 10GE Rev. 0.560
VS-SUP2T-10G	ANA 3.7.x-DP07	VS-SUP2T-10G 5 ports Supervisor Engine 2T 10GE w/ CTS Rev. 0.530
WS-C6513-E FAN	ANA 3.7.x-DP07	Enhanced 13-slot Fan Tray 1

Cisco Catalyst 6500 Series (IOS)—Supported Technologies

The following technologies are supported by the Cisco Catalyst 6500 Series (IOS) in Cisco Prime Network 3.9:

- IP, page 7-92
- Routing Protocols, page 7-96
- Ethernet, page 7-99
- ATM, page 7-105
- HDLC, page 7-111
- SONET/SDH, page 7-111
- TDM/DSx, page 7-112
- MPLS, page 7-116
- MPLS-TE, page 7-118
- VPN (VRF), page 7-120
- PWE3, page 7-121
- Security, page 7-122
- Hardware, page 7-124

- Serial, page 7-127
- Additional Technologies, page 7-128
- LocalSwitching, page 7-128
- BFD, page 7-129
- Carrier Ethernet, page 7-129
- CDP, page 7-132
- Discovery Protocol, page 7-132
- Ethernet OAM, page 7-133

Cisco Catalyst 6500 Series (IOS)—Supported Service Events

Table 7-57 Supported Service Events for Cisco Catalyst 6500 Series (IOS)—Cisco Prime Network 3.9

Event Name	Product_Version	Expedited
Active ip interfaces found	3.6.0	N
All ip interfaces down	3.6.0	N
BGP link down due to admin	3.6.0	N
BGP link down due to oper	3.6.0	N
BGP link down vrf due to admin	3.6.0	N
BGP link down vrf due to oper	3.6.0	N
BGP link up	3.6.0	N
BGP neighbor found	3.6.0	N
BGP neighbor loss due to admin	3.6.0	N
BGP neighbor loss due to oper	3.6.0	N
BGP neighbor loss VRF due to admin	3.6.0	N
BGP neighbor loss VRF due to oper	3.6.0	N
BGP process up	3.6.0	N
Card down	3.6.0	N
Card in	3.6.0	N
Card out	3.6.0	N
Card up	3.6.0	N
CPU utilization exceeded upper threshold	3.6.0	N
CPU utilization less than lower threshold	3.6.0	N
Device Managed	3.6.0	N
Device Partially Managed	3.6.0	N
Device Unsupported	3.6.0	N

Table 7-57 Supported Service Events for Cisco Catalyst 6500 Series (IOS)—Cisco Prime Network 3.9 (continued)

Event Name	Product_Version	Expedited
Discarded packet rate exceeded upper threshold	3.6.0	N
Discarded packet rate is below lower threshold	3.6.0	N
Dropped packet rate exceeded upper threshold	3.6.0	N
Dropped packet rate is below lower threshold	3.6.0	N
Dual stack IP added	3.6.0	N
Dual stack IP removed	3.6.0	N
High priority member down	3.6.0	N
High Priority MPLS-TE tunnel down	3.6.0	N
Interface status down	3.6.0	N
Interface status up	3.6.0	N
keepalive configured	3.6.0	N
keepalive not configured	3.6.0	N
l2tp peer established	3.6.0	N
l2tp peer is removed	3.6.0	N
LAG down	3.6.0	N
LAG Link down	3.6.0	N
LAG Link up	3.6.0	N
LAG up	3.6.0	N
Layer 2 tunnel up	3.6.0	N
LDP neighbor down	3.6.0	N
LDP neighbor up	3.6.0	N
Link down due to admin down	3.6.0	N
Link down due to Card event	3.6.0	N
Link down due to oper down	3.6.0	N
Link down on unreachable	3.6.0	N
Link over utilized	3.6.0	N
Link up	3.6.0	N
Link utilization normal	3.6.0	N
Logical port up	3.6.0	N
Low priority member down	3.6.0	N
Low Priority MPLS-TE tunnel down	3.6.0	N
Management Unreachable	3.6.0	N

Table 7-57 Supported Service Events for Cisco Catalyst 6500 Series (IOS)—Cisco Prime Network 3.9 (continued)

Event Name	Product_Version	Expedited
Medium priority member down	3.6.0	N
Medium Priority MPLS-TE tunnel down	3.6.0	N
Memory utilization exceeded upper threshold	3.6.0	N
Memory utilization less than lower threshold	3.6.0	N
Module Unsupported	3.6.0	N
MPLS Black hole cleared	3.6.0	N
MPLS Black hole found	3.6.0	N
MPLS interface added	3.6.0	N
MPLS interface removed	3.6.0	Y
MPLS TE FRR State Changed to Active	3.6.0	N
MPLS TE FRR State Changed to Ready	3.6.0	N
MPLS-TE tunnel down	3.6.0	N
MPLS-TE tunnel up	3.6.0	N
OSPF Neighbor Down	3.6.0	N
OSPF Neighbor Up	3.6.0	N
Port down due to admin	3.6.0	N
Port down due to Card down	3.6.0	N
Port down due to Card out	3.6.0	N
Port down due to oper	3.6.0	N
Port up	3.6.0	N
Primary HSRP interface active	3.6.0	N
Primary HSRP interface not active	3.6.0	N
rx dormant normal	3.6.0	N
Rx utilization exceeded upper threshold	3.6.0	N
Rx utilization is below lower threshold	3.6.0	N
Secondary HSRP interface active	3.6.0	N
Secondary HSRP interface not active	3.6.0	N
Service down	3.6.0	N
Service up	3.6.0	N
Shelf in	3.6.0	N

Table 7-57 Supported Service Events for Cisco Catalyst 6500 Series (IOS)—Cisco Prime Network 3.9 (continued)

Event Name	Product_Version	Expedited
Shelf out	3.6.7	N
SONET Path down due to Admin	3.6.0	N
SONET Path down due to Card	3.6.0	N
SONET Path down due to Oper	3.6.0	N
SONET Path Link down due to Card event	3.6.0	N
SONET Path Link down on unreachable	3.6.0	N
tx dormant normal	3.6.0	N
Tx utilization exceeded upper threshold	3.6.0	N
Tx utilization is below lower threshold	3.6.0	N
rep port role change	Prime Network 3.8	Y
pluggable transceiver out	Prime Network 3.8	N
fan-tray down	Prime Network 3.8	N
fan-tray out	Prime Network 3.8	N
power-supply down	Prime Network 3.8	N

Cisco ME 6500 Series Ethernet Switches (6524)

This section includes the following information about Cisco ME 6500 Series (6524) switches (for information on the NE types supported in Cisco Prime Network 3.9, see Cisco ME 6500 Series Ethernet Switches (6524)):

- Cisco ME 6500 Series (6524)—Supported Software Versions, page 7-70
- Cisco ME 6500 Series (6524)—Supported Topologies, page 7-70
- Cisco ME 6500 Series (6524)—Supported Modules, page 7-70
- Cisco ME 6500 Series (6524)—Supported Technologies, page 7-71
- Cisco ME 6500 Series (6524)—Supported Service Events, page 7-71

Cisco ME 6500 Series (6524)—Supported Software Versions

Table 7-58 Supported Software Versions for Cisco ME 6500 Series (6524)—Cisco Prime Network 3.9

Software Version	Product_Version
12.2	3.6.0
12.2(18)ZU	3.6.0[1]
12.2(18)ZU1	3.6.0[2]
12.2(18)ZU2	3.6.0[3]
12.2(33)SXI	3.7[4]

[1, 2, 3, 4]ANA models pluggable ports for this IOS version.

Cisco ME 6500 Series (6524)—Supported Topologies

Table 7-59 Supported Topologies for Cisco ME 6500 Series (6524)—Cisco Prime Network 3.9

Topology Type	Link Type	Product_Version
ATM	ATM	3.6.0
BGP	BGP	3.6.0
Ethernet	Ethernet	3.6.0
MPLS	MPLS	3.6.0
VPN (VRF)	VPN	3.6.0
Physical Layer	Physical Layer	3.6.0
LAG	LAG	3.6.2

Cisco ME 6500 Series (6524)—Supported Modules

Table 7-60 Supported Modules for Cisco ME 6500 Series (6524)—Cisco Prime Network 3.9

Module Name	Product_Version	Module Description
ME-C6524GT-8S	3.6.0	32 ports Cisco ME 6524 Ethernet Switch Rev. 1.1
WS-6148A-GE-TX	3.6.0	Catalyst 6500 48 port 10/100/1000BaseTX (RJ-45) module
WS-6148-GE-TX	3.6.0	Catalyst 6000 48 port10/100/1000BaseT(RJ-45) module

Cisco ME 6500 Series (6524)—Supported Technologies

The following technologies are supported by the Cisco ME 6500 Series (6524) in Cisco Prime Network 3.9:

- IP, page 7-92
- Routing Protocols, page 7-96
- Ethernet, page 7-99
- MPLS, page 7-116
- MPLS-TE, page 7-118
- VPN (VRF), page 7-120
- PWE3, page 7-121
- Security, page 7-122
- Hardware, page 7-124
- Serial, page 7-127
- Additional Technologies, page 7-128
- Carrier Ethernet, page 7-129
- LLDP, page 7-131
- CDP, page 7-132
- Discovery Protocol, page 7-132
- Ethernet OAM, page 7-133

Cisco ME 6500 Series (6524)—Supported Service Events

Table 7-61 Supported Service Events for Cisco ME 6500 Series (6524)—Cisco Prime Network 3.9

Event Name	Product_Version	Expedited
Active IP Interfaces Found	3.6.0	Y
All IP Interfaces Down	3.6.0	Y
BGP process up	3.6.0	N
Card Down	3.6.0	Y
Card In	3.6.0	Y
Card Out	3.6.0	Y
Card Up	3.6.0	Y
CPU utilization exceeded upper threshold	3.6.0	N
Device Unsupported	3.6.0	N
Link up	3.6.0	N
Memory utilization exceeded upper threshold	3.6.0	N

Table 7-61 Supported Service Events for Cisco ME 6500 Series (6524)—Cisco Prime Network 3.9

Event Name	Product_Version	Expedited
Module Unsupported	3.6.0	N
rep port role change	3.8.0	Y
pluggable transceiver out	3.8.0	N
fan-tray down	3.8.0	N
fan-tray out	3.8.0	N
power-supply down	3.8.0	N

Cisco ME 3600X Ethernet Access Switch

This section includes the following information about Cisco ME 3600X switches (for information on the NE types supported in Cisco Prime Network 3.9, see Cisco ME 3600X Ethernet Access Switch):

- Cisco ME 3600X—Supported Software Versions, page 7-72
- Cisco ME 3600X—Supported Topologies, page 7-72
- Cisco ME 3600X—Supported Modules, page 7-73
- Cisco ME 3600X—Supported Technologies, page 7-74
- Cisco ME 3600X—Supported Service Events, page 7-74

Cisco ME 3600X—Supported Software Versions

Table 7-62 Supported Software Versions for Cisco ME 3600X—Cisco Prime Network 3.9

Software Version	Product_Version
IOS 12.2(52)SE	3.7.1
IOS 12.2(52)EY	3.7.1.0.4
IOS 12.2(52)EY1	3.7.2-DP-3.0
IOS 12.2(52)EY2	3.7.X-DP-4.0
IOS 15.1(2)EY	3.7.X-DP-6.0
IOS 12.2(52)EY3	3.7.X-DP-9.0

Cisco ME 3600X—Supported Topologies

Table 7-63 Supported Topologies for Cisco ME 3600X—Cisco Prime Network 3.9

Topology Type	Link Type	Product_Version
BGP	BGP	3.7.1

Table 7-63 Supported Topologies for Cisco ME 3600X—Cisco Prime Network 3.9 (continued)

Topology Type	Link Type	Product_Version
Ethernet	Ethernet	3.7.1
MPLS	MPLS	3.7.1
Physical Layer	Physical Layer	3.7.1

Cisco ME 3600X—Supported Modules

Table 7-64 Supported Modules for Cisco ME 3600X—Cisco Prime Network 3.9

Module Name	Product_Version	Module Description
CWDM-SFP-1470	3.7.1	1470nm color coded CWDM SFP
CWDM-SFP-1490	3.7.1	1490nm color coded CWDM SFP
CWDM-SFP-1510	3.7.1	1510nm color coded CWDM SFP
CWDM-SFP-1530	3.7.1	1530nm color coded CWDM SFP
CWDM-SFP-1550	3.7.1	1550nm color coded CWDM SFP
CWDM-SFP-1570	3.7.1	1570nm color coded CWDM SFP
CWDM-SFP-1590	3.7.1	1590nm color coded CWDM SFP
CWDM-SFP-1610	3.7.1	1610nm color coded CWDM SFP
GLC-BX-D	3.7.1	1000BASE-BX10-D downstream bidirectional single fiber SFP
GLC-BX-U	3.7.1	1000BASE-BX10-U upstream bidirectional single fiber SFP
GLC-FE-100BX-D	3.7.1	Fiber Fast Ethernet bi-directional 10kmDownlink over SMF
GLC-FE-100BX-U	3.7.1	Fiber Fast Ethernet bi-directional 10km Uplinkover SMF
GLC-FE-100EX	3.7.1	100 BaseEX Fiber FastEthernet
GLC-FE-100FX	3.7.1	Short Wave Fiber Fast Ethernet
GLC-FE-100LX	3.7.1	Long Wave Fiber Fast Ethernet 10km over SMF
GLC-LH-SM	3.7.1	Longwavelength gigabit ethernet SFP
GLC-SX-MM	3.7.1	Shortwavelength gigabit ethernet SFP
GLC-T	3.7.1	Copper gigabit ethernet SFP
GLC-ZX-SM	3.7.1	Extended reach gigabit ethernet
ME-FANTRAY	3.7.1	Metro Ethernet 3600X/3800X Fan Tray
PWR-390W-AC	3.7.1	Metro Ethernet 3600X/3800X AC power supply
PWR-390W-DC	3.7.1	Metro Ethernet 3600X/3800X DC power supply
SFP-10G-LR	3.7.1	10Gigabit XFP Multi Mode Long Reach

Table 7-64 Supported Modules for Cisco ME 3600X—Cisco Prime Network 3.9 (continued)

Module Name	Product_Version	Module Description
SFP-10G-LRM	3.7.1	10GBASE-LRM SFP+ transceiver module for MMF and SMF, 1310-nm wavelength, LC duplex connector
SFP-10G-SR	3.7.1	10Gigabit XFP Multi Mode Short Reach
SFP-GE-L	3.7.1	1000BASE-LH/LX pluggable transceiver
SFP-GE-S	3.7.1	1000BASE-Sx Short wavelength gigabit ethernet SFP.

Cisco ME 3600X—Supported Technologies

The following technologies are supported by the Cisco ME 3600X in Cisco Prime Network 3.9:

- IP, page 7-92
- Routing Protocols, page 7-96
- Ethernet, page 7-99
- TDM/DSx, page 7-112
- MPLS, page 7-116
- MPLS-TE, page 7-118
- VPN (VRF), page 7-120
- PWE3, page 7-121
- Security, page 7-122
- Hardware, page 7-124
- LocalSwitching, page 7-128
- BFD, page 7-129
- Carrier Ethernet, page 7-129
- LLDP, page 7-131
- CDP, page 7-132
- Discovery Protocol, page 7-132
- Ethernet OAM, page 7-133

Cisco ME 3600X—Supported Service Events

Table 7-65 Supported Service Events for Cisco ME 3600X—Cisco Prime Network 3.9

Event Name	Product_Version	Expedited
Active IP Interfaces Found	3.7.1	Y
All IP Interfaces Down	3.7.1	Y

Table 7-65 Supported Service Events for Cisco ME 3600X—Cisco Prime Network 3.9 (continued)

Event Name	Product_Version	Expedited
BGP process up	3.7.1	N
Card Down	3.7.1	Y
Card Up	3.7.1	Y
CPU utilization exceeded upper threshold	3.7.1	N
Device Unsupported	3.7.1	N
Keepalive configured	3.7.1	N
Keepalive not configured	3.7.1	N
Layer 2 Tunnel Down	3.7.1	N
Link up	3.7.1	N
Memory utilization exceeded upper threshold	3.7.1	N
Module Unsupported	3.7.1	N
MPLS Black Hole found	3.7.1	N
Pluggable transceiver out	Prime Network 3.8	N
Port up	Prime Network 3.8	Y

Cisco ME 3800X Carrier Ethernet Switches

This section includes the following information about Cisco ME 3800X switches (for information on the NE types supported in Cisco Prime Network 3.9, see Cisco ME 3800X Carrier Ethernet Switches):

- Cisco ME 3800X—Supported Software Versions, page 7-75
- Cisco ME 3800X—Supported Topologies, page 7-76
- Cisco ME 3800X—Supported Modules, page 7-76
- Cisco ME 3800X—Supported Technologies, page 7-77
- Cisco ME 3800X—Supported Service Events, page 7-78

Cisco ME 3800X—Supported Software Versions

Table 7-66 Supported Software Versions for Cisco ME 3800X—Cisco Prime Network 3.9

Software Version	Product_Version
IOS 12.2(52)SE	3.7.1

Table 7-66 Supported Software Versions for Cisco ME 3800X—Cisco Prime Network 3.9

Software Version	Product_Version
IOS 12.2(52)EY	3.7.1.0.4
IOS 12.2(52)EY1	3.7.2-DP-3.0
IOS 12.2(52)EY2	3.7.X-DP-4.0
IOS 15.1(2)EY	3.7.X-DP-6.0
IOS 12.2(52)EY3	3.7.X-DP-9.0

Cisco ME 3800X—Supported Topologies

Table 7-67 Supported Topologies for Cisco ME 3800X—Cisco Prime Network 3.9

Topology Type	Link Type	Product_Version
BGP	BGP	3.7.1
Ethernet	Ethernet	3.7.1
MPLS	MPLS	3.7.1
LAG	LAG	3.7.1

Cisco ME 3800X—Supported Modules

Table 7-68 Supported Modules for Cisco ME 3800X—Cisco Prime Network 3.9

Module Name	Product_Version	Module Description
CWDM-SFP-1470	3.7.1	1470nm color coded CWDM SFP
CWDM-SFP-1490	3.7.1	1490nm color coded CWDM SFP
CWDM-SFP-1510	3.7.1	1510nm color coded CWDM SFP
CWDM-SFP-1530	3.7.1	1530nm color coded CWDM SFP
CWDM-SFP-1550	3.7.1	1550nm color coded CWDM SFP
CWDM-SFP-1570	3.7.1	1570nm color coded CWDM SFP
CWDM-SFP-1590	3.7.1	1590nm color coded CWDM SFP
CWDM-SFP-1610	3.7.1	1610nm color coded CWDM SFP
GLC-BX-D	3.7.1	1000BASE-BX10-D downstream bidirectional single fiber SFP
GLC-BX-U	3.7.1	1000BASE-BX10-U upstream bidirectional single fiber SFP
GLC-FE-100BX-D	3.7.1	Fiber Fast Ethernet bi-directional 10kmDownlink over SMF

Table 7-68 Supported Modules for Cisco ME 3800X—Cisco Prime Network 3.9 (continued)

Module Name	Product_Version	Module Description
GLC-FE-100BX-U	3.7.1	Fiber Fast Ethernet bi-directional 10km Uplinkover SMF
GLC-FE-100EX	3.7.1	100 BaseEX Fiber FastEthernet
GLC-FE-100FX	3.7.1	Short Wave Fiber Fast Ethernet
GLC-FE-100LX	3.7.1	Long Wave Fiber Fast Ethernet 10km over SMF
GLC-LH-SM	3.7.1	Longwavelength gigabit ethernet SFP
GLC-SX-MM	3.7.1	Shortwavelength gigabit ethernet SFP
GLC-T	3.7.1	Copper gigabit ethernet SFP
GLC-ZX-SM	3.7.1	Extended reach gigabit ethernet
ME-FANTRAY	3.7.1	Metro Ethernet 3600X/3800X Fan Tray
PWR-390W-AC	3.7.1	Metro Ethernet 3600X/3800X AC power supply
PWR-390W-DC	3.7.1	Metro Ethernet 3600X/3800X DC power supply
SFP-10G-LR	3.7.1	10Gigabit XFP Multi Mode Long Reach
SFP-10G-LRM	3.7.1	10GBASE-LRM SFP+ transceiver module for MMF and SMF, 1310-nm wavelength, LC duplex connector
SFP-10G-SR	3.7.1	10Gigabit XFP Multi Mode Short Reach
SFP-GE-L	3.7.1	1000BASE-LH/LX pluggable transceiver
SFP-GE-S	3.7.1	1000BASE-Sx Short wavelength gigabit ethernet SFP.

Cisco ME 3800X—Supported Technologies

The following technologies are supported by the Cisco ME 3800X in Cisco Prime Network 3.9:

- IP, page 7-92
- Routing Protocols, page 7-96
- Ethernet, page 7-99
- TDM/DSx, page 7-112
- MPLS, page 7-116
- MPLS-TE, page 7-118
- VPN (VRF), page 7-120
- PWE3, page 7-121
- Security, page 7-122
- Hardware, page 7-124
- LocalSwitching, page 7-128
- BFD, page 7-129
- Carrier Ethernet, page 7-129

- LLDP, page 7-131
- CDP, page 7-132
- Discovery Protocol, page 7-132
- Ethernet OAM, page 7-133

Cisco ME 3800X—Supported Service Events

Table 7-69 Supported Service Events for Cisco ME 3800X—Cisco Prime Network 3.9

Event Name	Product_Version	Expedited
Active IP Interfaces Found	3.7.1	Y
All IP Interfaces Down	3.7.1	Y
BGP process up	3.7.1	N
Card Down	3.7.1	Y
Card Up	3.7.1	Y
CPU utilization exceeded upper threshold	3.6.0	N
Device Unsupported	3.7.1	N
Keepalive configured	3.7.1	N
Keepalive not configured	3.7.1	N
Layer 2 Tunnel Down	3.7.1	N
Link up	3.7.1	N
Memory utilization exceeded upper threshold	3.7.1	N
Module Unsupported	3.7.1	Y
MPLS Black Hole found	3.7.1	N
Pluggable transceiver out	Prime Network 3.8	N
Rep port role change	Prime Network 3.8	Y

Cisco Nexus 7000 Series Switches

This section includes the following information about Cisco Nexus 7000 switches (for information on the NE types supported in Cisco Prime Network 3.9, see Cisco Nexus 7000 Series Switches):

- Cisco Nexus 7000—Supported Software Versions, page 7-79
- Cisco Nexus 7000—Supported Topologies, page 7-79
- Cisco Nexus 7000—Supported Modules, page 7-79

- Cisco Nexus 7000—Supported Technologies, page 7-80
- Cisco Nexus 7000—Supported Service Events, page 7-81

Cisco Nexus 7000—Supported Software Versions

Table 7-70 Supported Software Versions for Cisco Nexus 7000—Cisco Prime Network 3.9

Software Version	Product_Version
NX-OS 4.2(2)	3.7.1
NX-OS 4.2(3)	3.7.1
NX-OS 4.2(4)	3.7.2
NX-OS 5.0(3)	3.7.2
NX-OS 5.0(5)	ANA-3.7.2-DP1
NX-OS 5.1(1)	ANA-3.7.2-DP1
NX-OS 4.2(6)	ANA-3.7.2-DP3
NX-OS 6.0.2	ANA38 DP 2.0
NX-OS 5.2.1	373DP6.0

Cisco Nexus 7000—Supported Topologies

Table 7-71 Supported Topologies for Cisco Nexus 7000—Cisco Prime Network 3.9

Topology Type	Link Type	Product_Version
Business	Business	3.7.1
Ethernet	Ethernet	3.7.1
Physical Layer	Physical Layer	3.7.1

Cisco Nexus 7000—Supported Modules

Table 7-72 Supported Modules for Cisco Nexus 7000—Cisco Prime Network 3.9

Module Name	Product_Version	Module Description
GLC-SX-MM	3.7.1	1000BASE-SX SFP transceiver module for MMF, 850-nm wavelength
N7K-AC-7.5KW-US	3.7.1	Nexus 7000 - 7.5KW AC Power Supply Module US

Table 7-72 Supported Modules for Cisco Nexus 7000—Cisco Prime Network 3.9 (continued)

Module Name	Product_Version	Module Description
N7K-C7010-FAB-1	3.7.1	Nexus 7000 - 10 Slot Chassis - 46Gbps/Slot Fabric Module
N7K-C7018-FAB-1	3.7.1	Nexus 7000 - 18 Slot Chassis - 46Gbps/Slot Fabric Module
N7K-C7018-FAN	3.7.1	Nexus 7000 - 18 Slot Fan
N7K-DC-6.0KW	3.7.2	Nexus 7000 - 6.0KW DC Power Supply Module
N7K-M108X2-12L	3.7.2	Nexus 7000 - 8 Port 10GbE with XL option (req. X2)
N7K-M132XP-12	3.7.1	Nexus 7000 - 32 Port 10GbE, 80G Fabric (req. SFP+)
N7K-M148GS-11	3.7.1	Nexus 7000 - 48 Port 1G, SFP
N7K-M148GS-11L	3.7.2	Nexus 7000 - 48 Port GE Module with XL Option
N7K-M148GT-11	3.7.1	Nexus 7000 - 48 Port 10/100/1000, RJ-45
N7K-SUP1	3.7.1	Nexus 7000 - Supervisor, Includes External 8GB Log Flash
SFP-10G-LR	3.7.1	Cisco 10GBASE-LR SFP+ Module for SMF
SFP-10G-SR	3.7.1	Cisco 10GBASE-SR SFP+ Module for MMF
SFP-GE-S	3.7.1	1000BASE-SX pluggable transceiver
N7K-F132XP-15	ANA-3.7.2-DP1	Nexus 7000 - 32 Port 1G/10G Ethernet Module, SFP/SFP+
N7K-C7010-FAN-S	ANA-3.7.2-DP4	Nexus 7000 - 10 Slot System Fan
N7K-C7010-FAN-F	ANA-3.7.2-DP4	Nexus 7000 - 10 Slot Fabric Fan
N2K-C2248TP-1GE	ANA 3.7.x-DP9	Cisco Nexus 2000 Series 1GE Fabric Extender

Cisco Nexus 7000—Supported Technologies

The following technologies are supported by the Cisco Nexus 7000 in Cisco Prime Network 3.9:

- IP, page 7-92
- Routing Protocols, page 7-96
- Ethernet, page 7-99
- VPN (VRF), page 7-120
- Hardware, page 7-124
- Serial, page 7-127
- CDP, page 7-132

Cisco Nexus 7000—Supported Service Events

Table 7-73 Supported Service Events for Cisco Nexus 7000—Cisco Prime Network 3.9

Event Name	Product_Version	Expedited
Active IP Interfaces Found	3.7.1	Y
All IP Interfaces Down	3.7.1	Y
BGP process up	3.7.1	N
Card Down	3.7.1	Y
Card In	3.7.1	Y
Card Out	3.7.1	Y
Card Up	3.7.1	Y
CPU utilization exceeded upper threshold	3.7.1	N
Device Unsupported	3.7.1	N
Layer 2 Tunnel Down	3.7.1	N
Link up	3.7.1	N
Memory utilization exceeded upper threshold	3.7.1	N
Module Unsupported	3.7.1	N
MPLS Black Hole found	3.7.1	N
pluggable transceiver out	Prime Network 3.8	N
fan-tray down	Prime Network 3.8	N
fan-tray out	Prime Network 3.8	N
power-supply down	Prime Network 3.8	N

Cisco Nexus 5000 Series Switches

This section includes the following information about Cisco Nexus 5000 switches (for information on the NE types supported in Cisco Prime Network 3.9, see Cisco Nexus 5000 Series Switches):

- Cisco Nexus 5000—Supported Software Versions, page 7-82
- Cisco Nexus 5000—Supported Topologies, page 7-82
- Cisco Nexus 5000—Supported Modules, page 7-82

- Cisco Nexus 5000—Supported Technologies, page 7-83
- Cisco Nexus 5000—Supported Service Events, page 7-83

Cisco Nexus 5000—Supported Software Versions

Table 7-74 Supported Software Versions for Cisco Nexus 5000—Cisco Prime Network 3.9

Software Version	Product_Version
NX-OS 4.1(3)N2(1a))	3.7.2
NX-OS 4.2(1)N2(1)	3.7.2
5.0(2)N2(1)	3.7.2
5.0(2)N1(1)	ANA 3.7.x-DP08

Cisco Nexus 5000—Supported Topologies

Table 7-75 Supported Topologies for Cisco Nexus 5000—Cisco Prime Network 3.9

Topology Type	Link Type	Product_Version
Ethernet	Ethernet	3.7.2
Physical Layer	Physical Layer	3.7.2

Cisco Nexus 5000—Supported Modules

Table 7-76 Supported Modules for Cisco Nexus 5000—Cisco Prime Network 3.9

Module Name	Product_Version	Module Description
N5K-C5020-FAN	3.7.2	Cisco Nexus 5020 Fan Module
N5K-PAC-1200W	3.7.2	Nexus 5020 PSU module, 100-240VAC 1200W
SFP-10G-LR	3.7.2	Cisco 10GBASE-LR SFP+ Module for SMF
N5K-M1404	3.7.2	N5000 1000 Series Mod 4x10GE 4xFC 4/2/1G(req SFP+/SFP)
N5K-PAC-550W	ANA 3.7.x-DP08	Nexus 5010 PSU module, 110-208VAC 550w
N5K-C5010-FAN	ANA 3.7.x-DP08	Cisco Nexus 5010 Fan Module

Table 7-76 Supported Modules for Cisco Nexus 5000—Cisco Prime Network 3.9 (continued)

Module Name	Product_Version	Module Description
N2K-C2248TP-1GE	ANA 3.7.x-DP9	Cisco Nexus 2000 Series 1GE Fabric Extender

Cisco Nexus 5000—Supported Technologies

The following technologies are supported by the Cisco Nexus 5000 in Cisco Prime Network 3.9:

- IP, page 7-92
- Ethernet, page 7-99
- Hardware, page 7-124
- Serial, page 7-127
- CDP, page 7-132

Cisco Nexus 5000—Supported Service Events

Table 7-77 Supported Service Events for Cisco Nexus 5000—Cisco Prime Network 3.9

Event Name	Product_Version	Expedited
Active IP Interfaces Found	3.7.2	Y
All IP Interfaces Down	3.7.2	Y
Card Down	3.7.2	Y
Card In	3.7.2	Y
Card Out	3.7.2	Y
Card Up	3.7.2	Y
CPU utilization exceeded upper threshold	3.7.2	N
Device Unsupported	3.7.2	N
Link down due to admin down	3.7.2	Y
Link down due to Card event	3.7.2	Y
Link down due to oper down	3.7.2	Y
Link up	3.7.2	N
Memory utilization exceeded upper threshold	3.7.2	N
Module Unsupported	3.7.2	N
pluggable transceiver out	Prime Network 3.8	N

Table 7-77 Supported Service Events for Cisco Nexus 5000—Cisco Prime Network 3.9

Event Name	Product_Version	Expedited
fan-tray down	Prime Network 3.8	N
fan-tray out	Prime Network 3.8	N
power-supply down	Prime Network 3.8	N

Cisco Nexus 1000 Series Switches

This section includes the following information about Cisco Nexus 1000v switches (for information on the NE types supported in Cisco Prime Network 3.9, see Cisco Nexus 1000 Series Switches):

- Cisco Nexus 1000v—Supported Software Versions, page 7-84
- Cisco Nexus 1000v—Supported Modules, page 7-85
- Cisco Nexus 1000v—Supported Technologies, page 7-85

Cisco Nexus 1000v—Supported Software Versions

Table 7-78 Supported Software Versions for Cisco Nexus 1000v—Cisco Prime Network 3.9

Software Version	Product_Version
4.2(1)SV1(5.1)	ANA 3.7.x-DP09, CiscoPrimeNetwork-3.8-DP1

Cisco Nexus 1000v—Supported Modules

Table 7-79 Supported Modules for Cisco Nexus 1000v—Cisco Prime Network 3.9

Module Name	Product_Version	Module Description
VIRTUAL SUPERVISOR MODULE	ANA 3.7.x-DP09, CiscoPrimeNetwork-3.8-DP1	Virtual Supervisor Module
VIRTUAL ETHERNET MODULE	ANA 3.7.x-DP09, CiscoPrimeNetwork-3.8-DP1	Virtual Ethernet Module

Cisco Nexus 1000v—Supported Technologies

The following technologies are supported by the Cisco Nexus 1000v in Cisco Prime Network 3.9:

- IP, page 7-92
- Ethernet, page 7-99
- Hardware, page 7-124
- Serial, page 7-127
- CDP, page 7-132

Cisco ACE 4700 Series Access Control Engine

This section includes the following information about Cisco ACE 4700 switches (for information on the NE types supported in Cisco Prime Network 3.9, see Cisco ACE 4700 Series Access Control Engine):

- Cisco ACE 4700—Supported Software Versions, page 7-86
- Cisco ACE 4700—Supported Topologies, page 7-86
- Cisco ACE 4700—Supported Technologies, page 7-86
- Cisco ACE 4700—Supported Service Events, page 7-86

Cisco ACE 4700—Supported Software Versions

Table 7-80 Supported Software Versions for Cisco ACE 4700—Cisco Prime Network 3.9

Software Version	Product_Version
ACE Appliance SW 3.2	3.7.1

Cisco ACE 4700—Supported Topologies

Table 7-81 Supported Topologies for Cisco ACE 4700—Cisco Prime Network 3.9

Topology Type	Link Type	Product_Version
Business	Business	3.7.1
Ethernet	Ethernet	3.7.1
Physical Layer	Physical Layer	3.7.1

Cisco ACE 4700—Supported Technologies

The following technologies are supported by the Cisco ACE 4700 in Cisco Prime Network 3.9:

- IP, page 7-92
- Hardware, page 7-124
- Serial, page 7-127

Cisco ACE 4700—Supported Service Events

Table 7-82 Supported Service Events for Cisco ACE 4700—Cisco Prime Network 3.9

Event Name	Product_Version	Expedited
Active ip interfaces found	3.7.1	N
All ip interfaces down	3.7.1	N
BFD connectivity down	3.7.1	N
BFD connectivity up	3.7.1	N
BFD neighbor found	3.7.1	N
BFD neighbor loss	3.7.1	N
BGP link down due to admin	3.7.1	N
BGP link down due to oper	3.7.1	N
BGP link down vrf due to admin	3.7.1	N

Table 7-82 Supported Service Events for Cisco ACE 4700—Cisco Prime Network 3.9 (continued)

Event Name	Product_Version	Expedited
BGP link down vrf due to oper	3.7.1	N
BGP link up	3.7.1	N
BGP neighbor found	3.7.1	N
BGP neighbor loss due to admin	3.7.1	N
BGP neighbor loss due to oper	3.7.1	N
BGP neighbor loss VRF due to admin	3.7.1	N
BGP neighbor loss VRF due to oper	3.7.1	N
BGP process down	3.7.1	N
BGP process up	3.7.1	N
Card down	3.7.1	N
Card in	3.7.1	N
Card out	3.7.1	N
Card up	3.7.1	N
Device Managed	3.7.1	N
Device Partially Managed	3.7.1	N
Device Unsupported	3.7.1	N
Discarded packet rate exceeded upper threshold	3.7.1	N
Discarded packet rate is below lower threshold	3.7.1	N
Dropped packet rate exceeded upper threshold	3.7.1	N
Dropped packet rate is below lower threshold	3.7.1	N
DS1 Path down due to Admin	3.7.1	N
DS1 Path down due to Card	3.7.1	N
DS1 Path down due to Oper	3.7.1	N
DS1 Path Link down due to Card event	3.7.1	N
DS1 Path Link down on unreachable	3.7.1	N
DS1 Path up	3.7.1	N
DS3 Path down due to Admin	3.7.1	N
DS3 Path down due to Card	3.7.1	N
DS3 Path down due to Oper	3.7.1	N
DS3 Path Link down due to admin down	3.7.1	N

Table 7-82 Supported Service Events for Cisco ACE 4700—Cisco Prime Network 3.9 (continued)

Event Name	Product_Version	Expedited
DS3 Path Link down due to Card event	3.7.1	N
DS3 Path Link down due to oper down	3.7.1	N
DS3 Path Link down on unreachable	3.7.1	N
DS3 Path Link up	3.7.1	N
DS3 Path up	3.7.1	N
Dual stack IP added	3.7.1	N
Dual stack IP removed	3.7.1	N
GRE tunnel down	3.7.1	N
GRE tunnel up	3.7.1	N
High priority member down	3.7.1	N
High Priority MPLS-TE tunnel down	3.7.1	N
Interface status down	3.7.1	N
Interface status up	3.7.1	N
keepalive configured	3.7.1	N
keepalive not configured	3.7.1	N
l2tp peer established	3.7.1	N
l2tp peer is removed	3.7.1	N
l2tp peer not established	3.7.1	N
Layer 2 tunnel up	3.7.1	N
LDP neighbor down	3.7.1	N
LDP neighbor up	3.7.1	N
Link down due to admin down	3.7.1	N
Link down due to Card event	3.7.1	N
Link down due to oper down	3.7.1	N
Link down on unreachable	3.7.1	N
Link over utilized	3.7.1	N
Link up	3.7.1	N
Link utilization normal	3.7.1	N
Local switching entry down	3.7.1	N
Local switching entry up	3.7.1	N
Logical port down	3.7.1	N
Logical port up	3.7.1	N
Low priority member down	3.7.1	N
Low Priority MPLS-TE tunnel down	3.7.1	N
Management Unreachable	3.7.1	N

Table 7-82 Supported Service Events for Cisco ACE 4700—Cisco Prime Network 3.9 (continued)

Event Name	Product_Version	Expedited
Medium priority member down	3.7.1	N
Medium Priority MPLS-TE tunnel down	3.7.1	N
Memory utilization exceeded upper threshold	3.7.1	N
Memory utilization less than lower threshold	3.7.1	N
MPLS Black hole cleared	3.7.1	N
MPLS Black hole found	3.7.1	N
MPLS interface added	3.7.1	N
MPLS interface removed	3.7.1	N
MPLS TE FRR State Changed to Active	3.7.1	N
MPLS TE FRR State Changed to Ready	3.7.1	N
MPLS-TE tunnel down	3.7.1	N
MPLS-TE tunnel up	3.7.1	N
OSPF Neighbor Down	3.7.1	N
OSPF Neighbor Up	3.7.1	N
Port down due to admin	3.7.1	N
Port down due to Card down	3.7.1	N
Port down due to Card out	3.7.1	N
Port down due to oper	3.7.1	N
Port up	3.7.1	N
Primary HSRP interface is active	3.7.1	N
Primary HSRP interface is not active	3.7.1	N
rx dormant	3.7.1	N
rx dormant normal	3.7.1	N
Rx utilization exceeded upper threshold	3.7.1	N
Rx utilization is below lower threshold	3.7.1	N
Secondary HSRP interface is active	3.7.1	N
Secondary HSRP interface is not active	3.7.1	N
Service down	3.7.1	N
Service up	3.7.1	N
Shelf in	3.7.1	N

Table 7-82 Supported Service Events for Cisco ACE 4700—Cisco Prime Network 3.9 (continued)

Event Name	Product_Version	Expedited
Shelf out	3.7.1	N
SONET Path down due to Admin	3.7.1	N
SONET Path down due to Card	3.7.1	N
SONET Path Link down due to Card event	3.7.1	N
SONET Path Link down on unreachable	3.7.1	N
SONET Path up	3.7.1	N
tx dormant	3.7.1	N
tx dormant normal	3.7.1	N
Tx utilization exceeded upper threshold	3.7.1	N
Tx utilization is below lower threshold	3.7.1	N
VC changed	3.7.1	N
VC removed	3.7.1	N
VC Restored	3.7.1	N
fan-tray down	Prime Network 3.8	N
fan-tray out	Prime Network 3.8	N
power-supply down	Prime Network 3.8	N

Cisco Service Control Engines

This section includes the following information about Cisco SCE switches (for information on the NE types supported in Cisco Prime Network 3.9, see Cisco Service Control Engines):

- Cisco SCE—Supported Topologies, page 7-91
- Cisco SCE—Supported Technologies, page 7-91
- Cisco SCE—Supported Service Events, page 7-91

Cisco SCE—Supported Topologies

Table 7-83 Supported Topologies for Cisco SCE—Cisco Prime Network 3.9

Topology Type	Link Type	Product_Version
Business	Business	3.7
Ethernet	Ethernet	3.7
Physical Layer	Physical Layer	3.7

Cisco SCE—Supported Technologies

The following technologies are supported by the Cisco SCE in Cisco Prime Network 3.9:

- IP, page 7-92
- Ethernet, page 7-99
- Hardware, page 7-124
- Serial, page 7-127

Cisco SCE—Supported Service Events

Table 7-84 Supported Service Events for Cisco SCE—Cisco Prime Network 3.9

Event Name	Product_Version	Expedited
Active IP Interfaces Found	3.7.1	Y
All IP Interfaces Down	3.7.1	Y
BGP process up	3.7.1	N
Card Down	3.7.1	Y
Card Up	3.7.1	Y
CPU utilization exceeded upper threshold	3.7.1	N
Device Unsupported	3.7.1	Y
Layer 2 Tunnel Down	3.7.1	N
Link up	3.7.1	N
Memory utilization exceeded upper threshold	3.7.1	N
Module Unsupported	3.7.1	Y
MPLS Black Hole found	3.7.1	N

Supported Technologies on Cisco Switches

The following sections list the objects and attributes that are supported on Cisco switches in Cisco Prime Network 3.9 per technology:

- IP, page 7-92
- Routing Protocols, page 7-96
- Ethernet, page 7-99
- ATM, page 7-105
- Frame Relay, page 7-108
- PPP, page 7-110
- HDLC, page 7-111
- SONET/SDH, page 7-111
- TDM/DSx, page 7-112
- MPLS, page 7-116
- MPLS-TE, page 7-118
- VPN (VRF), page 7-120
- PWE3, page 7-121
- Security, page 7-122
- Hardware, page 7-124
- Serial, page 7-127
- Additional Technologies, page 7-128
- LocalSwitching, page 7-128
- BFD, page 7-129
- Carrier Ethernet, page 7-129
- LLDP, page 7-131
- CDP, page 7-132
- Discovery Protocol, page 7-132
- Ethernet OAM, page 7-133

IP

Table 7-85 IP Attribute Support on Cisco Switches—Cisco Prime Network 3.9

Attribute	1900	2900	ME3400	3500	3550	3560	3750	3750ME	4000	4500	4900	4924ME	5000	6500 CatOS	6500 IOS	6524ME	ME 3600X	ME 3800X	Nexus 7000	Nexus 5000	Nexus 1000v	ACE 4700	SCE
IMO Name—IIPInterface																							
IP Address		Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y

Table 7-85 IP Attribute Support on Cisco Switches—Cisco Prime Network 3.9 (continued)

Attribute	1900	2900	ME3400	3500	3550	3560	3750	3750ME	4000	4500	4900	4924ME	5000	6500 CatOS	6500 IOS	6524ME	ME 3600X	ME 3800X	Nexus 7000	Nexus 5000	Nexus 1000v	ACE 4700	SCE
Subnetwork Mask		Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y
IP Interface Addresses Array		Y			Y	Y		Y		Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y
Interface Name	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y
Interface Description						Y		Y	Y	Y	Y	Y	Y		Y	Y	Y	Y	Y	Y	Y	Y	Y
IP Interface State	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	
OSPF Interface Cost																							
Broadcast Address									Y														
MTU																							
Lookup Method																							
Address Resolution Type																							
ARP Timeout																							
Secured ARP																							
ICMP Mask Reply																							
IGMP Proxy																							
HSRP Groups								Y		Y [1]					Y	Y	Y	Y					
IP Multiplexing Table																							
IANA Type									Y														
Containing CTPs																							
Contained CTPs																							
IMO Name—IIPMuxEntry																							
Termination Point					Y	Y		Y							Y	Y							
Destination IP Subnet					Y	Y		Y							Y	Y							
IMO Name—IRoutingEntity																							
Routing Table		Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	
ARP Entity		Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y		Y	Y	Y	Y	Y	Y	Y	Y	Y	
Routing Table Changes													Y										
Name		Y	Y	Y	Y	Y	Y	Y	Y	Y	Y		Y	Y	Y	Y	Y	Y					
Logical Sons		Y	Y	Y	Y	Y	Y	Y	Y	Y	Y		Y	Y	Y	Y	Y	Y					
IMO Name—IRoutingEntry																							
Destination IP Subnet		Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	
Next Hop IP Address		Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	
Type		Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	

Table 7-85 IP Attribute Support on Cisco Switches—Cisco Prime Network 3.9 (continued)

Attribute	1900	2900	ME3400	3500	3550	3560	3750	3750ME	4000	4500	4900	4924ME	5000	6500 CatOS	6500 IOS	6524ME	ME 3600X	ME 3800X	Nexus 7000	Nexus 5000	Nexus 1000v	ACE 4700	SCE
Routing Protocol Type		Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	
Outgoing Interface Name		Y	Y	Y	Y	Y	Y	Y		Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	
IMO Name—IARPEntity																							
ARP Table		Y	Y	Y	Y	Y	Y	Y	Y	Y	Y		Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y
IMO Name—IARPEntry																							
IP Address		Y	Y	Y	Y	Y	Y	Y		Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y
MAC Address		Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y
Port		Y	Y	Y	Y	Y	Y	Y		Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y
Entry Type								Y	Y		Y	Y	Y		Y	Y	Y	Y	Y	Y	Y	Y	Y
IMO Name—IIPPool																							
IP Address Pool Entries																							
Name																							
Index																							
IMO Name—IIPRangeBasedIPPoolEntry																							
Start IP Address																							
End IP Address																							
Unused Addresses																							
Used Addresses																							
Reserved Addresses																							
IMO Name—IIPSubnetBasedIPPoolEntry																							
IP Subnet																							
Unused Addresses																							
Used Addresses																							
Reserved Addresses																							
IMO Name—HSRPGroupEntry																							
Group Number								Y		Y [2]	Y [3]				Y	Y	Y	Y					
Port Description								Y		Y [4]	Y [5]				Y	Y	Y	Y					
Priority								Y		Y [6]	Y [7]				Y	Y	Y	Y					
Coupled Router								Y		Y [8]	Y [9]				Y	Y	Y	Y					
State								Y		Y [10]	Y [11]				Y	Y	Y	Y					

Table 7-85 IP Attribute Support on Cisco Switches—Cisco Prime Network 3.9 (continued)

Attribute	1900	2900	ME3400	3500	3550	3560	3750	3750ME	4000	4500	4900	4924ME	5000	6500 CatOS	6500 IOS	6524ME	ME 3600X	ME 3800X	Nexus 7000	Nexus 5000	Nexus 1000v	ACE 4700	SCE
Tracking Interfaces																	Y						
Virtual IP Address								Y		Y [12]	Y [13]				Y	Y	Y	Y					
Virtual MAC Address								Y		Y [14]	Y [15]				Y	Y	Y	Y					
IMO Name—ITunnelGRE																							
Name								Y		Y [16]	Y [17]	Y	Y		Y	Y							
Tunnel Destination and Source								Y		Y [18]	Y [19]	Y	Y		Y	Y							
IP Address								Y		Y [20]	Y [21]	Y	Y		Y	Y							
IP Interface State											Y				Y	Y							
IANA Type																							
Containing CTPs																							
Contained CTPs																							
Keep Alive Time								Y		Y	Y		Y										
Keep Alive Retry								Y		Y	Y		Y										
IMO Name—IVrrpGroupEntry																							
Group Number																							
State																							
Port Description																							
Master IP Address																							
Primary IP Address																							
Priority																							
Virtual Mac Address																							
Preempt Mode																							
Admin State																							
Advertisement Interval																							
Tracking Interfaces																							
IMO Name—IIPSLAResponderService																							
responderStatus			Y [22]																				
TWAMPResponderStatus			Y [23]																				

Table 7-85 IP Attribute Support on Cisco Switches—Cisco Prime Network 3.9 (continued)

Attribute	1900	2900	ME3400	3500	3550	3560	3750	3750ME	4000	4500	4900	4924ME	5000	6500 CatOS	6500 IOS	6524ME	ME 3600X	ME 3800X	Nexus 7000	Nexus 5000	Nexus 1000v	ACE 4700	SCE
tcpConnect			Y [24]																				
udpEcho			Y [25]																				
IMO Name—IIPAddressPortPair																							
type			Y [26]																				
ipAddress			Y [27]																				
port			Y [28]																				

[1, 2, 3, 4, 5, 6, 7] Not supported for version 12.2(58)SE1

[8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18] Supported for 4503E, 4507RE, 4507, and 4506E only.

[19, 20, 21, 22, 23, 24, 25, 26, 27, 28] Validated with 12.2(52)SG only.

Routing Protocols

Table 7-86 Routing Protocols Attribute Support on Cisco Switches—Cisco Prime Network 3.9

Attribute	1900	2900	ME3400	3500	3550	3560	3750	3750ME	4000	4500	4900	4924ME	5000	6500 CatOS	6500 IOS	6524ME	ME 3600X	ME 3800X	Nexus 7000	Nexus 5000	Nexus 1000v	ACE 4700	SCE
IMO Name—IBgpNeighborEntry																							
Remote Identifier						Y		Y		Y [1]	Y [2]	Y			Y	Y	Y	Y	Y				
Neighbor Type																			Y				
Distributing Interfaces																							
Remote Address						Y		Y		Y [3]	Y [4]	Y			Y	Y	Y	Y	Y				
Remote Autonomous System						Y		Y		Y [5]	Y [6]	Y			Y	Y	Y	Y	Y				
Peer State						Y		Y		Y [7]	Y [8]	Y			Y	Y	Y	Y	Y				
Peer AdminState								Y											Y				
Hold Time						Y		Y		Y [9]	Y [10]	Y			Y	Y	Y	Y	Y				

Table 7-86 Routing Protocols Attribute Support on Cisco Switches—Cisco Prime Network 3.9 (continued)

Attribute	1900	2900	ME3400	3500	3550	3560	3750	3750ME	4000	4500	4900	4924ME	5000	6500 CatOS	6500 IOS	6524ME	ME 3600X	ME 3800X	Nexus 7000	Nexus 5000	Nexus 1000v	ACE 4700	SCE
Keep Alive Time						Y		Y		Y [11]	Y [12]	Y			Y	Y	Y	Y	Y				
VrfName																			Y				
Address family						Y													Y				
IMO Name—IOspfEntry																							
Area Identifier			Y					Y		Y [13]	Y [14]	Y			Y	Y	Y	Y					
IP Address			Y					Y		Y [15]	Y [16]	Y			Y	Y	Y	Y					
Type			Y					Y		Y [17]	Y [18]	Y			Y	Y	Y	Y					
Administrative Status			Y					Y		Y [19]	Y [20]	Y			Y	Y	Y	Y					
Ospf Entry State			Y					Y		Y [21]	Y [22]	Y			Y	Y	Y	Y					
IMO Name—IOspfProcess																							
Process Id																	Y	Y	Y				
OSPF Version																	Y	Y	Y				
Router Id																	Y	Y	Y				
IMO Name—IOspfNeighbor																							
Neighbor Id																	Y	Y	Y				
Outgoing Interface																	Y	Y	Y				
State																	Y	Y	Y				
Neighbor Interface Address																	Y	Y	Y				
Area Id																	Y	Y	Y				
IMO Name—IOspfInterface																							
Area Id																	Y	Y	Y				
Network Type																	Y	Y	Y				
Cost																	Y	Y	Y				
State																	Y	Y	Y				
Interface Address																							
Type																	Y	Y	Y				
IF Proirity																	Y	Y	Y				
DR Id																	Y	Y	Y				
BDR Id																	Y	Y	Y				

Table 7-86 Routing Protocols Attribute Support on Cisco Switches—Cisco Prime Network 3.9 (continued)

Attribute	1900	2900	ME3400	3500	3550	3560	3750	3750ME	4000	4500	4900	4924ME	5000	6500 CatOS	6500 IOS	6524ME	ME 3600X	ME 3800X	Nexus 7000	Nexus 5000	Nexus 1000v	ACE 4700	SCE
IMO Name—ISpfTimers																							
Schedule Delay																	Y	Y	Y				
Min Hold Time																	Y	Y	Y				
Max Wait Time																	Y	Y	Y				
IMO Name—IISISProcess																							
ISIS Version																	Y	Y					
Manual Area Address																	Y	Y					
IS Type																	Y	Y					
System Id																	Y	Y					
Process Id																	Y	Y					
IMO Name—IISISMetric																							
IS Type																	Y	Y					
Metric Style																	Y	Y					
Metric Value																	Y	Y					
Address Family																	Y	Y					
IMO Name—IISISInterface																							
Interface Name																	Y	Y					
IMO Name—IISISNeighbor																							
IS Type																	Y	Y					
System Id																	Y	Y					
Admin State																	Y	Y					
Hold Time																	Y	Y					
SNPA																	Y	Y					
Interface Name																	Y	Y					
IP Address																	Y	Y					
Adress Family																	Y	Y					

[1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11] Supported for 4503E, 4507RE, 4507, and 4506E only.

[12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22] Validated with 12.2(52)SG only.

Ethernet

Table 7-87 Ethernet Attribute Support on Cisco Switches—Cisco Prime Network 3.9

Attribute	1900	2900	ME3400	3500	3550	3560	3750	3750ME	4000	4500	4900	4924ME	5000	6500 CatOS	6500 IOS	6524ME	ME 3600X	ME 3800X	Nexus 7000	Nexus 5000	Nexus 1000v	ACE 4700	SCE
IMO Name—ILinkAggregationGroup802dot3ad																							
dot3adAggMACAddress		Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y				
dot3adAggActorSystemPriority		Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y				
dot3adAggActorSystemID		Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y				
dot3adAggActorAdminKey		Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y				
dot3adAggActorOperKey		Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y				
dot3adAggPartnerSystemID		Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y				
dot3adAggPartnerSystemPriority		Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y				
dot3adAggPartnerOperKey		Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y				
dot3adAggCollectorMaxDelay		Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y				
GroupNumber		Y	Y	Y	Y	Y	Y		Y	Y	Y	Y	Y	Y	Y	Y			Y				
AggregationProtocolType		Y	Y	Y	Y	Y	Y		Y	Y	Y	Y	Y	Y	Y	Y			Y				
MacAddress		Y	Y	Y	Y	Y	Y		Y	Y	Y	Y	Y	Y	Y	Y			Y				
ChannelAdminStatus		Y	Y	Y	Y	Y	Y		Y	Y	Y	Y	Y	Y	Y	Y			Y				
ChannelOperStatus		Y	Y	Y	Y	Y	Y		Y	Y	Y	Y	Y	Y	Y	Y			Y				
IMO Name—IEthernet																							
MAC Address	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y		Y			Y
Duplex Mode																							
Output Flow Control																							
Input Flow Control																							
IANA Type																Y							
Containing CTPs																							
Contained CTPs																							
Port Type			Y																				
isElmiEnabled								Y							Y								
isLOAMEnabled								Y							Y		Y	Y					
IMO Name—IVlanInterface																							
Mode			Y		Y	Y	Y	Y		Y [1]	Y	Y		Y	Y	Y	Y	Y	Y				

Table 7-87 Ethernet Attribute Support on Cisco Switches—Cisco Prime Network 3.9 (continued)

Attribute	1900	2900	ME3400	3500	3550	3560	3750	3750ME	4000	4500	4900	4924ME	5000	6500 CatOS	6500 IOS	6524ME	ME 3600X	ME 3800X	Nexus 7000	Nexus 5000	Nexus 1000v	ACE 4700	SCE
Native VLAN Identification			Y		Y	Y	Y	Y		Y [2]	Y	Y		Y	Y	Y	Y	Y	Y				
Virtual LAN Table																							
IANA Type																Y							
Containing CTPs																	Y	Y					
Contained CTPs																	Y	Y					
vlanAdminType			Y					Y			Y			Y			Y	Y					
vlanencapType			Y					Y			Y			Y			Y	Y					
getAccess																							
Allowed Vlans								Y			Y			Y			Y	Y					
IMO Name—IVlanEncapMux																							
IANA Type							Y	Y															
Containing CTPs																							
Contained CTPs																							
IMO Name—IVlanMapping																							
direction			Y [3]					Y							Y	Y							
vlanMatchCriteria			Y [4]					Y							Y	Y							
vlanRewriteDefinition			Y [5]					Y							Y	Y							
Drop			Y [6]					Y							Y	Y							
Vlan			Y [7]					Y							Y	Y							
innerVlan			Y [8]					Y							Y	Y							
translatedVlan			Y [9]					Y							Y	Y							
translatedInnerVlan			Y [10]					Y							Y	Y							
IMO Name—IIEEE802																							
VLAN Identification			Y	Y	Y	Y	Y	Y	Y	Y	Y	Y			Y	Y							
Binding Information																							
Binding Status																							
IANA Type				Y	Y	Y	Y	Y	Y	Y					Y	Y							

Table 7-87 Ethernet Attribute Support on Cisco Switches—Cisco Prime Network 3.9 (continued)

Attribute	1900	2900	ME3400	3500	3550	3560	3750	3750ME	4000	4500	4900	4924ME	5000	6500 CatOS	6500 IOS	6524ME	ME 3600X	ME 3800X	Nexus 7000	Nexus 5000	Nexus 1000v	ACE 4700	SCE
Containing CTPs																							
Contained CTPs																							
IMO Name—IStpService																							
StpProtocol		Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y		Y	Y	Y	Y	Y	Y				
StpMaxAge		Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y				
StpHelloTime		Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y				
StpBridgeForwardDelay		Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y				
StpInstanceInfoTable		Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y		Y	Y	Y	Y	Y	Y				
Same as ISystemService																			Y				
StpUplinkFastState		Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y		Y	Y	Y	Y	Y	Y				
StpBackboneFastState		Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y		Y	Y	Y	Y	Y	Y				
StpForwardDelay		Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y				
StpBridgeMaxAge		Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y				
StpBridgeHelloTime		Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y				
IMO Name—IMstService																							
MstProperties		Y					Y						Y						Y				
Same as IStpService		Y					Y						Y						Y				
IMO Name—IPvstpService																							
UpLinkFast		Y	Y	Y	Y	Y		Y	Y	Y	Y	Y		Y	Y	Y	Y	Y	Y				
BackboneFast		Y	Y	Y	Y	Y		Y	Y	Y	Y	Y		Y	Y	Y	Y	Y	Y				
IMO Name—IMstProperties																							
MstForceVersion		Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y		Y	Y	Y	Y	Y	Y				
MstCfgIdFmtSel		Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y		Y	Y	Y	Y	Y	Y				
MstExternalRootCost		Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y		Y	Y	Y	Y	Y	Y				
MstMaxInstances		Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y		Y	Y	Y	Y	Y	Y				
MstCfgIdName		Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y		Y	Y	Y	Y	Y	Y				
MstCfgIdRevLevel		Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y		Y	Y	Y	Y	Y	Y				
IMO Name—IStpInstanceInfo																							
Object Identification																			Y				
StpBridgeId		Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y		Y	Y	Y	Y	Y	Y				
BridgePriority		Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y		Y	Y	Y	Y	Y	Y				
Designated Parent and Root Bridges		Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y		Y	Y	Y	Y	Y	Y				
StpRootCost		Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y		Y	Y	Y	Y	Y	Y				

Table 7-87 Ethernet Attribute Support on Cisco Switches—Cisco Prime Network 3.9 (continued)

Attribute	1900	2900	ME3400	3500	3550	3560	3750	3750ME	4000	4500	4900	4924ME	5000	6500 CatOS	6500 IOS	6524ME	ME 3600X	ME 3800X	Nexus 7000	Nexus 5000	Nexus 1000v	ACE 4700	SCE
IsRoot		Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y		Y	Y	Y	Y	Y	Y				
StpRootPort		Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y		Y	Y	Y	Y	Y	Y				
StpPortInfoTable		Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y		Y	Y	Y	Y	Y	Y				
STP Instance Id		Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y		Y	Y	Y	Y	Y	Y				
Vlan Id																			Y				
StpDesignatedBridge		Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y		Y	Y	Y	Y	Y	Y				
StpDesignatedRoot		Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y		Y	Y	Y	Y	Y	Y				
IMO Name—IMstInstanceInfo																							
MstVlanIds		Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y		Y	Y	Y	Y	Y	Y				
Same as IStpInstanceInfo		Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y		Y	Y	Y	Y	Y	Y				
IMO Name—IPvstpInstanceInfo																							
Protocol Type		Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y		Y	Y	Y	Y	Y	Y				
StpBridgeMaxAge		Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y		Y	Y	Y	Y	Y	Y				
StpBridgeHelloTime		Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y		Y	Y	Y	Y	Y	Y				
StpBridgeForwardDelay		Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y		Y	Y	Y	Y	Y	Y				
StpProtocolSpecification		Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y		Y	Y	Y	Y	Y	Y				
StpVlanId		Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y		Y	Y	Y	Y	Y	Y				
StpForwardDelay		Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y		Y	Y	Y	Y	Y	Y				
StpMaxAge		Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y		Y	Y	Y	Y	Y	Y				
IMO Name—IRstpInstanceInfo																							
StpForceVersion		Y	11	Y	Y	Y	12	13	Y	Y	Y	Y		Y	14	Y	15	16					
Same as IStpInstanceInfo		Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y		Y	Y	Y	Y	Y					
IMO Name—IStpPortInfo																							
StpPort		Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y		Y	Y		Y	Y	Y				
StpPortPriority		Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y		Y	Y		Y	Y	Y				
StpPortState		Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y		Y	Y		Y	Y	Y				
StpPortPathCost		Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y		Y	Y		Y	Y	Y				
StpPortEdgePort		Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y		Y	Y		Y	Y	Y				
StpPortPointToPoint		Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y		Y	Y		Y	Y	Y				
StpPortRole		Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y		Y	Y		Y	Y	Y				
StpDesignatedPortIdentifier		Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y		Y	Y		Y	Y	Y				
StpDesignatedBridge		Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y		Y	Y		Y	Y	Y				
StpPortIdentifier		Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y		Y	Y		Y	Y	Y				
StpPortBpduGuardState		Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y		Y	Y		Y	Y	Y				

Table 7-87 Ethernet Attribute Support on Cisco Switches—Cisco Prime Network 3.9 (continued)

Attribute	1900	2900	ME3400	3500	3550	3560	3750	3750ME	4000	4500	4900	4924ME	5000	6500 CatOS	6500 IOS	6524ME	ME 3600X	ME 3800X	Nexus 7000	Nexus 5000	Nexus 1000v	ACE 4700	SCE
StpPortBpduFilterState		Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y		Y	Y		Y	Y	Y				
IMO Name—IMstPortInfo																							
MstPortHelloTime		Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y			Y		Y	Y					
Same as IStpPortInfo		Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y		Y	Y		Y	Y	Y				
IMO Name—IPvstpPortInfo																							
PvstpPortFastState		Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y		Y	Y		Y	Y	Y				
IMO Name—IEthernetChannel																							
Group Number		Y [17]	Y	Y	Y [18]	Y [19]	Y	Y	Y	Y	Y	Y		Y	Y	Y	Y	Y	Y		Y		
Bandwidth		Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y		Y	Y	Y	Y	Y	Y		Y		
Aggregation Protocol		Y [20]	Y	Y	Y [21]	Y [22]	Y	Y	Y	Y	Y			Y	Y	Y	Y	Y	Y		Y		
IANA Type		Y [23]	Y	Y	Y [24]	Y [25]	Y	Y	Y	Y	Y			Y	Y	Y	Y	Y	Y		Y		
Containing CTPs																			Y				
Contained CTPs																			Y				
Mac Address								Y									Y	Y	Y		Y		
Admin Status								Y						Y			Y	Y	Y		Y		
Oper Status								Y						Y			Y	Y	Y		Y		
IMO Name—ITokenRingLayer2																							
MAC Address																							
IANA Type																							
Containing CTPs																							
Contained CTPs																							
IMO Name—ITokenRingLayer1																							
Same as IPhysicalLayer																							
IMO Name—IVtpService																							
Version	Y	Y	[26]	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y							
OperatingMode	Y	Y	[27]	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y							
DomainName		Y	[28]	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y							
ConfigurationRevision	Y	Y	[29]	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y							
isPruningEnabled	Y	Y	[30]	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y							
isAuthenticationEnabled	Y	Y	[31]	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y							

Table 7-87 Ethernet Attribute Support on Cisco Switches—Cisco Prime Network 3.9 (continued)

Attribute	1900	2900	ME3400	3500	3550	3560	3750	3750ME	4000	4500	4900	4924ME	5000	6500 CatOS	6500 IOS	6524ME	ME 3600X	ME 3800X	Nexus 7000	Nexus 5000	Nexus 1000v	ACE 4700	SCE
IMO Name—IREPService																							
version		Y [32]	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y		Y	Y	Y	Y					
administrativeVlan		Y [33]	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y		Y	Y	Y	Y					
notificationEnabled		Y [34]	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y		Y	Y	Y	Y					
IMO Name—IREPSegmentInfo																							
segmentId		Y [35]	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y		Y	Y	Y	Y					
segmentComplete		Y [36]	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y		Y	Y	Y	Y					
IMO Name—IREPPortInfo																							
portName		Y [37]	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y		Y	Y	Y	Y					
portKey		Y [38]	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y		Y	Y	Y	Y					
segmentId		Y [39]	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y		Y	Y	Y	Y					
portType		Y [40]	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y		Y	Y	Y	Y					
portRole		Y [41]	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y		Y	Y	Y	Y					
operStatus		Y [42]	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y		Y	Y	Y	Y					
blockedVlans		Y [43]	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y		Y	Y	Y	Y					
preemptTimer		Y [44]	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y		Y	Y	Y	Y					
lslAgeoutTimer		Y [45]	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y		Y	Y	Y	Y					
remoteDeviceName		Y [46]	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y		Y	Y	Y	Y					
remoteDeviceMac		Y [47]	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y		Y	Y	Y	Y					
remotePortName		Y [48]	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y		Y	Y	Y	Y					
configuredLoadBalancingBlockedVlans		Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y		Y	Y	Y	Y					

Table 7-87 Ethernet Attribute Support on Cisco Switches—Cisco Prime Network 3.9 (continued)

Attribute	1900	2900	ME3400	3500	3550	3560	3750	3750ME	4000	4500	4900	4924ME	5000	6500 CatOS	6500 IOS	6524ME	ME 3600X	ME 3800X	Nexus 7000	Nexus 5000	Nexus 1000v	ACE 4700	SCE
IMO Name—IBridgeILan																							
Id																							
IMO Name—IIBBridgeEntry																							
IS Id																							
IBridge																							
BBridge																							

[1, 2, 3]SNMP is supported from ANA 3.6.0

[4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20]Not Supported on IOS version 12.2(25)SEE2

[21, 22, 23, 24, 25, 26, 27, 28]Supported only on ME3400-E devices.

[29, 42, 43, 46, 47, 48]CSCti41937

[30, 31, 32, 33, 34, 35]The MIB provides data by default, but the device does not support VTP.

[36, 37, 38, 39, 40, 41]SNMP is supported on ANA 3.6.0 and later.

[44, 45]Supported for 12.2(25)EWA14 only.

ATM

Table 7-88 ATM Attribute Support on Cisco Switches—Cisco Prime Network 3.9

Attribute	1900	2900	ME3400	3500	3550	3560	3750	3750ME	4000	4500	4900	4924ME	5000	6500 CatOS	6500 IOS	6524ME	ME 3600X	ME 3800X	Nexus 7000	Nexus 5000	Nexus 1000v	ACE 4700	SCE
IMO Name—IAtm																							
ATM Address																							
Interface Type																							
VP and VC Ranges																							
VC Table															Y								
Cross-Connect Table																							
IANA Type															Y								
Containing CTPs																							
Contained CTPs																							
Tx Allocated Bandwidth															Y								
Tx Maximum Bandwidth															Y								
Tx UBR Allocated Bandwidth															Y								

Table 7-88 ATM Attribute Support on Cisco Switches—Cisco Prime Network 3.9 (continued)

Attribute	1900	2900	ME3400	3500	3550	3560	3750	3750ME	4000	4500	4900	4924ME	5000	6500 CatOS	6500 IOS	6524ME	ME 3600X	ME 3800X	Nexus 7000	Nexus 5000	Nexus 1000v	ACE 4700	SCE
Tx CBR Allocated Bandwidth															Y								
Rx Allocated Bandwidth															Y								
Rx Maximum Bandwidth															Y								
Rx UBR Allocated Bandwidth															Y								
Rx CBR Allocated Bandwidth															Y								
IMO Name—IAtmVc																							
Virtual Channel Identifier															Y								
Virtual Path Identifier															Y								
Shaping Profile																							
Discarded and Received Input Data Counters															Y								
Dropped and Forward Output Data Counters															Y								
Ingress Traffic Descriptor															Y								
Egress Traffic Descriptor															Y								
Administrative Status															Y								
Operational Status															Y								
IANA Type																							
Containing CTPs																							
Contained CTPs																							
IMO Name—IAtmTrafficDescriptor																							
Traffic Descriptor Type															Y								
Service Category															Y								
Cell Loss Priority															Y								
Cell Delay Variation																							
Cell Delay Variation Tolerance															Y								
Maximum High Priority and Aggregate Cell Rates															Y								
Minimum High Priority and Aggregate Cell Rates															Y								
Sustainable High Priority and Aggregate Cell Rates															Y								

Table 7-88 ATM Attribute Support on Cisco Switches—Cisco Prime Network 3.9 (continued)

Attribute	1900	2900	ME3400	3500	3550	3560	3750	3750ME	4000	4500	4900	4924ME	5000	6500 CatOS	6500 IOS	6524ME	ME 3600X	ME 3800X	Nexus 7000	Nexus 5000	Nexus 1000v	ACE 4700	SCE
Peak High Priority and Aggregate Cell Rates															Y								
Name																							
Index																							
IMO Name—IAtmTrafficShapingDescriptor																							
Maximum Burst Size																							
Sustainable and Peak Cell Rates																							
Cell Delay Variation																							
State																							
Buffer Size																							
Cell Loss Priority Discarded Size																							
Name																							
Index																							
IMO Name—IAtmTrunk																							
Same as IAtm																							
IMO Name—IAtmLogicalPort/Trunk																							
Resource Management Cell Termination																							
Resource Management Cell Generation																							
Effective Check Input and Output Capacities																							
Admin Status																							
Oper Status																							
Same as IAtm																							
IMO Name—IAtmTrunkVc																							
Destination Description																							
Same as IAtmVc																							
IMO Name—IVcSwitchingEntity																							
Cross Connect Table																							
crossConnectTableSize																							
Logical Sons																							
IMO Name—IIMAGroup																							
AdminStatus																							

Table 7-88 ATM Attribute Support on Cisco Switches—Cisco Prime Network 3.9 (continued)

Attribute	1900	2900	ME3400	3500	3550	3560	3750	3750ME	4000	4500	4900	4924ME	5000	6500 CatOS	6500 IOS	6524ME	ME 3600X	ME 3800X	Nexus 7000	Nexus 5000	Nexus 1000v	ACE 4700	SCE
OperStatus																							
GroupNumber																							
ImaVersion																							
Speed																							
ConfiguredBandwidth																							
NumberOfLinks																							
NumberOfActiveLinks																							
MinimumNumberOfTxLinks																							
MinimumNumberOfRxLinks																							
ClockMode																							
FrameLength																							
interfaceName																							
groupStatus																							

Frame Relay

Table 7-89 Frame Relay Attribute Support on Cisco Switches—Cisco Prime Network 3.9

Attribute	1900	2900	ME3400	3500	3550	3560	3750	3750ME	4000	4500	4900	4924ME	5000	6500 CatOS	6500 IOS	6524ME	ME 3600X	ME 3800X	Nexus 7000	Nexus 5000	Nexus 1000v	ACE 4700	SCE
IMO Name—IFrameRelay/IFrTrunk																							
Protocol Type																							
VC Table																							
Cross-Connect Table																							
IANA Type																							
Containing CTPs																							
Contained CTPs																							
IMO Name—IFrVc																							
Data Link Connection Identifier																							
Traffic Descriptor																							

Table 7-89 Frame Relay Attribute Support on Cisco Switches—Cisco Prime Network 3.9 (continued)

Attribute	1900	2900	ME3400	3500	3550	3560	3750	3750ME	4000	4500	4900	4924ME	5000	6500 CatOS	6500 IOS	6524ME	ME 3600X	ME 3800X	Nexus 7000	Nexus 5000	Nexus 1000v	ACE 4700	SCE
Discard and Received Input Data Counters																							
Dropped and Forward Output Data Counters																							
Ingress Traffic Descriptor																							
Egress Traffic Descriptor																							
Administrative Status																							
Operational Status																							
IANA Type																							
Containing CTPs																							
Contained CTPs																							
IMO Name—IFRTrafficDescriptor																							
Committed Rate																							
Excess Burst Rate																							
Name																							
Index																							
IMO Name—IFrameRelayLogicalPort/Trunk																							
Admin Status																							
Oper Status																							
Same as IFrameRelay																							
IMO Name—IFrTrunkVc																							
Destination Description																							
Same as IFrVc																							
IMO Name—IEncapsulation																							
Virtual Connection Interface														Y									
Binding Information																							
IMO Name—IFramerelayLogicalPort/Trunk																							
Admin Status																							
Oper Status																							
Same as IFrameRelay																							

PPP

Table 7-90 PPP Attribute Support on Cisco Switches—Cisco Prime Network 3.9

Attribute	1900	2900	ME3400	3500	3550	3560	3750	3750ME	4000	4500	4900	4924ME	5000	6500 CatOS	6500 IOS	6524ME	ME 3600X	ME 3800X	Nexus 7000	Nexus 5000	Nexus 1000v	ACE 4700	SCE
IMO Name—IVcBasedEncapsulation																							
Virtual Connection																							
Binding Information																							
Binding Status														Y									
IANA Type														Y									
Containing CTPs																							
Contained CTPs																							
IMO Name—IMLPPP																							
InterfaceName																							
GroupNumber																							
MTU																							
FragmentDelay																							
FragmentDisable																							
FragmentMaximum																							
FragmentSize																							
Interleave																							
Keepalive																							
KeepaliveTime																							
KeepaliveRetry																							
ActiveLink																							
MinimumConfiguredLink																							
MaximumConfiguredLink																							
LocalMRRU																							
RemoteMRRU																							
LoadThreshold																							
LCPStatus																							
AdminStatus																							
OperStatus																							

HDLC

Table 7-91 HDLC Attribute Support on Cisco Switches—Cisco Prime Network 3.9

Attribute	1900	2900	ME3400	3500	3550	3560	3750	3750ME	4000	4500	4900	4924ME	5000	6500 CatOS	6500 IOS	6524ME	ME 3600X	ME 3800X	Nexus 7000	Nexus 5000	Nexus 1000v	ACE 4700	SCE
IMO Name—IEncapsulation (HDLC/PPP)																							
Virtual Connection																							
Binding Information															Y								
Binding Status															Y								
IANA Type															Y								
Containing CTPs																							
Contained CTPs																							

SONET/SDH

Table 7-92 SONET/SDH Attribute Support on Cisco Switches—Cisco Prime Network 3.9

Attribute	1900	2900	ME3400	3500	3550	3560	3750	3750ME	4000	4500	4900	4924ME	5000	6500 CatOS	6500 IOS	6524ME	ME 3600X	ME 3800X	Nexus 7000	Nexus 5000	Nexus 1000v	ACE 4700	SCE
IMO Name—ISonetSdh																							
Specific Type																							
Loopback Type															Y								
Scrambling Mode															Y								
Same as IPhysicalLayer																							
TCAThresholdB1																							
TCAThresholdB2																							
TCAThresholdB3																							
clocking																							
IMO Name—IDS1PdhChannelized																							
Au4Number																							
Au3Number																							
Sts1Number																							
Tug3Number																							
Tug2Number																							
VtNumber																							

Table 7-92 SONET/SDH Attribute Support on Cisco Switches—Cisco Prime Network 3.9 (continued)

Attribute	1900	2900	ME3400	3500	3550	3560	3750	3750ME	4000	4500	4900	4924ME	5000	6500 CatOS	6500 IOS	6524ME	ME 3600X	ME 3800X	Nexus 7000	Nexus 5000	Nexus 1000v	ACE 4700	SCE
C11Number																							
C12Number																							
Vt15Number																							
Vt2Number																							
T1Number																							
E1Number																							
PathType																							
Description																							
IMO Name—ISonetSdhHop																							
Description																							
AppliqueType																							
PathType																							
IMO Name—ISonetSts1																							
Sts1Number																							
IMO Name—ISdhAu4																							
Au4Number																							
IMO Name—ISdhAu3																							
Au3Number																							

TDM/DSx

Table 7-93 TDM/DSx Attribute Support on Cisco Switches—Cisco Prime Network 3.9

Attribute	1900	2900	ME3400	3500	3550	3560	3750	3750ME	4000	4500	4900	4924ME	5000	6500 CatOS	6500 IOS	6524ME	ME 3600X	ME 3800X	Nexus 7000	Nexus 5000	Nexus 1000v	ACE 4700	SCE
IMO Name—IDS0Bundle																							
Bundled Time Slots															Y								
Bundle Location																							
IANA Type															Y								
Containing CTPs																							
Contained CTPs																							
AdminStatus																							
OperStatus																							

Table 7-93 TDM/DSx Attribute Support on Cisco Switches—Cisco Prime Network 3.9 (continued)

Attribute	1900	2900	ME3400	3500	3550	3560	3750	3750ME	4000	4500	4900	4924ME	5000	6500 CatOS	6500 IOS	6524ME	ME 3600X	ME 3800X	Nexus 7000	Nexus 5000	Nexus 1000v	ACE 4700	SCE
IMO Name—IDS1Pdh / IDS3Pdh																							
Framing Type																							
Cell Mapping Type																							
Loopback Type															Y								
Scrambling Mode															Y								
Same as IPhysicalLayer																							
portDescription																							
internationalBit																							
nationalBits																							
framing																							
lineCode																							
cableLength																							
recoveredClockingId																							
clocking																							
loopback																							
alarmState																							
IMO Name—IClockService																							
ActiveClockSource																	Y	Y					
NcsMode																	Y	Y					
HoldTimeout																	Y	Y					
UseStratum4																	Y	Y					
Mode																	Y	Y					
NcsPriorityList																	Y	Y					
PtpService																	Y	Y					
ClockSourceTable																	Y	Y					
PseudowireClockRecovery																	Y	Y					
SynchronousEthernet																	Y	Y					
IMO Name—IClockSource																							
Priority																	Y	Y					
Source																	Y	Y					
Status																	Y	Y					
Type																	Y	Y					
IMO Name—IPtpService																							
Mode																							

Table 7-93 TDM/DSx Attribute Support on Cisco Switches—Cisco Prime Network 3.9 (continued)

Attribute	1900	2900	ME3400	3500	3550	3560	3750	3750ME	4000	4500	4900	4924ME	5000	6500 CatOS	6500 IOS	6524ME	ME 3600X	ME 3800X	Nexus 7000	Nexus 5000	Nexus 1000v	ACE 4700	SCE
ClockId																							
Domain																							
Priority1																							
Priority2																							
PtpEnabled																							
PtpInterfaceList																							
ptpState																							
IMO Name—IPtpInterface																							
Version																							
AnnounceInterval																							
AnnounceTimeout																							
DestinationAddress																							
SourceAddress																							
DelayReq																							
MasterMode																							
SlaveMode																							
SyncInterval																							
SyncLimit																							
InterfaceXid																							
Role																							
Transport																							
State																							
IMO Name—IACRService																							
RecoveredClockSource																							
RecoveredClockMode																							
CemInterface																							
RecoveredClockList																							
IMO Name—IRecoveredClock																							
ClockId																							
RecoveredClockMode																							
Port																							
Cem																							
Status																							
FrequencyOffset																							

Table 7-93 TDM/DSx Attribute Support on Cisco Switches—Cisco Prime Network 3.9 (continued)

Attribute	1900	2900	ME3400	3500	3550	3560	3750	3750ME	4000	4500	4900	4924ME	5000	6500 CatOS	6500 IOS	6524ME	ME 3600X	ME 3800X	Nexus 7000	Nexus 5000	Nexus 1000v	ACE 4700	SCE
CEMGroupId																							
CEMInterfaceName																							
TransferType																							
IMO Name—ICEMEncap																							
cemIfName																							
IMO Name—ICEMGroup																							
IdlePattern																							
IdleCAS																							
DeJitter																							
PayloadSize																							
RTP																							
RTPHeader																							
TimeSlots																							
AdminStatus																							
OperStatus																							
IMO Name—ISyncE																							
synchronousMode																	Y	Y					
equipmentClock																	Y	Y					
clockMode																	Y	Y					
ssmOption																	Y	Y					
esmcMode																	Y	Y					
holdOffTimer																	Y	Y					
waitToRestore																	Y	Y					
Revertive																	Y	Y					
IMO Name—ISyncEInterface																							
InterfaceName																							
selectionInput																	Y	Y					
ingressESMCMode																	Y	Y					
egressESMCMode																	Y	Y					
ingressQLMode																	Y	Y					
ingressQuality																	Y	Y					
egressQLMode																	Y	Y					
egressQuality																	Y	Y					
waitToRestore																	Y	Y					

Table 7-93 TDM/DSx Attribute Support on Cisco Switches—Cisco Prime Network 3.9 (continued)

Attribute	1900	2900	ME3400	3500	3550	3560	3750	3750ME	4000	4500	4900	4924ME	5000	6500 CatOS	6500 IOS	6524ME	ME 3600X	ME 3800X	Nexus 7000	Nexus 5000	Nexus 1000v	ACE 4700	SCE
holdOffTimer																	Y	Y					
ingressConfQuality																	Y	Y					
egressConfQuality																	Y	Y					
Priority																	Y	Y					
ingressSSM																	Y	Y					
egressSSM																	Y	Y					
clockModeStr																	Y	Y					

MPLS

Table 7-94 MPLS Attribute Support on Cisco Switches—Cisco Prime Network 3.9

Attribute	1900	2900	ME3400	3500	3550	3560	3750	3750ME	4000	4500	4900	4924ME	5000	6500 CatOS	6500 IOS	6524ME	ME 3600X	ME 3800X	Nexus 7000	Nexus 5000	Nexus 1000v	ACE 4700	SCE
IMO Name—IMpls																							
Distribution Protocol								Y							Y	Y	Y	Y					
LabelStack																							
TopLabel																							
Outer and Inner Labels																							
Traffic Engineering Properties								Y							Y	Y	Y	Y					
Resource reservation Properties																							
IANA Type								Y							Y		Y	Y					
Containing CTPs																							
Contained CTPs																							
IMO Name—ILse																							
MPLS Table								Y							Y	Y	Y	Y					
MPLS Aggregate Table								Y							Y	Y	Y	Y					
MPLS Tunnel Segments								Y									Y	Y					
LDP Service								Y									Y	Y					
Logical Sons								Y							Y	Y	Y	Y					

Table 7-94 MPLS Attribute Support on Cisco Switches—Cisco Prime Network 3.9 (continued)

Attribute	1900	2900	ME3400	3500	3550	3560	3750	3750ME	4000	4500	4900	4924ME	5000	6500 CatOS	6500 IOS	6524ME	ME 3600X	ME 3800X	Nexus 7000	Nexus 5000	Nexus 1000v	ACE 4700	SCE
IMO Name—ILdpService																							
Local Identification Status								Y									Y	Y					
LDP Peers								Y							Y	Y	Y	Y					
IMO Name—ILdpPeer																							
Peer Identification								Y							Y	Y	Y	Y					
Transport Address								Y							Y	Y	Y	Y					
Distribution Method								Y							Y	Y	Y	Y					
Protocol Type								Y									Y	Y					
Path Vector Limit								Y							Y	Y	Y	Y					
Session Status								Y							Y	Y	Y	Y					
Protocol Version Hold Time															Y	Y							
Hold Time								Y							Y	Y	Y	Y					
Keep Alive Time															Y	Y							
Peer Discovery Sources								Y							Y	Y	Y	Y					
IMO Name—ILdpDiscoverySource																							
Interface Name								Y							Y	Y	Y	Y					
Source Address								Y							Y	Y	Y	Y					
Type								Y							Y	Y	Y	Y					
IMO Name—IMplsEntry																							
Incoming Label								Y							Y	Y	Y	Y					
Outgoing Interface and Label								Y							Y	Y	Y	Y					
Switching Action								Y							Y	Y	Y	Y					
Next Hop IP Address								Y							Y	Y	Y	Y					
Destination Mask								Y							Y	Y	Y	Y					
Destination address								Y							Y	Y	Y	Y					
IMO Name—IMplsAggregateEntry																							
Virtual Routing Entity								Y							Y	Y	Y	Y					
Incoming Label								Y							Y	Y	Y	Y					
Outgoing Interface and Label								Y							Y	Y	Y	Y					
Switching Action								Y							Y	Y	Y	Y					
Next Hop IP Address								Y							Y	Y	Y	Y					

Table 7-94 MPLS Attribute Support on Cisco Switches—Cisco Prime Network 3.9 (continued)

Attribute	1900	2900	ME3400	3500	3550	3560	3750	3750ME	4000	4500	4900	4924ME	5000	6500 CatOS	6500 IOS	6524ME	ME 3600X	ME 3800X	Nexus 7000	Nexus 5000	Nexus 1000v	ACE 4700	SCE
IMO Name—IMplsLabelRange																							
Type								Y									Y	Y					
minValue								Y									Y	Y					
MaxValue								Y									Y	Y					

MPLS-TE

Table 7-95 MPLS-TE Attribute Support on Cisco Switches—Cisco Prime Network 3.9

Attribute	1900	2900	ME3400	3500	3550	3560	3750	3750ME	4000	4500	4900	4924ME	5000	6500 CatOS	6500 IOS	6524ME	ME 3600X	ME 3800X	Nexus 7000	Nexus 5000	Nexus 1000v	ACE 4700	SCE
IMO Name—IMplsTETunnel																							
Destination Address								Y							Y	Y	Y	Y					
Outgoing Interface and Label								Y							Y	Y	Y	Y					
LSP Identification								Y							Y	Y	Y	Y					
Requested Bandwidth								Y							Y	Y	Y	Y					
Measured Average Burst and Peak Bandwidth								Y							Y	Y	Y	Y					
Setup and Hold Priority								Y							Y	Y	Y	Y					
Affinity Bits and Mask								Y							Y	Y	Y	Y					
Automatic Route Announcement Status								Y							Y	Y	Y	Y					
Optimization Lock Down Status								Y							Y	Y	Y	Y					
Path Option								Y							Y	Y	Y	Y					
Name								Y							Y	Y	Y	Y					
Description								Y							Y	Y	Y	Y					
Administrative Status								Y							Y	Y	Y	Y					
Operational Status								Y							Y	Y	Y	Y					
IANA Type								Y							Y	Y	Y	Y					
is FRR Enabled																	Y	Y					
TunnelType								Y									Y	Y					

Table 7-95 MPLS-TE Attribute Support on Cisco Switches—Cisco Prime Network 3.9 (continued)

Attribute	1900	2900	ME3400	3500	3550	3560	3750	3750ME	4000	4500	4900	4924ME	5000	6500 CatOS	6500 IOS	6524ME	ME 3600X	ME 3800X	Nexus 7000	Nexus 5000	Nexus 1000v	ACE 4700	SCE
DestinationAddress								Y									Y	Y					
Sub Lsp Status								Y									Y	Y					
OutInterface																							
OutLabel																							
TunnelAffinity																							
TunnelAffinityMask																							
TunnelAutoRoute								Y									Y	Y					
TunnelBandwidthKbps																							
TunnelAverageRateKbps																							
TunnelBurstKbps																							
TunnelPeakRateKbps																							
TunnelSetupPriority																							
TunnelHoldPriority																							
TunnelLockdown																							
TunnelPolicyClass																							
P2MPDestinations								Y									Y	Y					
IMO Name—IMplsTEProperties																							
Administrative Weight								Y							Y	Y	Y	Y					
Attributes Identifier																Y							
Signaling Protocol								Y							Y		Y	Y					
Available Physical and Reservable Bandwidth								Y							Y	Y	Y	Y					
Reserved Bandwidth								Y							Y	Y	Y	Y					
IMO Name—IMplsTEPropertiesAllocationEntry																							
Priority Level																							
Allocated and Cumulative Bandwidth																							
IMO Name—IMplsTESegment																							
Segment Type								Y							Y	Y							
Measured Average Burst and Peak Bandwidth								Y							Y	Y							
LSP Identification								Y							Y	Y							
Name								Y							Y	Y							
FRRTunnelName																	Y	Y					
FRRTunnelState																	Y	Y					

Table 7-95 MPLS-TE Attribute Support on Cisco Switches—Cisco Prime Network 3.9 (continued)

Attribute	1900	2900	ME3400	3500	3550	3560	3750	3750ME	4000	4500	4900	4924ME	5000	6500 CatOS	6500 IOS	6524ME	ME 3600X	ME 3800X	Nexus 7000	Nexus 5000	Nexus 1000v	ACE 4700	SCE
AverageBandwidth								Y							Y	Y							
In Interface								Y							Y	Y							
Out interface								Y							Y	Y							
In Label								Y							Y	Y							
Out Label								Y							Y	Y							
Source address								Y							Y	Y							
Destination address								Y							Y	Y							
TunnelType								Y															

VPN (VRF)

Table 7-96 VPN (VRF) Attribute Support on Cisco Switches—Cisco Prime Network 3.9

Attribute	1900	2900	ME3400	3500	3550	3560	3750	3750ME	4000	4500	4900	4924ME	5000	6500 CatOS	6500 IOS	6524ME	ME 3600X	ME 3800X	Nexus 7000	Nexus 5000	Nexus 1000v	ACE 4700	SCE
IMO Name—IVrf																							
Virtual Routing Table						Y		Y							Y	Y	Y	Y	Y				
Exported Route Targets						Y		Y							Y	Y	Y	Y					
Imported Route Targets						Y		Y							Y	Y	Y	Y					
Route Distinguisher						Y		Y							Y	Y	Y	Y					
ARP Entity						Y		Y							Y	Y	Y	Y	Y				
Name						Y		Y							Y	Y	Y	Y	Y				
Logical Sons						Y		Y							Y	Y	Y	Y					
Description																	Y	Y					
Import Route-Map																	Y	Y					
Export Route-Map																	Y	Y					
IMO Name—IVrfEntry																							
Next Hop BGP Address						Y		Y							Y	Y	Y	Y					
Incoming and Outgoing Inner Label						Y		Y							Y	Y	Y	Y					
Outer Label						Y		Y							Y	Y	Y	Y					
Destination IP Subnet						Y		Y							Y	Y	Y	Y	Y				
Next Hop IP Address						Y		Y							Y	Y	Y	Y	Y				

Table 7-96 VPN (VRF) Attribute Support on Cisco Switches—Cisco Prime Network 3.9 (continued)

Attribute	1900	2900	ME3400	3500	3550	3560	3750	3750ME	4000	4500	4900	4924ME	5000	6500 CatOS	6500 IOS	6524ME	ME 3600X	ME 3800X	Nexus 7000	Nexus 5000	Nexus 1000v	ACE 4700	SCE
Type						Y		Y							Y	Y	Y	Y					
Routing Protocol Type						Y		Y							Y	Y	Y	Y	Y				
Outgoing Interface Name						Y		Y							Y	Y	Y	Y	Y				
IMO Name—IMpBgp																							
BGP Identifier						Y		Y		Y	Y	Y			Y	Y	Y	Y	Y				
Local Autonomous System						Y		Y		Y	Y	Y			Y	Y	Y	Y	Y				
Cross Virtual Routing Table								Y									Y	Y					
BGP Neighbors						Y		Y		Y	Y	Y				Y	Y	Y	Y				
Logical Sons						Y		Y							Y	Y	Y	Y					
IMO Name—ICrossVrf																							
Virtual Routing Entries								Y									Y	Y					
Virtual Routing Entity Name								Y									Y	Y					
IMO Name—ICrossVrfRoutingEntry																							
Outgoing Virtual Routing Entity Identifier																							
Incoming and Outgoing Virtual Routing Tags																							
Destination IP Subnet								Y							Y	Y	Y	Y					
Next Hop IP Address								Y							Y	Y	Y	Y					
Type								Y							Y	Y	Y	Y					
Routing Protocol Type								Y							Y	Y	Y	Y					
Outgoing Interface Name																							

PWE3

Table 7-97 PWE3 Attribute Support on Cisco Switches—Cisco Prime Network 3.9

Attribute	1900	2900	ME3400	3500	3550	3560	3750	3750ME	4000	4500	4900	4924ME	5000	6500 CatOS	6500 IOS	6524ME	ME 3600X	ME 3800X	Nexus 7000	Nexus 5000	Nexus 1000v	ACE 4700	SCE
IMO Name—IPTPLayer2MplsTunnel																							
Local and Remote Router Addresses								Y							Y	Y	Y	Y					

Table 7-97 PWE3 Attribute Support on Cisco Switches—Cisco Prime Network 3.9 (continued)

Attribute	1900	2900	ME3400	3500	3550	3560	3750	3750ME	4000	4500	4900	4924ME	5000	6500 CatOS	6500 IOS	6524ME	ME 3600X	ME 3800X	Nexus 7000	Nexus 5000	Nexus 1000v	ACE 4700	SCE
Local and Remote Virtual Connection Labels								Y							Y	Y	Y	Y					
Tunnel Identification								Y							Y	Y	Y	Y					
Tunnel Status								Y							Y	Y	Y	Y					
Local and Remote Tunnel Interface																Y							
IANA Type								Y							Y	Y	Y	Y					
Containing CTPs																							
Contained CTPs																							
PsuedowireType								Y							Y		Y	Y					
PreferredPathTunnel								Y							Y		Y	Y					
LocalMTU								Y							Y		Y	Y					
RemoteMTU								Y							Y		Y	Y					
PeerStatus								Y							Y		Y	Y					
SignalingProtocol								Y							Y		Y	Y					
VFIName								Y							Y		Y	Y					
psuedowireRole								Y															
PeerRouterIp																							
LocalRouterIp																							
LocalVcLabel																							
PeerVcLabel																							

Security

Table 7-98 Security Attribute Support on Cisco Switches—Cisco Prime Network 3.9

Attribute	1900	2900	ME3400	3500	3550	3560	3750	3750ME	4000	4500	4900	4924ME	5000	6500 CatOS	6500 IOS	6524ME	ME 3600X	ME 3800X	Nexus 7000	Nexus 5000	Nexus 1000v	ACE 4700	SCE
IMO Name—IAccessList																							
Type		Y	Y					Y		Y [1]	Y [2]	Y			Y	Y	Y	Y					
Access List Entries		Y	Y					Y		Y [3]	Y [4]	Y			Y	Y	Y	Y					

Table 7-98 Security Attribute Support on Cisco Switches—Cisco Prime Network 3.9 (continued)

Attribute	1900	2900	ME3400	3500	3550	3560	3750	3750ME	4000	4500	4900	4924ME	5000	6500 CatOS	6500 IOS	6524ME	ME 3600X	ME 3800X	Nexus 7000	Nexus 5000	Nexus 1000v	ACE 4700	SCE
Name or Id		Y	Y					Y		Y [5]	Y [6]	Y			Y	Y	Y	Y					
Index		Y	Y					Y		Y [7]	Y [8]	Y			Y	Y	Y	Y					
IMO Name—IAccessListEntry																							
Entry Identification		Y	Y					Y		Y [9]	Y [10]	Y			Y	Y	Y	Y					
Action Logic		Y	Y					Y		Y [11]	Y [12]	Y			Y	Y	Y	Y					
Source and Destination Address		Y	Y					Y		Y [13]	Y [14]	Y			Y	Y	Y	Y					
Source and Destination Wildcard		Y	Y					Y		Y [15]	Y [16]	Y			Y	Y	Y	Y					
Protocol Type		Y	Y					Y		Y [17]	Y [18]	Y			Y	Y	Y	Y					
Source and Destination Port Ranges		Y	Y					Y		Y [19]	Y [20]	Y			Y	Y	Y	Y					
Source and Destination Port Action		Y	Y					Y		Y [21]	Y [22]	Y			Y	Y	Y	Y					
Protocol Specific Info		Y	Y					Y		Y [23]	Y [24]	Y			Y	Y	Y	Y					
Differential Services Code Points		Y	Y					Y		Y [25]	Y [26]	Y			Y	Y	Y	Y					
Type of Service		Y	Y					Y		Y [27]	Y [28]	Y			Y	Y	Y	Y					
Precedence		Y	Y					Y		Y [29]	Y [30]	Y			Y	Y	Y	Y					
Matches		Y	Y					Y		Y [31]	Y [32]	Y			Y	Y	Y	Y					

[1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16] Supported for 4503E, 4507RE, 4507, and 4506E only.

[17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 31, 32] Validated with 12.2(52)SG only.

Hardware

Table 7-99 Hardware Attribute Support on Cisco Switches—Cisco Prime Network 3.9

Attribute	1900	2900	ME3400	3500	3550	3560	3750	3750ME	4000	4500	4900	4924ME	5000	6500 CatOS	6500 IOS	6524ME	ME 3600X	ME 3800X	Nexus 7000	Nexus 5000	Nexus 1000v	ACE 4700	SCE
IMO Name—IChassis																							
Description			Y [1]			Y		Y	Y	Y	Y	Y		Y	Y	Y	Y	Y	Y	Y	Y	Y	
Equipment Holder Type				Y				Y	Y	Y						Y	Y	Y	Y	Y	Y	Y	Y
Contained Equipment Holders																							
Contained Equipments																							
Serial Number		Y	Y	Y		Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	
IMO Name—IShelf																							
Description																							
Status																							
Equipment Holder Type																							
Contained Equipment Holders																							
Contained Equipments																							
Serial Number																							
IMO Name—IModule																							
Module Name		Y	Y	Y	Y	Y	Y	Y		Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y
Module Description			Y	Y	Y	Y	Y	Y		Y	Y	Y	Y	Y	Y	Y	Y [2]	Y [3]	Y	Y	Y	Y	Y
Software Version		Y	Y		Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y
Operational Status		Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y
Hardware Type + Version		Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y
Managed IP Address																							
Redundant Equipment																							
Configured Redundancy										Y									Y	Y			
Redundancy Status				Y	Y	Y	Y			Y					Y	Y			Y	Y		Y	
Operational Status Last Changed			Y	Y	Y	Y		Y	Y	Y	Y	Y			Y	Y	Y	Y	Y	Y		Y	
Supported Physical Termination Points			Y							Y	Y	Y			Y	Y						Y	
Serial Number (soft property)		Y	Y		Y	Y		Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y

Table 7-99 Hardware Attribute Support on Cisco Switches—Cisco Prime Network 3.9 (continued)

Attribute	1900	2900	ME3400	3500	3550	3560	3750	3750ME	4000	4500	4900	4924ME	5000	6500 CatOS	6500 IOS	6524ME	ME 3600X	ME 3800X	Nexus 7000	Nexus 5000	Nexus 1000v	ACE 4700	SCE
Slots Number																							Y
IMO Name—IPowerSupply																							
Same as IModule						Y				Y	Y	Y			Y				Y	Y			
IMO Name—IFanTray																							
Same as IModule						Y				Y	Y	Y			Y				Y	Y			
IMO Name—IPluggableTransceiver																							
ConnectorDescription			Y			Y		Y		Y	Y	Y			Y	Y	Y	Y	Y	Y			
PID			Y			Y		Y		Y	Y	Y			Y	Y	Y	Y	Y	Y			
ConnectorSerialNumber			Y			Y		Y		Y	Y	Y			Y	Y	Y	Y	Y	Y			
ConnectorType			Y			Y		Y		Y	Y	Y			Y	Y	Y	Y	Y	Y			
PluggablePortState			Y			Y		Y		Y	Y	Y			Y	Y	Y	Y	Y	Y			
PluggableType			Y			Y		Y		Y	Y	Y			Y	Y	Y	Y	Y	Y			
IMO Name—IManagedElement																							
IP Address		Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y
Communication State		Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y
Investigation State		Y	Y	Y	Y	Y		Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y
Element Category		Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y
Element Type and Key		Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y
Device Name		Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y [4]	Y [5]	Y	Y	Y	Y	Y
System Name		Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y
System Description	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y
Up Time		Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y
Software Version	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y
Vendor Identity		Y	Y	Y	Y	Y	Y	Y		Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y
Memory and CPU Usage		Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	
DRAM Free	Y	Y	Y	Y		Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y		Y		
DRAM Used	Y	Y	Y	Y		Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y		Y		
DRAM Usage	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y			
Flash Device Size		Y	Y	Y		Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y			Y	Y			
NVRAM Size		Y	Y	Y		Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y				
Processor DRAM		Y	Y	Y		Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y				
Sys Contact	Y	Y	Y	Y		Y	Y	Y	Y	Y	Y	Y		Y	Y	Y	Y	Y	Y	Y	Y	Y	Y
Sys Location	Y	Y	Y	Y		Y	Y	Y	Y	Y	Y	Y		Y	Y	Y	Y	Y	Y	Y	Y	Y	Y

Table 7-99 Hardware Attribute Support on Cisco Switches—Cisco Prime Network 3.9 (continued)

Attribute	1900	2900	ME3400	3500	3550	3560	3750	3750ME	4000	4500	4900	4924ME	5000	6500 CatOS	6500 IOS	6524ME	ME 3600X	ME 3800X	Nexus 7000	Nexus 5000	Nexus 1000v	ACE 4700	SCE
Serial Number		Y	Y	Y		Y	Y	Y	Y	Y	Y	Y		Y	Y	Y	Y	Y	Y	Y	Y	Y	
File Systems																							
IMO Name—IContext																							
Name					Y	Y		Y								Y						Y	
Bounded Connections																							
IP Address Pools																							
Forwarding Components List																							
Traffic Descriptors List																							
Tunnel Containers List																							
Data Link Aggregation Containers List																							
IMO Name—ISystemService																							
Type																							
Status																							
Up Time		Y	Y	Y	Y	Y	Y	Y	Y	Y				Y	Y	Y						Y	
IMO Name—IBridge																							
Bridge Table		Y	Y		Y	Y		Y	Y	Y	Y	Y		Y	Y	Y	Y	Y	Y				
Type		Y	Y		Y	Y		Y		Y	Y	Y		Y	Y	Y	Y	Y	Y				
MAC Address		Y	Y		Y	Y		Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y				
IP Interface		Y			Y	Y		Y	Y	Y			Y		Y	Y	Y	Y	Y				
Name		Y	Y		Y	Y			Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y				
Logical Sons		Y	Y		Y	Y			Y	Y	Y	Y		Y	Y	Y	Y	Y					
Vlan Type			Y																				
IMO Name—IBridgeEntry																							
Destination MAC		Y	Y		Y	Y		Y	Y	Y	Y	Y		Y	Y	Y	Y	Y	Y				
Outgoing Interface			Y					Y			Y	Y		Y	Y	Y	Y	Y	Y				

[1]Supported for 12.2(50)SE only.

[2, 4]"show interfaces switchport" command will be used to get PortMode

[3, 5]Device Name is Mapped to Element Name in GUI

Serial

Table 7-100 Serial Attribute Support on Cisco Switches—Cisco Prime Network 3.9

Attribute	1900	2900	ME3400	3500	3550	3560	3750	3750ME	4000	4500	4900	4924ME	5000	6500 CatOS	6500 IOS	6524ME	ME 3600X	ME 3800X	Nexus 7000	Nexus 5000	Nexus 1000v	ACE 4700	SCE
IMO Name—IPhysicalLayer																							
Media Type		Y	Y	Y	Y	Y	Y	Y		Y		Y	Y	Y	Y	Y			Y	Y	Y	Y	Y
Clocking Source															Y	Y						Y	
Maximum Speed	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y			Y	Y	Y	Y	Y
Is Internal Port		Y	Y	Y	Y	Y	Y	Y		Y				Y	Y	Y			Y	Y	Y	Y	
Discarded Bandwidth																							
Dropped Bandwidth																							
Input Bandwidth																							
Output Bandwidth																							
Discarded and Received Input Data Counters		Y		Y	Y	Y	Y	Y	Y	Y				Y	Y	Y						Y	
Dropped and Forward Output Data Counters		Y		Y	Y	Y	Y	Y	Y	Y				Y	Y	Y						Y	
Administrative Status	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y			Y	Y	Y	Y	Y
Operational Status	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y			Y	Y	Y	Y	Y
Last Changed	Y	Y		Y	Y	Y	Y	Y	Y	Y			Y	Y	Y	Y						Y	Y
IANA Type		Y		Y	Y	Y	Y	Y		Y				Y	Y	Y						Y	
Containing CTPs																							
Contained CTPs																							
Port Alias	Y	Y	Y	Y		Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y			Y	Y	Y	Y	Y
Location	Y	Y	Y	Y		Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y			Y	Y	Y	Y	Y
Sending Alarms	Y	Y	Y	Y		Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y			Y	Y	Y	Y	Y
Connector Description		Y	Y	Y		Y	Y	Y	Y	Y	Y	Y		Y	Y	Y			Y	Y		Y	
Part ID		Y	Y	Y		Y	Y	Y	Y	Y	Y	Y		Y	Y	Y			Y	Y		Y	
Connector Serial Num		Y	Y	Y		Y	Y	Y	Y	Y	Y	Y		Y	Y	Y			Y	Y		Y	
Product		Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y		Y	Y	Y			Y	Y	Y	Y	Y
Status		Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y			Y	Y	Y	Y	Y
Managed		Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y			Y	Y	Y	Y	Y

Additional Technologies

Table 7-101 Additional Technologies Attribute Support on Cisco Switches—Cisco Prime Network 3.9

Attribute	1900	2900	ME3400	3500	3550	3560	3750	3750ME	4000	4500	4900	4924ME	5000	6500 CatOS	6500 IOS	6524ME	ME 3600X	ME 3800X	Nexus 7000	Nexus 5000	Nexus 1000v	ACE 4700	SCE
IMO Name—POS																							
POS			Y		Y	Y		Y			Y	Y			Y	Y							

LocalSwitching

Table 7-102 LocalSwitching Attribute Support on Cisco Switches—Cisco Prime Network 3.9

Attribute	1900	2900	ME3400	3500	3550	3560	3750	3750ME	4000	4500	4900	4924ME	5000	6500 CatOS	6500 IOS	6524ME	ME 3600X	ME 3800X	Nexus 7000	Nexus 5000	Nexus 1000v	ACE 4700	SCE
IMO Name—ILocalSwitchingEntity																							
LocalSwitchingTable								Y							Y								
PWSwitchingTable																	Y	Y					
IMO Name—ILocalSwitchingEntry																							
Local Switching Entry Key								Y							Y		Y	Y					
Local Switching Entry Status								Y							Y		Y	Y					
Segment 1								Y							Y		Y	Y					
Segment 1 Port Name								Y							Y		Y	Y					
Segment 1 Status								Y							Y		Y	Y					
Segment 2								Y							Y		Y	Y					
Segment 2 Port Name								Y							Y		Y	Y					
Segment 2 Status								Y							Y		Y	Y					

BFD

Table 7-103 BFD Attribute Support on Cisco Switches—Cisco Prime Network 3.9

Attribute	1900	2900	ME3400	3500	3550	3560	3750	3750ME	4000	4500	4900	4924ME	5000	6500 CatOS	6500 IOS	6524ME	ME 3600X	ME 3800X	Nexus 7000	Nexus 5000	Nexus 1000v	ACE 4700	SCE
IMO Name—IBfdService																							
Status								Y							Y		Y	Y					
IMO Name—IBfdCommon																							
RegisteredProtocols								Y							Y		Y	Y					
InterfaceName								Y							Y		Y	Y					
IMO Name—IBfdSession																							
SourceIp								Y							Y		Y	Y					
DestinationIp								Y							Y		Y	Y					
Interval								Y							Y		Y	Y					
Multiplier								Y							Y		Y	Y					
Protocol								Y							Y		Y	Y					
State								Y							Y		Y	Y					
Interface								Y							Y		Y	Y					
Process								Y							Y		Y	Y					

Carrier Ethernet

Table 7-104 Carrier Ethernet Attribute Support on Cisco Switches—Cisco Prime Network 3.9

Attribute	1900	2900	ME3400	3500	3550	3560	3750	3750ME	4000	4500	4900	4924ME	5000	6500 CatOS	6500 IOS	6524ME	ME 3600X	ME 3800X	Nexus 7000	Nexus 5000	Nexus 1000v	ACE 4700	SCE
IMO Name—IVsi																							
vsiInstanceName															Y	Y	Y	Y					
vpnId															Y	Y	Y	Y					
discoveryMode															Y	Y	Y	Y					
vsiMode															Y	Y	Y	Y					
Operational state															Y	Y	Y	Y					
Administrative state															Y	Y	Y	Y					
IMO Name—IPseudowireProperties																							
isSplitHorizonEnabled															Y		Y	Y					

Table 7-104 Carrier Ethernet Attribute Support on Cisco Switches—Cisco Prime Network 3.9 (continued)

Attribute	1900	2900	ME3400	3500	3550	3560	3750	3750ME	4000	4500	4900	4924ME	5000	6500 CatOS	6500 IOS	6524ME	ME 3600X	ME 3800X	Nexus 7000	Nexus 5000	Nexus 1000v	ACE 4700	SCE
isAutoDiscovered															Y		Y	Y					
IMO Name—IVLANTaggedInterface																							
InterfaceName															Y								
Inner Vlan Id															Y								
Outer Vlan Id															Y								
Encap Type															Y								
Operational state															Y								
Administrative state															Y								
ConfiguredDescription															Y								
IMO Name—IEfp																							
EfpId															Y [1]		Y	Y					
RewriteParams															Y [2]								
EncapsParams															Y [3]		Y	Y					
AdminStatus															Y [4]		Y	Y					
OperStatus															Y [5]		Y	Y					
SplitHorizonGroup															Y [6]								
MatchCriteria															Y [7]		Y	Y					
ConfiguredDescription															Y								
GetServiceInstanceId															Y [8]		Y	Y					
SetServiceInstanceId															Y [9]		Y	Y					

[1, 2, 3, 4, 5, 6, 7, 8, 9] For version greater than SRD SNMP is used

LLDP

Table 7-105 LLDP Attribute Support on Cisco Switches—Cisco Prime Network 3.9

Attribute	1900	2900	ME3400	3500	3550	3560	3750	3750ME	4000	4500	4900	4924ME	5000	6500 CatOS	6500 IOS	6524ME	ME 3600X	ME 3800X	Nexus 7000	Nexus 5000	Nexus 1000v	ACE 4700	SCE
IMO Name—ILLDPService																							
status		Y [1]	Y [2]				Y	Y [3]		Y [4]	Y [5]	Y				Y [6]	Y	Y					
lldpAdvertisementsInterval		Y [7]	Y [8]				Y	Y [9]		Y [10]	Y [11]	Y				Y [12]	Y	Y					
lldpHoldTime		Y [13]	Y [14]				Y	Y [15]		Y [16]	Y [17]	Y				Y [18]	Y	Y					
lldpReinitialisationDelay		Y [19]	Y [20]				Y	Y [21]		Y [22]	Y [23]	Y				Y [24]	Y	Y					
localChassisID		Y [25]	Y [26]				Y	Y [27]		Y [28]	Y [29]	Y				Y [30]	Y	Y					
localSystemName		Y [31]	Y [32]				Y	Y [33]		Y [34]	Y [35]	Y				Y [36]	Y	Y					
IMO Name—ILLDPNeighbor																							
localPortName		Y [37]	Y [38]				Y	Y [39]		Y [40]	Y [41]	Y				Y [42]	Y	Y					
remotePortDesc		Y [43]	Y [44]				Y	Y [45]		Y [46]	Y [47]	Y				Y [48]	Y	Y					
remoteChassisId		Y [49]	Y [50]				Y	Y [51]		Y [52]	Y [53]	Y				Y [54]	Y	Y					
remoteManagementIP		Y [55]	Y [56]				Y	Y [57]		Y [58]	Y [59]	Y				Y [60]	Y	Y					
localPortId		Y [61]	Y [62]				Y	Y [63]		Y [64]	Y [65]	Y				Y [66]	Y	Y					
remotePortId		Y [67]	Y [68]				Y	Y [69]		Y [70]	Y [71]	Y				Y [72]	Y	Y					
remoteDeviceId		Y [73]	Y [74]				Y	Y [75]		Y [76]	Y [77]	Y				Y [78]	Y	Y					

1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 31, 32, 33, 34, 35, 36, 37, 38, 39, 40, 41, 42, 43, 44, 45, 46, 47, 48, 49, 50, 51, 52, 53, 54, 55, 56, 57, 58, 59, 60, 61, 62, 63, 64, 65, 66, 67, 68, 69, 70, 71, 72, 73, 74, 75, 76, 77, 78 LLDP links are not modeled properly on IOS version 12.2(51) and earlier IOS versions that support LLDP.This is because the IOS displays the port description in place of local port ID in LLDP Neighbor Table.

CDP

Table 7-106 CDP Attribute Support on Cisco Switches—Cisco Prime Network 3.9

Attribute	1900	2900	ME3400	3500	3550	3560	3750	3750ME	4000	4500	4900	4924ME	5000	6500 CatOS	6500 IOS	6524ME	ME 3600X	ME 3800X	Nexus 7000	Nexus 5000	Nexus 1000v	ACE 4700	SCE
IMO Name—ICdpService																							
cdpHoldtime		Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y		
cdpMessageInterval		Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y		
cdpDeviceId		Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y		
cdpState		Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y		
cdpVersion		Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y		
IMO Name—ICdpNeighbor																							
remoteDeviceId	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y		
remotePortId	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y		
remoteIPAddress	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y		
localPortId	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y		

Discovery Protocol

Table 7-107 Discovery Protocol Attribute Support on Cisco Switches—Cisco Prime Network 3.9

Attribute	1900	2900	ME3400	3500	3550	3560	3750	3750ME	4000	4500	4900	4924ME	5000	6500 CatOS	6500 IOS	6524ME	ME 3600X	ME 3800X	Nexus 7000	Nexus 5000	Nexus 1000v	ACE 4700	SCE
IMO Name—IDiscoveryProtocol																							
DiscoveryProtocolType	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y		Y	Y	Y	Y					
Info	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y		Y	Y	Y	Y					

Ethernet OAM

Table 7-108 Ethernet OAM Attribute Support on Cisco Switches—Cisco Prime Network 3.9

Attribute	1900	2900	ME3400	3500	3550	3560	3750	3750ME	4000	4500	4900	4924ME	5000	6500 CatOS	6500 IOS	6524ME	ME 3600X	ME 3800X	Nexus 7000	Nexus 5000	Nexus 1000v	ACE 4700	SCE
IMO Name—ICfmService																							
cacheSize			Y					Y							Y	Y	Y	Y					
maximumCacheSize			Y					Y							Y	Y	Y	Y					
holdTime			Y					Y							Y	Y	Y	Y					
version			Y					Y							Y	Y	Y	Y					
maintenanceIntermedatePointsTable			Y					Y							Y	Y	Y	Y					
maintenanceDomain			Y					Y							Y	Y	Y	Y					
IMO Name—IMaintenanceDomain																							
name			Y					Y							Y	Y	Y	Y					
level			Y					Y							Y	Y	Y	Y					
Id			Y					Y							Y	Y	Y	Y					
maintenanceAssociation			Y					Y							Y	Y	Y	Y					
IMO Name—IMaintenanceEndPoint																							
macAddress			Y					Y							Y	Y	Y	Y					
Interface			Y					Y							Y	Y	Y	Y					
continuityCheckStatus			Y					Y							Y	Y	Y	Y					
direction			Y					Y							Y	Y	Y	Y					
IMO Name—IMaintenanceAssociation																							
name			Y					Y							Y	Y	Y	Y					
associationType			Y					Y							Y	Y	Y	Y					
maximalMeps			Y					Y							Y	Y	Y	Y					
continuityCheckInterval			Y					Y							Y	Y	Y	Y					
continuityCheckEnable			Y					Y							Y	Y	Y	Y					
crossCheckEnable			Y					Y							Y	Y	Y	Y					
direction			Y					Y							Y	Y	Y	Y					
bridge			Y					Y							Y	Y	Y	Y					
maintenanceEndPoints			Y					Y							Y		Y	Y					
cfmRemoteMaintenanceEndPoints			Y					Y							Y	Y	Y	Y					
IMO Name—IMaintenanceIntermediatePoint																							
level			Y					Y							Y	Y	Y	Y					

Table 7-108 Ethernet OAM Attribute Support on Cisco Switches—Cisco Prime Network 3.9 (continued)

Attribute	1900	2900	ME3400	3500	3550	3560	3750	3750ME	4000	4500	4900	4924ME	5000	6500 CatOS	6500 IOS	6524ME	ME 3600X	ME 3800X	Nexus 7000	Nexus 5000	Nexus 1000v	ACE 4700	SCE
cfmInterface			Y					Y							Y	Y	Y	Y					
isAutocreated			Y					Y							Y	Y	Y	Y					
Vlans			Y					Y							Y	Y	Y	Y					
macAddress			Y					Y							Y	Y	Y	Y					
IMO Name—IRemoteMaintenanceEndPoint																							
mepId			Y					Y							Y	Y	Y	Y					
macAddress			Y					Y							Y	Y	Y	Y					
level			Y					Y							Y	Y	Y	Y					
maintenanceEndPointStatus			Y					Y							Y	Y	Y	Y					
maintenanceEndPointOid			Y					Y							Y	Y	Y	Y					
IMO Name—IOAMData																							
adminState			Y					Y							Y		Y	Y					
pduMaxRate			Y					Y							Y		Y	Y					
pduMinRate			Y					Y							Y		Y	Y					
linkTimeout			Y					Y							Y		Y	Y					
highThresholdAction			Y					Y							Y		Y	Y					
linkFaultAction			Y					Y							Y		Y	Y					
dyingGaspAction			Y					Y							Y		Y	Y					
criticalEventAction			Y					Y							Y		Y	Y					
mode			Y					Y							Y		Y	Y					
unidirectional			Y					Y							Y		Y	Y					
linkMonitor			Y					Y							Y		Y	Y					
remoteLoopback			Y					Y							Y		Y	Y					
portStatus			Y					Y							Y		Y	Y					
loopbackStatus			Y					Y							Y		Y	Y					
remoteData			Y					Y							Y		Y	Y					
name			Y					Y							Y		Y	Y					
ethernetPort			Y					Y							Y		Y	Y					
IMO Name—IOAMRemoteData																							
macAddress			Y					Y							Y		Y	Y					
vendor			Y					Y							Y		Y	Y					
mode			Y					Y							Y		Y	Y					
unidirection			Y					Y							Y		Y	Y					
linkMonitor			Y					Y							Y		Y	Y					

Table 7-108 Ethernet OAM Attribute Support on Cisco Switches—Cisco Prime Network 3.9 (continued)

Attribute	1900	2900	ME3400	3500	3550	3560	3750	3750ME	4000	4500	4900	4924ME	5000	6500 CatOS	6500 IOS	6524ME	ME 3600X	ME 3800X	Nexus 7000	Nexus 5000	Nexus 1000v	ACE 4700	SCE
remoteLoopback			Y					Y							Y		Y	Y					
IMO Name—IUNIProperties																							
UNIId			Y					Y							Y		Y	Y					
isServiceMultiplexing			Y					Y							Y		Y	Y					
isBundlingEnabled			Y					Y							Y		Y	Y					
bundlingType			Y					Y							Y		Y	Y					
IMO Name—IEthernetLMI																							
isGlobalEnabled			Y [1]					Y [2]															
mode			Y [3]					Y [4]															
ELMIInterfaces			Y					Y							Y		Y	Y					
deviceEVCs			Y					Y							Y		Y	Y					
IMO Name—IDeviceEVC																							
EVCName			Y					Y							Y		Y	Y					
EVCStatus			Y					Y							Y		Y	Y					
EVCType			Y					Y							Y		Y	Y					
cfmMaName			Y					Y							Y		Y	Y					
configuredRemoteUNICount			Y					Y							Y		Y	Y					
activeRemoteUNICount			Y					Y							Y		Y	Y					
UNIInterfaces			Y					Y							Y		Y	Y					
IMO Name—IUNIInterfaces																							
UNIStatus			Y					Y							Y		Y	Y					
UNIId			Y					Y							Y		Y	Y					
interfaceName			Y					Y							Y		Y	Y					
vlanList			Y					Y							Y		Y	Y					
lmiLinkStatus			Y					Y							Y		Y	Y					
IMO Name—IELMIInterfaces																							
interfaceName			Y					Y							Y		Y	Y					
T391			Y					Y							Y		Y	Y					
T392			Y					Y							Y		Y	Y					
N391			Y					Y							Y		Y	Y					
N393			Y					Y							Y		Y	Y					

[1, 2, 3, 4]Supported from IOS version 12.2(35)SE onwards



CHAPTER 8

Support Information for Cisco Optical Transport

This chapter contains support information for Virtual Network Elements (VNEs) that manage Cisco optical transport in Cisco Prime Network 3.9.

- Cisco Carrier Packet Transport Series Devices, page 8-1
- Supported Technologies on Cisco Optical Transport, page 8-8

Note For more information about the technologies described in this chapter , see Part 2 Technology Support.

Cisco Carrier Packet Transport Series Devices

This section includes the following information about Cisco CPT Devices optical transport (for information on the NE types supported in Cisco Prime Network 3.9, see Cisco Carrier Packet Transport Series Devices):

- Cisco CPT Devices—Supported Software Versions, page 8-1
- Cisco CPT Devices—Supported Topologies, page 8-2
- Cisco CPT Devices—Supported Modules, page 8-2
- Cisco CPT Devices—Supported Technologies, page 8-6
- Cisco CPT Devices—Supported Service Events, page 8-7

Cisco CPT Devices—Supported Software Versions

Table 8-1 Supported Software Versions for Cisco CPT Devices—Cisco Prime Network 3.9

Software Version	Product_Version
Image 09.30	Prime Network 3.8
Image 09.50	Prime Network 3.8 DP3

Cisco CPT Devices—Supported Topologies

Table 8-2 Supported Topologies for Cisco CPT Devices—Cisco Prime Network 3.9

Topology Type	Link Type	Product_Version
Ethernet	Ethernet	3.6.0
MPLS	MPLS	3.6.0
Physical Layer	Physical Layer	3.6.0
LAG	LAG	3.6.0
BFD	BFD	3.7.1
MPLS-TP	Tunnel	Prime Network 3.8

Cisco CPT Devices—Supported Modules

Table 8-3 Supported Modules for Cisco CPT Devices—Cisco Prime Network 3.9

Module Name	Product_Version	Module Description
POWER-SUPPLY	Prime Network 3.8	4000W DC PS for M6/M2 Chassis
FAN-TRAY	Prime Network 3.8	Fan try for M6/M2 Chassis
TNC	Prime Network 3.8	Transport Node Controller Ethernet PTP for M2, M6 Chassis
TSC	Prime Network 3.8	Transport Shelf Controller Ethernet PTP for M2, M6 Chassis
IO-SLOT	Prime Network 3.8	IO Slot for M6/M2 Chassis
PTF_10GE_LINE_CARD	Prime Network 3.8	Packet Transport Fabric 256G Fabric Card w/ 4x10GE
NGXP	Prime Network 3.8	Next Generation Process Module
PTSA_GE_LINE_CARD	Prime Network 3.8	

Table 8-3 Supported Modules for Cisco CPT Devices—Cisco Prime Network 3.9 (continued)

Module Name	Product_Version	Module Description
OC48AS-IR-1310	Prime Network 3.8	
OC192LR	Prime Network 3.8	
XC10G	Prime Network 3.8	
XFP-10G-MM-SR	Prime Network 3.8	
ONS-XC-10G-S1	Prime Network 3.8	
ONS-SE+-10G-LR	Prime Network 3.8	SFP+ LR - EXT Temp
ONS-SC+-10G-LRM	Prime Network 3.8	SFP+ LRM - Commercial Temp
ONS-SI-GE-EX	Prime Network 3.8	SFP - 100Base EX - I-Temp
ONS-SC-GE-BXU	Prime Network 3.8	SFP-1000Base BX D- GE Bidirectional Downstream C Temp
ONS-SC-GE-BXD	Prime Network 3.8	SFP-1000Base BX D- GE Bidirectional Upstream C Temp
ONS-SC+-10G-ZR	Prime Network 3.8	SFP+ ZR - Commercial Temp
ONS-SC-E1-T1-CES	Prime Network 3.8	SFP - E1/DS1 PDH over FE Pseudowire (w / sync-E) - C-Temp
ONS-SC-E3-T3-CES	Prime Network 3.8	SFP ñ E3/DS3 PDH over FE Pseudowire (w / sync-E) - C-Temp
ONS-SC+-10G-30.3	Prime Network 3.8	10G MR, SFP+ 1530.33, 100 GHz, LC

Table 8-3 Supported Modules for Cisco CPT Devices—Cisco Prime Network 3.9 (continued)

Module Name	Product_Version	Module Description
ONS-SC+-10G-31.1	Prime Network 3.8	10G MR, SFP+ 1531.12, 100 GHz, LC
ONS-SC+-10G-31.9	Prime Network 3.8	10G MR, SFP+ 1531.90, 100 GHz, LC
ONS-SC+-10G-32.6	Prime Network 3.8	10G MR, SFP+ 1532.68, 100 GHz, LC
ONS-SC+-10G-33.4	Prime Network 3.8	10G MR, SFP+ 1533.47, 100 GHz, LC
ONS-SC+-10G-34.2	Prime Network 3.8	10G MR, SFP+ 1534.25, 100 GHz, LC
ONS-SC+-10G-35.0	Prime Network 3.8	10G MR, SFP+ 1535.04, 100 GHz, LC
ONS-SC+-10G-35.8	Prime Network 3.8	10G MR, SFP+ 1535.82, 100 GHz, LC
ONS-SC+-10G-36.6	Prime Network 3.8	10G MR, SFP+ 1536.61, 100 GHz, LC
ONS-SC+-10G-37.4	Prime Network 3.8	10G MR, SFP+ 1537.40, 100 GHz, LC
ONS-SC+-10G-38.1	Prime Network 3.8	10G MR, SFP+ 1538.19, 100 GHz, LC
ONS-SC+-10G-38.9	Prime Network 3.8	10G MR, SFP+ 1538.98, 100 GHz, LC
ONS-SC+-10G-39.7	Prime Network 3.8	10G MR, SFP+ 1539.77, 100 GHz, LC
ONS-SC+-10G-40.5	Prime Network 3.8	10G MR, SFP+ 1540.56, 100 GHz, LC
ONS-SC+-10G-41.3	Prime Network 3.8	10G MR, SFP+ 1541.35, 100 GHz, LC

Table 8-3 Supported Modules for Cisco CPT Devices—Cisco Prime Network 3.9 (continued)

Module Name	Product_Version	Module Description
ONS-SC+-10G-42.1	Prime Network 3.8	10G MR, SFP+ 1542.14, 100 GHz, LC
ONS-SC+-10G-42.9	Prime Network 3.8	10G MR, SFP+ 1542.94, 100 GHz, LC
ONS-SC+-10G-43.7	Prime Network 3.8	10G MR, SFP+ 1543.73, 100 GHz, LC
ONS-SC+-10G-44.5	Prime Network 3.8	10G MR, SFP+ 1544.53, 100 GHz, LC
ONS-SC+-10G-45.3	Prime Network 3.8	10G MR, SFP+ 1545.32, 100 GHz, LC
ONS-SC+-10G-46.1	Prime Network 3.8	10G MR, SFP+ 1546.12, 100 GHz, LC
ONS-SC+-10G-46.9	Prime Network 3.8	10G MR, SFP+ 1546.92, 100 GHz, LC
ONS-SC+-10G-47.7	Prime Network 3.8	10G MR, SFP+ 1547.72, 100 GHz, LC
ONS-SC+-10G-48.5	Prime Network 3.8	10G MR, SFP+ 1548.51, 100 GHz, LC
ONS-SC+-10G-49.3	Prime Network 3.8	10G MR, SFP+ 1549.32, 100 GHz, LC
ONS-SC+-10G-50.1	Prime Network 3.8	10G MR, SFP+ 1550.12, 100 GHz, LC
ONS-SC+-10G-50.9	Prime Network 3.8	10G MR, SFP+ 1550.92, 100 GHz, LC
ONS-SC+-10G-51.7	Prime Network 3.8	10G MR, SFP+ 1551.72, 100 GHz, LC
ONS-SC+-10G-52.5	Prime Network 3.8	10G MR, SFP+ 1552.52, 100 GHz, LC

Table 8-3 Supported Modules for Cisco CPT Devices—Cisco Prime Network 3.9 (continued)

Module Name	Product_Version	Module Description
ONS-SC+-10G-53.3	Prime Network 3.8	10G MR, SFP+ 1553.33, 100 GHz, LC
ONS-SC+-10G-54.1	Prime Network 3.8	10G MR, SFP+ 1554.13, 100 GHz, LC
ONS-SC+-10G-54.9	Prime Network 3.8	10G MR, SFP+ 1554.94, 100 GHz, LC
ONS-SC+-10G-55.7	Prime Network 3.8	10G MR, SFP+ 1555.75, 100 GHz, LC
ONS-SC+-10G-56.5	Prime Network 3.8	10G MR, SFP+ 1556.55, 100 GHz, LC
ONS-SC+-10G-57.3	Prime Network 3.8	10G MR, SFP+ 1557.36, 100 GHz, LC
ONS-SC+-10G-58.1	Prime Network 3.8	10G MR, SFP+ 1558.17, 100 GHz, LC
ONS-SC+-10G-58.9	Prime Network 3.8	10G MR, SFP+ 1558.98, 100 GHz, LC
ONS-SC+-10G-59.7	Prime Network 3.8	10G MR, SFP+ 1559.79, 100 GHz, LC
ONS-SC+-10G-60.6	Prime Network 3.8	10G MR, SFP+ 1560.61, 100 GHz, LC
ONS-SC+-10G-61.4	Prime Network 3.8	10G MR, SFP+ 1561.43, 100 GHz, LC

Cisco CPT Devices—Supported Technologies

The following technologies are supported by the Cisco CPT Devices in Cisco Prime Network 3.9:

- IP, page 8-8
- Routing Protocols, page 8-11
- Ethernet, page 8-13
- MPLS, page 8-18
- MPLS-TE, page 8-20

- MPLS-TP, page 8-22
- PWE3, page 8-24
- Security, page 8-25
- Hardware, page 8-26
- Serial, page 8-28
- BFD, page 8-29
- Carrier Ethernet, page 8-30
- CDP, page 8-31
- Discovery Protocol, page 8-31
- Ethernet OAM, page 8-31

Cisco CPT Devices—Supported Service Events

Table 8-4 Supported Service Events for Cisco CPT Devices—Cisco Prime Network 3.9

Event Name	Product_Version	Expedited
Active IP Interfaces Found	Prime Network 3.8	N
All IP Interfaces Down	Prime Network 3.8	N
Card Down	Prime Network 3.8	Y
Card In	Prime Network 3.8	Y
Card Out	Prime Network 3.8	Y
Card Up	Prime Network 3.8	Y
CPU utilization exceeded upper threshold	Prime Network 3.8	N
CPU utilization less than lower threshold	Prime Network 3.8	N
Device Unsupported	Prime Network 3.8	N

Table 8-4 Supported Service Events for Cisco CPT Devices—Cisco Prime Network 3.9

Event Name	Product_Version	Expedited
Link up	Prime Network 3.8	N

Supported Technologies on Cisco Optical Transport

The following sections list the objects and attributes that are supported on Cisco optical transport in Cisco Prime Network 3.9 per technology:

- IP, page 8-8
- Routing Protocols, page 8-11
- Ethernet, page 8-13
- MPLS, page 8-18
- MPLS-TE, page 8-20
- MPLS-TP, page 8-22
- PWE3, page 8-24
- Security, page 8-25
- Hardware, page 8-26
- Serial, page 8-28
- BFD, page 8-29
- Carrier Ethernet, page 8-30
- CDP, page 8-31
- Discovery Protocol, page 8-31
- Ethernet OAM, page 8-31

IP

Table 8-5 IP Attribute Support on Cisco Optical Transport—Cisco Prime Network 3.9

Attribute	CPT
IMO Name—IIPInterface	
IP Address	Y
Subnetwork Mask	Y
IP Interface Addresses Array	Y
Interface Name	Y
Interface Description	Y
IP Interface State	Y

Table 8-5 IP Attribute Support on Cisco Optical Transport—Cisco Prime Network 3.9

Attribute	CPT
OSPF Interface Cost	
Broadcast Address	
MTU	
Lookup Method	
Address Resolution Type	
ARP Timeout	
Secured ARP	
ICMP Mask Reply	
IGMP Proxy	
HSRP Groups	
IP Multiplexing Table	
IANA Type	
Containing CTPs	
Contained CTPs	
IMO Name—IIPMuxEntry	
Termination Point	
Destination IP Subnet	
IMO Name—IRoutingEntity	
Routing Table	Y
ARP Entity	Y
Routing Table Changes	
Name	Y
Logical Sons	Y
IMO Name—IRoutingEntry	
Destination IP Subnet	Y
Next Hop IP Address	Y
Type	Y
Routing Protocol Type	Y
Outgoing Interface Name	Y
IMO Name—IARPEntity	
ARP Table	Y
IMO Name—IARPEntry	
IP Address	Y
MAC Address	Y
Port	Y
Entry Type	Y

Table 8-5 IP Attribute Support on Cisco Optical Transport—Cisco Prime Network 3.9

Attribute	CPT
IMO Name—IIPPool	
IP Address Pool Entries	
Name	
Index	
IMO Name—IIPRangeBasedIPPoolEntry	
Start IP Address	
End IP Address	
Unused Addresses	
Used Addresses	
Reserved Addresses	
IMO Name—IIPSubnetBasedIPPoolEntry	
IP Subnet	
Unused Addresses	
Used Addresses	
Reserved Addresses	
IMO Name—HSRPGroupEntry	
Group Number	
Port Description	
Priority	
Coupled Router	
State	
Tracking Interfaces	
Virtual IP Address	
Virtual MAC Address	
IMO Name—ITunnelGRE	
Name	
Tunnel Destination and Source	
IP Address	
IP Interface State	
IANA Type	
Containing CTPs	
Contained CTPs	
Keep Alive Time	
Keep Alive Retry	
IMO Name—IVrrpGroupEntry	
Group Number	

Table 8-5 IP Attribute Support on Cisco Optical Transport—Cisco Prime Network 3.9

Attribute	CPT
State	
Port Description	
Master IP Address	
Primary IP Address	
Priority	
Virtual Mac Address	
Preempt Mode	
Admin State	
Advertisement Interval	
Tracking Interfaces	
IMO Name—IIPSLAResponderService	
responderStatus	
TWAMPResponderStatus	
tcpConnect	
udpEcho	
IMO Name—IIPAddressPortPair	
type	
ipAddress	
port	

Routing Protocols

Table 8-6 Routing Protocols Attribute Support on Cisco Optical Transport—Cisco Prime Network 3.9

Attribute	CPT
IMO Name—IBgpNeighborEntry	
Remote Identifier	
Neighbor Type	
Distributing Interfaces	
Remote Address	
Remote Autonomous System	
Peer State	
Peer AdminState	
Hold Time	
Keep Alive Time	

Table 8-6 Routing Protocols Attribute Support on Cisco Optical Transport—Cisco Prime Network 3.9 (continued)

Attribute	CPT
VrfName	
Address family	
IMO Name—IOspfEntry	
Area Identifier	
IP Address	
Type	
Administrative Status	
Ospf Entry State	
IMO Name—IOspfProcess	
Process Id	Y
OSPF Version	Y
Router Id	Y
IMO Name—IOspfNeighbor	
Neighbor Id	Y
Outgoing Interface	Y
State	Y
Neighbor Interface Address	Y
Area Id	Y
IMO Name—IOspfInterface	
Area Id	Y
Network Type	Y
Cost	Y
State	Y
Interface Address	Y
Type	Y
IF Proirity	Y
DR Id	Y
BDR Id	Y
IMO Name—ISpfTimers	
Schedule Delay	Y
Min Hold Time	Y
Max Wait Time	Y
IMO Name—IISISProcess	
ISIS Version	
Manual Area Address	

Table 8-6 Routing Protocols Attribute Support on Cisco Optical Transport—Cisco Prime Network 3.9 (continued)

Attribute	CPT
IS Type	
System Id	
Process Id	
IMO Name—IISISMetric	
IS Type	
Metric Style	
Metric Value	
Address Family	
IMO Name—IISISInterface	
Interface Name	
IMO Name—IISISNeighbor	
IS Type	
System Id	
Admin State	
Hold Time	
SNPA	
Interface Name	
IP Address	
Adress Family	

Ethernet

Table 8-7 Ethernet Attribute Support on Cisco Optical Transport—Cisco Prime Network 3.9

Attribute	CPT
IMO Name—ILinkAggregationGroup802dot3ad	
dot3adAggMACAddress	Y
dot3adAggActorSystemPriority	Y
dot3adAggActorSystemID	Y
dot3adAggActorAdminKey	Y
dot3adAggActorOperKey	Y
dot3adAggPartnerSystemID	Y
dot3adAggPartnerSystemPriority	Y
dot3adAggPartnerOperKey	Y

Table 8-7 Ethernet Attribute Support on Cisco Optical Transport—Cisco Prime Network 3.9

Attribute	CPT
dot3adAggCollectorMaxDelay	Y
GroupNumber	Y
AggregationProtocolType	Y
MacAddress	Y
ChannelAdminStatus	Y
ChannelOperStatus	Y
IMO Name—IEthernet	
MAC Address	Y
Duplex Mode	
Output Flow Control	
Input Flow Control	
IANA Type	
Containing CTPs	
Contained CTPs	
Port Type	Y
isElmiEnabled	Y
isLOAMEnabled	
IMO Name—IVlanInterface	
Mode	
Native VLAN Identification	
Virtual LAN Table	
IANA Type	
Containing CTPs	
Contained CTPs	
vlanAdminType	
vlanencapType	
getAccess	
Allowed Vlans	
IMO Name—IVlanEncapMux	
IANA Type	Y
Containing CTPs	
Contained CTPs	
IMO Name—IVlanMapping	
direction	
vlanMatchCriteria	
vlanRewriteDefinition	

Table 8-7 Ethernet Attribute Support on Cisco Optical Transport—Cisco Prime Network 3.9

Attribute	CPT
Drop	
Vlan	
innerVlan	
translatedVlan	
translatedInnerVlan	
IMO Name—IIEEE802	
VLAN Identification	
Binding Information	
Binding Status	
IANA Type	
Containing CTPs	
Contained CTPs	
IMO Name—IStpService	
StpProtocol	
StpMaxAge	
StpHelloTime	
StpBridgeForwardDelay	
StpInstanceInfoTable	
Same as ISystemService	
StpUplinkFastState	
StpBackboneFastState	
StpForwardDelay	
StpBridgeMaxAge	
StpBridgeHelloTime	
IMO Name—IMstService	
MstProperties	
Same as IStpService	
IMO Name—IPvstpService	
UpLinkFast	
BackboneFast	
IMO Name—IMstProperties	
MstForceVersion	
MstCfgIdFmtSel	
MstExternalRootCost	
MstMaxInstances	
MstCfgIdName	

Table 8-7 Ethernet Attribute Support on Cisco Optical Transport—Cisco Prime Network 3.9

Attribute	CPT
MstCfgIdRevLevel	
IMO Name—IStpInstanceInfo	
Object Identification	
StpBridgeId	
BridgePriority	
Designated Parent and Root Bridges	
StpRootCost	
IsRoot	
StpRootPort	
StpPortInfoTable	
STP Instance Id	
Vlan Id	
StpDesignatedBridge	
StpDesignatedRoot	
IMO Name—IMstInstanceInfo	
MstVlanIds	
Same as IStpInstanceInfo	
IMO Name—IPvstpInstanceInfo	
Protocol Type	
StpBridgeMaxAge	
StpBridgeHelloTime	
StpBridgeForwardDelay	
StpProtocolSpecification	
StpVlanId	
StpForwardDelay	
StpMaxAge	
IMO Name—IRstpInstanceInfo	
StpForceVersion	
Same as IStpInstanceInfo	
IMO Name—IStpPortInfo	
StpPort	
StpPortPriority	
StpPortState	
StpPortPathCost	
StpPortEdgePort	

Table 8-7 Ethernet Attribute Support on Cisco Optical Transport—Cisco Prime Network 3.9

Attribute	CPT
StpPortPointToPoint	
StpPortRole	
StpDesignatedPortIdentifier	
StpDesignatedBridge	
StpPortIdentifier	
StpPortBpduGuardState	
StpPortBpduFilterState	
IMO Name—IMstPortInfo	
MstPortHelloTime	
Same as IStpPortInfo	
IMO Name—IPvstpPortInfo	
PvstpPortFastState	
IMO Name—IEthernetChannel	
Group Number	
Bandwidth	
Aggregation Protocol	
IANA Type	
Containing CTPs	
Contained CTPs	
Mac Address	
Admin Status	
Oper Status	
IMO Name—ITokenRingLayer2	
MAC Address	
IANA Type	
Containing CTPs	
Contained CTPs	
IMO Name—ITokenRingLayer1	
Same as IPhysicalLayer	
IMO Name—IVtpService	
Version	
OperatingMode	
DomainName	
ConfigurationRevision	
isPruningEnabled	
isAuthenticationEnabled	

Table 8-7 Ethernet Attribute Support on Cisco Optical Transport—Cisco Prime Network 3.9

Attribute	CPT
IMO Name—IREPService	
version	Y
administrativeVlan	Y
notificationEnabled	Y
IMO Name—IREPSegmentInfo	
segmentId	Y
segmentComplete	Y
IMO Name—IREPPortInfo	
portName	Y
portKey	Y
segmentId	Y
portType	Y
portRole	Y
operStatus	Y
blockedVlans	Y
preemptTimer	Y
lslAgeoutTimer	Y
remoteDeviceName	Y
remoteDeviceMac	Y
remotePortName	Y
configuredLoadBalancingBlockedVlans	Y
IMO Name—IBridgeILan	
Id	
IMO Name—IIBBridgeEntry	
IS Id	
IBridge	
BBridge	

MPLS

Table 8-8 MPLS Attribute Support on Cisco Optical Transport—Cisco Prime Network 3.9

Attribute	CPT
IMO Name—IMpls	
Distribution Protocol	Y

Table 8-8 MPLS Attribute Support on Cisco Optical Transport—Cisco Prime Network 3.9

Attribute	CPT
LabelStack	
TopLabel	
Outer and Inner Labels	
Traffic Engineering Properties	Y
Resource reservation Properties	
IANA Type	Y
Containing CTPs	
Contained CTPs	
IMO Name—ILse	
MPLS Table	Y
MPLS Aggregate Table	Y
MPLS Tunnel Segments	Y
LDP Service	Y
Logical Sons	Y
IMO Name—ILdpService	
Local Identification Status	Y
LDP Peers	Y
IMO Name—ILdpPeer	
Peer Identification	Y
Transport Address	Y
Distribution Method	Y
Protocol Type	Y
Path Vector Limit	Y
Session Status	Y
Protocol Version Hold Time	
Hold Time	Y
Keep Alive Time	
Peer Discovery Sources	Y
IMO Name—ILdpDiscoverySource	
Interface Name	Y
Source Address	Y
Type	Y
IMO Name—IMplsEntry	
Incoming Label	Y
Outgoing Interface and Label	Y
Switching Action	Y

Table 8-8 MPLS Attribute Support on Cisco Optical Transport—Cisco Prime Network 3.9

Attribute	CPT
Next Hop IP Address	Y
Destination Mask	Y
Destination address	Y
IMO Name—IMplsAggregateEntry	
Virtual Routing Entity	Y
Incoming Label	Y
Outgoing Interface and Label	Y
Switching Action	Y
Next Hop IP Address	Y
IMO Name—IMplsLabelRange	
Type	Y
minValue	Y
MaxValue	Y

MPLS-TE

Table 8-9 MPLS-TE Attribute Support on Cisco Optical Transport—Cisco Prime Network 3.9

Attribute	CPT
IMO Name—IMplsTETunnel	
Destination Address	Y
Outgoing Interface and Label	Y
LSP Identification	Y
Requested Bandwidth	Y
Measured Average Burst and Peak Bandwidth	Y
Setup and Hold Priority	Y
Affinity Bits and Mask	Y
Automatic Route Announcement Status	Y
Optimization Lock Down Status	Y
Path Option	Y
Name	Y
Description	Y
Administrative Status	Y
Operational Status	Y

Table 8-9 MPLS-TE Attribute Support on Cisco Optical Transport—Cisco Prime Network 3.9

Attribute	CPT
IANA Type	Y
is FRR Enabled	Y
TunnelType	Y
DestinationAddress	Y
Sub Lsp Status	Y
OutInterface	Y
OutLabel	Y
TunnelAffinity	Y
TunnelAffinityMask	Y
TunnelAutoRoute	Y
TunnelBandwidthKbps	Y
TunnelAverageRateKbps	Y
TunnelBurstKbps	Y
TunnelPeakRateKbps	Y
TunnelSetupPriority	Y
TunnelHoldPriority	Y
TunnelLockdown	Y
TunnelPolicyClass	
P2MPDestinations	Y
IMO Name—IMplsTEProperties	
Administrative Weight	Y
Attributes Identifier	
Signaling Protocol	Y
Available Physical and Reservable Bandwidth	Y
Reserved Bandwidth	Y
IMO Name—IMplsTEPropertiesAllocationEntry	
Priority Level	
Allocated and Cumulative Bandwidth	
IMO Name—IMplsTESegment	
Segment Type	Y
Measured Average Burst and Peak Bandwidth	Y
LSP Identification	Y

Table 8-9 MPLS-TE Attribute Support on Cisco Optical Transport—Cisco Prime Network 3.9

Attribute	CPT
Name	Y
FRRTunnelName	
FRRTunnelState	
AverageBandwidth	Y
In Interface	Y
Out interface	Y
In Label	Y
Out Label	Y
Source address	Y
Destination address	Y
TunnelType	Y

MPLS-TP

Table 8-10 MPLS-TP Attribute Support on Cisco Optical Transport—Cisco Prime Network 3.9

Attribute	CPT
IMO Name—IMPLSTPGlobal	
icc	Y
globalId	Y
protectionMode	Y
redundancyMode	Y
routerId	Y
tpEnabledLinks	Y
lspEndpoints	Y
lspMidpoints	Y
mplsTpTunnelEps	Y
IMO Name—IMPLSTPTunnelEP	
tunnelId	Y
remoteTunnelId	Y
globalId	Y
destGlobalId	Y
localInfo	Y
peerInfo	Y
adminStatus	Y
operStatus	Y

Table 8-10 MPLS-TP Attribute Support on Cisco Optical Transport—Cisco Prime Network 3.9

Attribute	CPT
bandwidthTransmit	Y
bfdTemplate	Y
workingLspNum	Y
protectLspNum	Y
wlBfdState	Y
plBfdState	Y
wlFaultOAM	Y
plFaultOAM	Y
pseudowireList	Y
direction	Y
lspEndPoints	Y
lspMidPoints	Y
internalId	Y
tpDescription	Y
PeerTunnelId	Y
PeerGlobalId	Y
MPLSTPDirection	Y
IMO Name—ILSPEntry	
lspId	Y
internalId	Y
umc	Y
lspType	Y
IMO Name—ILSPMPEntry	
fwdInLabel	Y
fwdOutLabel	Y
fwdBandwidth	Y
fwdOutInterface	Y
revInLabel	Y
revOutLabel	Y
revOutLinkId	Y
revBandwidth	Y
revOutInterface	Y
bandwidthDiff	Y
IMO Name—ILSPEPEntry	
inLabel	Y
outLabel	Y

Table 8-10 MPLS-TP Attribute Support on Cisco Optical Transport—Cisco Prime Network 3.9

Attribute	CPT
outLinkId	Y
bandwidth	Y
outInterface	Y
state	Y
IMO Name—ITPEnabledLink	
linkId	Y
interfaceAddress	Y
nextHop	Y
IMO Name—IMPLSTPBfdSession	
lspType	Y

PWE3

Table 8-11 PWE3 Attribute Support on Cisco Optical Transport—Cisco Prime Network 3.9

Attribute	CPT
IMO Name—IPTPLayer2MplsTunnel	
Local and Remote Router Addresses	Y
Local and Remote Virtual Connection Labels	Y
Tunnel Identification	Y
Tunnel Status	Y
Local and Remote Tunnel Interface	
IANA Type	Y
Containing CTPs	
Contained CTPs	
PsuedowireType	Y
PreferredPathTunnel	Y
LocalMTU	Y
RemoteMTU	Y
PeerStatus	Y
SignalingProtocol	Y
VFIName	Y
psuedowireRole	Y
PeerRouterIp	Y

Table 8-11 PWE3 Attribute Support on Cisco Optical Transport—Cisco Prime Network 3.9

Attribute	CPT
LocalRouterIp	Y
LocalVcLabel	Y
PeerVcLabel	Y

Security

Table 8-12 Security Attribute Support on Cisco Optical Transport—Cisco Prime Network 3.9

Attribute	CPT
IMO Name—IAccessList	
Type	Y
Access List Entries	Y
Name or Id	Y
Index	Y
IMO Name—IAccessListEntry	
Entry Identification	Y
Action Logic	Y
Source and Destination Address	Y
Source and Destination Wildcard	Y
Protocol Type	Y
Source and Destination Port Ranges	Y
Source and Destination Port Action	Y
Protocol Specific Info	Y
Differential Services Code Points	Y
Type of Service	Y
Precedence	Y
Matches	Y

Hardware

Table 8-13 Hardware Attribute Support on Cisco Optical Transport—Cisco Prime Network 3.9

Attribute	CPT
IMO Name—IChassis	
Description	Y
Equipment Holder Type	Y
Contained Equipment Holders	
Contained Equipments	
Serial Number	Y
IMO Name—IShelf	
Description	
Status	
Equipment Holder Type	
Contained Equipment Holders	
Contained Equipments	
Serial Number	
IMO Name—IModule	
Module Name	Y
Module Description	Y
Software Version	Y
Operational Status	Y
Hardware Type + Version	Y
Managed IP Address	
Redundant Equipment	
Configured Redundancy	
Redundancy Status	
Operational Status Last Changed	Y
Supported Physical Termination Points	Y
Serial Number (soft property)	Y
Slots Number	
IMO Name—IPowerSupply	
Same as IModule	Y
IMO Name—IFanTray	
Same as IModule	Y
IMO Name—IPluggableTransceiver	
ConnectorDescription	Y

Table 8-13 Hardware Attribute Support on Cisco Optical Transport—Cisco Prime Network 3.9

Attribute	CPT
PID	Y
ConnectorSerialNumber	Y
ConnectorType	Y
PluggablePortState	Y
PluggableType	Y
IMO Name—IManagedElement	
IP Address	Y
Communication State	Y
Investigation State	Y
Element Category	Y
Element Type and Key	Y
Device Name	Y
System Name	Y
System Description	Y
Up Time	Y
Software Version	Y
Vendor Identity	Y
Memory and CPU Usage	Y
DRAM Free	Y
DRAM Used	Y
DRAM Usage	Y
Flash Device Size	Y
NVRAM Size	Y
Processor DRAM	Y
Sys Contact	Y
Sys Location	Y
Serial Number	Y
File Systems	
IMO Name—IContext	
Name	Y
Bounded Connections	
IP Address Pools	
Forwarding Components List	
Traffic Descriptors List	
Tunnel Containers List	

Table 8-13 Hardware Attribute Support on Cisco Optical Transport—Cisco Prime Network 3.9

Attribute	CPT
Data Link Aggregation Containers List	
IMO Name—ISystemService	
Type	
Status	
Up Time	Y
IMO Name—IBridge	
Bridge Table	
Type	Y
MAC Address	
IP Interface	
Name	Y
Logical Sons	Y
Vlan Type	Y
IMO Name—IBridgeEntry	
Destination MAC	
Outgoing Interface	

Serial

Table 8-14 Serial Attribute Support on Cisco Optical Transport—Cisco Prime Network 3.9

Attribute	CPT
IMO Name—IPhysicalLayer	
Media Type	Y
Clocking Source	
Maximum Speed	Y
Is Internal Port	Y
Discarded Bandwidth	
Dropped Bandwidth	
Input Bandwidth	
Output Bandwidth	
Discarded and Received Input Data Counters	Y
Dropped and Forward Output Data Counters	Y
Administrative Status	Y

Table 8-14 Serial Attribute Support on Cisco Optical Transport—Cisco Prime Network 3.9

Attribute	CPT
Operational Status	Y
Last Changed	Y
IANA Type	Y
Containing CTPs	
Contained CTPs	
Port Alias	Y
Location	Y
Sending Alarms	Y
Connector Description	Y
Part ID	Y
Connector Serial Num	Y
Product	Y
Status	Y
Managed	Y

BFD

Table 8-15 BFD Attribute Support on Cisco Optical Transport—Cisco Prime Network 3.9

Attribute	CPT
IMO Name—IBfdService	
Status	
IMO Name—IBfdCommon	
RegisteredProtocols	Y
InterfaceName	Y
IMO Name—IBfdSession	
SourceIp	Y
DestinationIp	Y
Interval	Y
Multiplier	Y
Protocol	Y
State	Y
Interface	Y
Process	Y

Carrier Ethernet

Table 8-16 Carrier Ethernet Attribute Support on Cisco Optical Transport—Cisco Prime Network 3.9

Attribute	CPT
IMO Name—IVsi	
vsiInstanceName	
vpnId	
discoveryMode	
vsiMode	
Operational state	
Administrative state	
IMO Name—IPseudowireProperties	
isSplitHorizonEnabled	
isAutoDiscovered	
IMO Name—IVLANTaggedInterface	
InterfaceName	
Inner Vlan Id	
Outer Vlan Id	
Encap Type	
Operational state	
Administrative state	
ConfiguredDescription	
IMO Name—IEfp	
EfpId	Y
RewriteParams	Y
EncapsParams	Y
AdminStatus	Y
OperStatus	Y
SplitHorizonGroup	Y
MatchCriteria	Y
ConfiguredDescription	Y
GetServiceInstanceId	Y
SetServiceInstanceId	Y

CDP

Table 8-17 CDP Attribute Support on Cisco Optical Transport—Cisco Prime Network 3.9

Attribute	CPT
IMO Name—ICdpService	
cdpHoldtime	Y
cdpMessageInterval	Y
cdpDeviceId	Y
cdpState	Y
cdpVersion	Y
IMO Name—ICdpNeighbor	
remoteDeviceId	Y
remotePortId	Y
remoteIPAddress	Y
localPortId	Y

Discovery Protocol

Table 8-18 Discovery Protocol Attribute Support on Cisco Optical Transport—Cisco Prime Network 3.9

Attribute	CPT
IMO Name—IDiscoveryProtocol	
DiscoveryProtocolType	Y
Info	Y

Ethernet OAM

Table 8-19 Ethernet OAM Attribute Support on Cisco Optical Transport—Cisco Prime Network 3.9

Attribute	CPT
IMO Name—ICfmService	
cacheSize	Y
maximumCacheSize	Y
holdTime	Y
version	Y

Table 8-19 Ethernet OAM Attribute Support on Cisco Optical Transport—Cisco Prime Network 3.9 (continued)

Attribute	CPT
maintenanceIntermedatePointsTable	Y
maintenanceDomain	Y
IMO Name—IMaintenanceDomain	
name	Y
level	Y
Id	Y
maintenanceAssociation	Y
IMO Name—IMaintenanceEndPoint	
macAddress	Y
Interface	Y
continuityCheckStatus	Y
direction	Y
IMO Name—IMaintenanceAssociation	
name	Y
associationType	Y
maximalMeps	Y
continuityCheckInterval	Y
continuityCheckEnable	Y
crossCheckEnable	Y
direction	Y
bridge	Y
maintenanceEndPoints	Y
cfmRemoteMaintenanceEndPoints	Y
IMO Name—IMaintenanceIntermediatePoint	
level	Y
cfmInterface	Y
isAutocreated	Y
Vlans	Y
macAddress	Y
IMO Name—IRemoteMaintenanceEndPoint	
mepId	Y
macAddress	Y

Table 8-19 Ethernet OAM Attribute Support on Cisco Optical Transport—Cisco Prime Network 3.9 (continued)

Attribute	CPT
level	Y
maintenanceEndPointStatus	Y
maintenanceEndPointOid	Y
IMO Name—IOAMData	
adminState	Y
pduMaxRate	Y
pduMinRate	Y
linkTimeout	Y
highThresholdAction	Y
linkFaultAction	Y
dyingGaspAction	Y
criticalEventAction	Y
mode	Y
unidirectional	Y
linkMonitor	Y
remoteLoopback	Y
portStatus	Y
loopbackStatus	Y
remoteData	Y
name	Y
ethernetPort	Y
IMO Name—IOAMRemoteData	
macAddress	Y
vendor	Y
mode	Y
unidirection	Y
linkMonitor	Y
remoteLoopback	Y
IMO Name—IUNIProperties	
UNIId	
isServiceMultiplexing	
isBundlingEnabled	
bundlingType	
IMO Name—IEthernetLMI	
isGlobalEnabled	

Table 8-19 Ethernet OAM Attribute Support on Cisco Optical Transport—Cisco Prime Network 3.9 (continued)

Attribute	CPT
mode	
ELMIInterfaces	
deviceEVCs	
IMO Name—IDeviceEVC	
EVCName	
EVCStatus	
EVCType	
cfmMaName	
configuredRemoteUNICount	
activeRemoteUNICount	
UNIInterfaces	
IMO Name—IUNIInterfaces	
UNIStatus	
UNIId	
interfaceName	
vlanList	
lmiLinkStatus	
IMO Name—IELMIInterfaces	
interfaceName	
T391	
T392	
N391	
N393	



CHAPTER 9

Support Information for Cisco DataCentre

This chapter contains support information for Virtual Network Elements (VNEs) that manage Cisco datacentre in Cisco Prime Network 3.9.

- Cisco UCS 61xx Series Switches, page 9-1
- Supported Technologies on Cisco DataCentre, page 9-4

Note For more information about the technologies described in this chapter , see Part 2 Technology Support.

Cisco UCS 61xx Series Switches

This section includes the following information about CiscoUCS 6120 datacentre (for information on the NE types supported in Cisco Prime Network 3.9, see Cisco UCS 61xx Series Switches):

- CiscoUCS 6120—Supported Software Versions, page 9-1
- CiscoUCS 6120—Supported Modules, page 9-2
- CiscoUCS 6120—Supported Technologies, page 9-3
- CiscoUCS 6120—Supported Service Events, page 9-3

CiscoUCS 6120—Supported Software Versions

Table 9-1 Supported Software Versions for CiscoUCS 6120—Cisco Prime Network 3.9

Software Version	Product_Version
NX-OS 4.2(1)N1(1.1j)	Prime Network 3.9

CiscoUCS 6120—Supported Modules

Table 9-2 Supported Modules for CiscoUCS 6120—Cisco Prime Network 3.9

Module Name	Product_Version	Module Description
N20-I6584	Prime Network 3.9	UCS 2104XP Fabric Extender/4 external 10Gb ports
N20-AC0002	Prime Network 3.9	Cisco N20-AC0002 UCS M81KR Virtual Interface Card/PCIe/2-port 10Gb
N20-FAN5	Prime Network 3.9	Fan module for UCS 5108
N10-FAN1	Prime Network 3.9	Fan module for UCS 6120XP Fabric Interconnect
N10-S6100-SUP	Prime Network 3.9	UCS 6100 Series Fabric Interconnect 20x10GE/Supervisor
N10-E0060	Prime Network 3.9	20x10GE/Supervisor
N10-S6100	Prime Network 3.9	UCS 6100 Series Fabric Interconnect
N10-E0080	Prime Network 3.9	Cisco N10-E0080 UCS 6100 8-Port 4Gb Fibre Channel Expansion module, SFP-uplink
N20-B6620-1	Prime Network 3.9	UCS B200 M1 Blade Server w/o CPU, memory, HDD, mezzanine
N20-B6620-2	Prime Network 3.9	UCS B250 M1 Blade Server w/o CPU, memory, HDD, mezzanine
N20-AQ0002	Prime Network 3.9	UCS M71KR-Q QLogic Converged Network Adapter/PCIe/2port 10Gb
N20-B6625-1	Prime Network 3.9	UCS B200 M2 Blade Server w/o CPU, memory, HDD, mezzanine
N20-PAC5-2500W	Prime Network 3.9	2500W power supply unit for UCS 5108

Table 9-2 Supported Modules for CiscoUCS 6120—Cisco Prime Network 3.9 (continued)

Module Name	Product_Version	Module Description
N10-PAC1-550W	Prime Network 3.9	AC power supply
N20-C6508	Prime Network 3.9	UCS 5108 Blade Server Chassis/0 PSU/8 fans/0 fabric extender

CiscoUCS 6120—Supported Technologies

The following technologies are supported by the CiscoUCS 6120 in Cisco Prime Network 3.9:

- IP, page 9-5
- Hardware, page 9-8
- CDP, page 9-11

CiscoUCS 6120—Supported Service Events

Table 9-3 Supported Service Events for CiscoUCS 6120—Cisco Prime Network 3.9

Event Name	Product_Version	Expedited
Chassis Connected	Prime Network 3.9	Y
Chassis Disconnected	Prime Network 3.9	Y
Card Down	Prime Network 3.9	N
Card In	Prime Network 3.9	N
Card Out	Prime Network 3.9	N
Card Out Chassis Disconnected	Prime Network 3.9	Y

Table 9-3 Supported Service Events for CiscoUCS 6120—Cisco Prime Network 3.9 (continued)

Event Name	Product_Version	Expedited
Card Up	Prime Network 3.9	N
power-supply down	Prime Network 3.9	N
Power-supply out	Prime Network 3.9	N
Port down due to admin	Prime Network 3.9	N
Port down due to Card down	Prime Network 3.9	N
Port down due to Card out	Prime Network 3.9	N
Port down due to oper	Prime Network 3.9	N
fan-tray down	Prime Network 3.9	N
Fan-tray out	Prime Network 3.9	N
Interface status up	Prime Network 3.9	N
Port up	Prime Network 3.9	N
Interface status down	Prime Network 3.9	N

Supported Technologies on Cisco DataCentre

The following sections list the objects and attributes that are supported on Cisco datacentre in Cisco Prime Network 3.9 per technology:

- IP, page 9-5

- Hardware, page 9-8
- CDP, page 9-11

IP

Table 9-4 IP Attribute Support on Cisco DataCentre—Cisco Prime Network 3.9

Attribute	UCS 6120
IMO Name—IIPInterface	
IP Address	Y
Subnetwork Mask	Y
IP Interface Addresses Array	Y
Interface Name	Y
Interface Description	Y
IP Interface State	Y
OSPF Interface Cost	
Broadcast Address	
MTU	
Lookup Method	
Address Resolution Type	
ARP Timeout	
Secured ARP	
ICMP Mask Reply	
IGMP Proxy	
HSRP Groups	
IP Multiplexing Table	
IANA Type	
Containing CTPs	
Contained CTPs	
IMO Name—IIPMuxEntry	
Termination Point	
Destination IP Subnet	
IMO Name—IRoutingEntity	
Routing Table	
ARP Entity	
Routing Table Changes	
Name	

Table 9-4 IP Attribute Support on Cisco DataCentre—Cisco Prime Network 3.9 (continued)

Attribute	UCS 6120
Logical Sons	
IMO Name—IRoutingEntry	
Destination IP Subnet	
Next Hop IP Address	
Type	
Routing Protocol Type	
Outgoing Interface Name	
IMO Name—IARPEntity	
ARP Table	
IMO Name—IARPEntry	
IP Address	
MAC Address	
Port	
Entry Type	
IMO Name—IIPPool	
IP Address Pool Entries	
Name	
Index	
IMO Name—IIPRangeBasedIPPoolEntry	
Start IP Address	
End IP Address	
Unused Addresses	
Used Addresses	
Reserved Addresses	
IMO Name—IIPSubnetBasedIPPoolEntry	
IP Subnet	
Unused Addresses	
Used Addresses	
Reserved Addresses	
IMO Name—HSRPGroupEntry	
Group Number	
Port Description	
Priority	
Coupled Router	
State	

Table 9-4 IP Attribute Support on Cisco DataCentre—Cisco Prime Network 3.9 (continued)

Attribute	UCS 6120
Tracking Interfaces	
Virtual IP Address	
Virtual MAC Address	
IMO Name—ITunnelGRE	
Name	
Tunnel Destination and Source	
IP Address	
IP Interface State	
IANA Type	
Containing CTPs	
Contained CTPs	
Keep Alive Time	
Keep Alive Retry	
IMO Name—IVrrpGroupEntry	
Group Number	
State	
Port Description	
Master IP Address	
Primary IP Address	
Priority	
Virtual Mac Address	
Preempt Mode	
Admin State	
Advertisement Interval	
Tracking Interfaces	
IMO Name—IIPSLAResponderService	
responderStatus	
TWAMPResponderStatus	
tcpConnect	
udpEcho	
IMO Name—IIPAddressPortPair	
type	
ipAddress	
port	

Hardware

Table 9-5 Hardware Attribute Support on Cisco DataCentre—Cisco Prime Network 3.9

Attribute	UCS 6120
IMO Name—IChassis	
Description	Y
Equipment Holder Type	
Contained Equipment Holders	
Contained Equipments	
Serial Number (Soft property)	Y
Configuration State (Soft property)	Y
Operability (Soft property)	Y
Power (Soft property)	Y
Thermal (Soft property)	Y
Name (Soft property)	Y
PID (Soft property)	Y
VID (Soft property)	Y
IMO Name—IShelf	
Description	
Status	
Equipment Holder Type	
Contained Equipment Holders	
Contained Equipments	
Serial Number	
IMO Name—IModule	
Module Name	Y
Module Description	Y
Software Version	Y
Operational Status	Y
Hardware Type + Version	Y
Managed IP Address	
Redundant Equipment	
Configured Redundancy	Y
Redundancy Status	Y
Supported Physical Termination Points	

Table 9-5 Hardware Attribute Support on Cisco DataCentre—Cisco Prime Network 3.9

Attribute	UCS 6120
Serial Number (soft property)	Y
Admin State(Soft property)	Y
Discovery State(Soft property)	Y
Power State (Soft property)	Y
Slot ID (Soft property)	Y
Chassis ID (Soft property)	Y
Name (Soft property)	Y
Description (Soft property)	Y
PID (Soft property)	Y
VID (Soft property)	Y
Operating Memory Voltage(Soft property)	Y
Avail State (Soft property)	Y
Assoc State (Soft property)	Y
Slot Status (Soft property)	Y
Check Point (Soft property)	Y
Number Of Processor (Soft property)	Y
Effective Memory (Soft property)	Y
Total Memory (Soft property)	Y
Operating Memory Speed (Soft property)	Y
Operating Memory Voltage (Soft property)	Y
Slot Number (Soft property)	Y
Part Number (Soft property)	Y
Running Version (Soft property)	Y
Package Version (Soft property)	Y
Backup Version (Soft property)	Y
Update Status (Soft property)	Y
Startup Version (Soft property)	Y
Activate Status (Soft property)	Y
IMO Name—IPowerSupply	
Same as IModule	Y

Table 9-5 Hardware Attribute Support on Cisco DataCentre—Cisco Prime Network 3.9

Attribute	UCS 6120
IMO Name—IFanTray	
Same as IModule	Y
IMO Name—IPluggableTransceiver	
ConnectorDescription	
PID	
ConnectorSerialNumber	
ConnectorType	
PluggablePortState	
PluggableType	
IMO Name—IManagedElement	
IP Address	Y
Communication State	Y
Investigation State	Y
Element Category	Y
Element Type and Key	Y
Device Name	Y
System Name	Y
System Description	Y
Up Time	Y
Software Version	Y
Vendor Identity	Y
Memory and CPU Usage	
DRAM Free	
DRAM Used	
DRAM Usage	
Flash Device Size	
NVRAM Size	
Processor DRAM	
Sys Contact	
Sys Location	
Serial Number	
File Systems	
IMO Name—IContext	
Name	
Bounded Connections	

Table 9-5 Hardware Attribute Support on Cisco DataCentre—Cisco Prime Network 3.9

Attribute	UCS 6120
IP Address Pools	
Forwarding Components List	
Traffic Descriptors List	
Tunnel Containers List	
Data Link Aggregation Containers List	
IMO Name—ISystemService	
Type	
Status	
Up Time	
IMO Name—IBridge	
Bridge Table	
Type	
MAC Address	
IP Interface	
Name	
Logical Sons	
Vlan Type	
IMO Name—IBridgeEntry	
Destination MAC	
Outgoing Interface	

CDP

Table 9-6 CDP Attribute Support on Cisco DataCentre—Cisco Prime Network 3.9

Attribute	UCS 6120
IMO Name—ICdpService	
cdpHoldtime	Y
cdpMessageInterval	Y
cdpDeviceId	Y
cdpState	Y
cdpVersion	Y

Table 9-6 CDP Attribute Support on Cisco DataCentre—Cisco Prime Network 3.9 (continued)

Attribute	UCS 6120
IMO Name—ICdpNeighbor	
remoteDeviceId	Y
remotePortId	Y
remoteIPAddress	Y
localPortId	Y



CHAPTER 10

Support Information for Generic Devices

This chapter contains support information for Virtual Network Elements (VNEs) that manage Generic devices in Cisco Prime Network 3.9.

- Understanding the Generic VNE, page 10-1
- Supported Technologies on Generic Devices, page 10-5

Note For more information about the technologies described in this chapter , see Part 2 Technology Support.

Understanding the Generic VNE

The generic VNE can be used to model any NE that is not currently supported by Cisco ANA. The generic VNE provides a basic level of network management that provides information such as the physical interfaces available on the device and their status, rudimentary logical modeling, and parsing of basic traps.

The generic VNE models NEs using SNMP MIB2, which is the most generic and widely used management interface. The generic VNE does not consider the device vendor, device type, or software version of the NE that it models.

This section contains the following topics:

- Physical Inventory Model, page 10-2
- Logical Inventory Model, page 10-2
- Generic VNE—Supported Traps, page 10-3
- Generic VNE—Supported Events, page 10-4
- Generic VNE Limitations, page 10-4
- Generic VNE—Supported Technologies, page 10-4
- Generic VNE—Supported Service Events, page 10-4

Physical Inventory Model

The generic VNE uses a static model for the device chassis. The rest of the physical inventory is modeled using the ifTable. Since modules are not modeled, the generic VNE creates a single generic module on which all of the physical interfaces reside.

Table 10-1 on page 10-2 describes which MIB tables are used to model the physical inventory components that are supported by the generic VNE.

Table 10-1 MIBs Used for Physical Inventory Model of Generic VNE—Cisco ANA 3.7

Logical Component	MIB Table	Columns/Tables Used For Modeling
Interfaces	ifTable	• ifDescr • ifType • ifOperStatus
Ports Port status Port speed MAC address	 ifTable ifTable ifTable	• ifOperStatus and ifAdminStatus • ifSpeed • ifPhysAddress (Ethernet ports)

Note Certain general properties on the managed element, such as system description, are modeled using the system MIB.

Logical Inventory Model

Table 10-2 on page 10-2 describes which MIB tables are used to model the logical inventory components that are supported by the generic VNE.

Table 10-2 MIBs Used for Logical Inventory Model of Generic VNE—Cisco ANA 3.7

Logical Component	MIB Table	Columns/Tables Used For Modeling
IP Interfaces	ipAddrTable	• ipAdEntIfIndex • ipAdEntNetMask
ARP table	ipNetToMediaTable	• ipNetToMediaPhysAddress • ipNetToMediaType
Routing table	ipRouteTable	• ipRouteDest • ipRouteIfIndex • ipRouteNextHop • ipRouteType • ipRouteMask
Bridging table	dot1dTpFdbTable	—

Table 10-2 MIBs Used for Logical Inventory Model of Generic VNE—Cisco ANA 3.7 (continued)

Logical Component	MIB Table	Columns/Tables Used For Modeling
Default bridge	dot1dBridge	• dot1dBaseBridgeAddress • dot1dBaseType

Generic VNE—Supported Traps

The generic VNE can parse the standard MIB2 traps listed in Table 10-3 on page 10-3.

Table 10-3 Supported Traps for Generic VNE—Cisco ANA<nbsp/>3.7

authenticationFailure	mplsTunnelReoptimized
bgpBackwardTransition	mplsTunnelRerouted
bgpEstablished	mplsTunnelUp
coldStart	ospfIfAuthFailure
entConfigChange	ospfIfConfigError
linkDown	ospfIfRxBadPacket
linkUp	ospfIfStateChange (down)
mplsL3VpnVrfDown	ospfIfStateChange (up)
mplsL3VpnVrfNumVrfRouteMaxThreshExceeded	ospfMaxAgeLsa
mplsL3VpnVrfRouteMidThreshExceeded	ospfNbrStateChange (down)
mplsL3VpnVrfUp	ospfNbrStateChange (up)
mplsLdpInitSessionThresholdExceeded	ospf-if-packet-retransmit
mplsLdpSessionDown	ospfOriginateLsa
mplsLdpSessionUp	ospfTxRetransmit
mplsTunnelDown	warmStart

The generic VNE can identify traps, but it cannot correlate them. This is because the generic VNE does not include the model entities required by higher trap parsing levels.

For example, if Prime Network receives an mplsTunnelDown trap from a device modeled with the generic VNE, Prime Network can identify the Tunnel Down trap, but it cannot perform correlation on the trap. The reason is that the generic VNE does not investigate tunnels, which means that there is no Device Component in the model to which Prime Network can attach a correlation flow.

Generic VNE—Supported Events

The generic VNE supports the service events listed in Table 10-4 on page 10-4.

Table 10-4 Supported Service Events for Generic VNE—Cisco ANA 3.7.1

Event Name	ANA Version	Expedited
Device Unreachable	3.6.0	N
Discard Packets	3.6.0	N
Dropped Packets	3.6.0	N
Port Flapping	3.6.0	N
Port Down	3.6.0	N

Generic VNE Limitations

The generic VNE uses MIB2 to cover the widest possible range of NEs. Although MIB2 is a widely accepted industry standard, most network equipment vendors augment MIB2 with other Management Interfaces such as private MIBs, Telnet, XML, and so on. In addition, different vendors sometimes have different implementations of standard MIBs. As a result, even the limited model created by the generic VNE is dependent on the vendor's adherence to general network management standards.

Generic VNE—Supported Technologies

The following technologies are supported by the Generic VNE in Cisco Prime Network 3.9:

- IP, page 10-5
- Ethernet, page 10-8
- Hardware, page 10-13
- Serial, page 10-15

Generic VNE—Supported Service Events

Table 10-5 Supported Service Events for Generic VNE—Cisco Prime Network 3.9

Event Name	Product_Version	Expedited
Device Unreachable		N
Discarded packet rate exceeded upper threshold		N
Dropped packet rate exceeded upper threshold		N
Port Down		N

Supported Technologies on Generic Devices

The following sections list the objects and attributes that are supported on Generic devices in Cisco Prime Network 3.9 per technology:

- IP, page 10-5
- Ethernet, page 10-8
- Hardware, page 10-13
- Serial, page 10-15

IP

Table 10-6 IP Attribute Support on Generic Devices—Cisco Prime Network 3.9

Attribute	Generic
IMO Name—IIPInterface	
IP Address	Y
Subnetwork Mask	Y
IP Interface Addresses Array	
Interface Name	
Interface Description	Y
IP Interface State	Y
OSPF Interface Cost	
Broadcast Address	
MTU	
Lookup Method	
Address Resolution Type	
ARP Timeout	
Secured ARP	
ICMP Mask Reply	
IGMP Proxy	
HSRP Groups	
IP Multiplexing Table	
IANA Type	
Containing CTPs	
Contained CTPs	
IMO Name—IIPMuxEntry	
Termination Point	
Destination IP Subnet	

Table 10-6 IP Attribute Support on Generic Devices—Cisco Prime Network 3.9 (continued)

Attribute	Generic
IMO Name—IRoutingEntity	
Routing Table	Y
ARP Entity	Y
Routing Table Changes	
Name	Y
Logical Sons	Y
IMO Name—IRoutingEntry	
Destination IP Subnet	Y
Next Hop IP Address	Y
Type	Y
Routing Protocol Type	Y
Outgoing Interface Name	Y
IMO Name—IARPEntity	
ARP Table	Y
IMO Name—IARPEntry	
IP Address	Y
MAC Address	Y
Port	Y
Entry Type	Y
IMO Name—IIPPool	
IP Address Pool Entries	
Name	
Index	
IMO Name—IIPRangeBasedIPPoolEntry	
Start IP Address	
End IP Address	
Unused Addresses	
Used Addresses	
Reserved Addresses	
IMO Name—IIPSubnetBasedIPPoolEntry	
IP Subnet	
Unused Addresses	
Used Addresses	
Reserved Addresses	

Table 10-6 IP Attribute Support on Generic Devices—Cisco Prime Network 3.9 (continued)

Attribute	Generic
IMO Name—HSRPGroupEntry	
Group Number	
Port Description	
Priority	
Coupled Router	
State	
Tracking Interfaces	
Virtual IP Address	
Virtual MAC Address	
IMO Name—ITunnelGRE	
Name	
Tunnel Destination and Source	
IP Address	
IP Interface State	
IANA Type	
Containing CTPs	
Contained CTPs	
Keep Alive Time	
Keep Alive Retry	
IMO Name—IIPSLAResponderService	
responderStatus	
TWAMPResponderStatus	
tcpConnect	
udpEcho	
IMO Name—IIPAddressPortPair	
type	
ipAddress	
port	

Ethernet

Table 10-7 Ethernet Attribute Support on Generic Devices—Cisco Prime Network 3.9

Attribute	Generic
IMO Name—ILinkAggregationGroup802dot3ad	
dot3adAggMACAddress	
dot3adAggActorSystemPriority	
dot3adAggActorSystemID	
dot3adAggActorAdminKey	
dot3adAggActorOperKey	
dot3adAggPartnerSystemID	
dot3adAggPartnerSystemPriority	
dot3adAggPartnerOperKey	
dot3adAggCollectorMaxDelay	
GroupNumber	
AggregationProtocolType	
MacAddress	
ChannelAdminStatus	
ChannelOperStatus	
IMO Name—IEthernet	
MAC Address	Y
Duplex Mode	
Output Flow Control	
Input Flow Control	
IANA Type	
Containing CTPs	
Contained CTPs	
Port Type	
isElmiEnabled	
isLOAMEnabled	
IMO Name—IVlanInterface	
Mode	
Native VLAN Identification	
Virtual LAN Table	
IANA Type	

Table 10-7 Ethernet Attribute Support on Generic Devices—Cisco Prime Network 3.9 (continued)

Attribute	Generic
Containing CTPs	
Contained CTPs	
vlanAdminType	
vlanencapType	
getAccess	
Allowed Vlans	
IMO Name—IVlanEncapMux	
IANA Type	
Containing CTPs	
Contained CTPs	
IMO Name—IVlanMapping	
direction	
vlanMatchCriteria	
vlanRewriteDefinition	
Drop	
Vlan	
innerVlan	
translatedVlan	
translatedInnerVlan	
IMO Name—IIEEE802	
VLAN Identification	
Binding Information	
Binding Status	
IANA Type	
Containing CTPs	
Contained CTPs	
IMO Name—IStpService	
StpProtocol	
StpMaxAge	
StpHelloTime	
StpBridgeForwardDelay	
StpInstanceInfoTable	
Same as ISystemService	
StpUplinkFastState	
StpBackboneFastState	

Table 10-7 Ethernet Attribute Support on Generic Devices—Cisco Prime Network 3.9 (continued)

Attribute	Generic
StpForwardDelay	
StpBridgeMaxAge	
StpBridgeHelloTime	
IMO Name—IMstService	
MstProperties	
Same as IStpService	
IMO Name—IPvstpService	
UpLinkFast	
BackboneFast	
IMO Name—IMstProperties	
MstForceVersion	
MstCfgIdFmtSel	
MstExternalRootCost	
MstMaxInstances	
MstCfgIdName	
MstCfgIdRevLevel	
IMO Name—IStpInstanceInfo	
Object Identification	
StpBridgeId	
BridgePriority	
Designated Parent and Root Bridges	
StpRootCost	
IsRoot	
StpRootPort	
StpPortInfoTable	
STP Instance Id	
Vlan Id	
StpDesignatedBridge	
StpDesignatedRoot	
IMO Name—IMstInstanceInfo	
MstVlanIds	
Same as IStpInstanceInfo	
IMO Name—IPvstpInstanceInfo	
Protocol Type	

Table 10-7 Ethernet Attribute Support on Generic Devices—Cisco Prime Network 3.9 (continued)

Attribute	Generic
StpBridgeMaxAge	
StpBridgeHelloTime	
StpBridgeForwardDelay	
StpProtocolSpecification	
StpVlanId	
StpForwardDelay	
StpMaxAge	
IMO Name—IRstpInstanceInfo	
StpForceVersion	
Same as IStpInstanceInfo	
IMO Name—IStpPortInfo	
StpPort	
StpPortPriority	
StpPortState	
StpPortPathCost	
StpPortEdgePort	
StpPortPointToPoint	
StpPortRole	
StpDesignatedPortIdentifier	
StpDesignatedBridge	
StpPortIdentifier	
StpPortBpduGuardState	
StpPortBpduFilterState	
IMO Name—IMstPortInfo	
MstPortHelloTime	
Same as IStpPortInfo	
IMO Name—IPvstpPortInfo	
PvstpPortFastState	
IMO Name—IEthernetChannel	
Group Number	
Bandwidth	
Aggregation Protocol	
IANA Type	
Containing CTPs	
Contained CTPs	

Table 10-7 Ethernet Attribute Support on Generic Devices—Cisco Prime Network 3.9 (continued)

Attribute	Generic
Mac Address	
Admin Status	
Oper Status	
IMO Name—ITokenRingLayer2	
MAC Address	
IANA Type	
Containing CTPs	
Contained CTPs	
IMO Name—ITokenRingLayer1	
Same as IPhysicalLayer	
IMO Name—IVtpService	
Version	
OperatingMode	
DomainName	
ConfigurationRevision	
isPruningEnabled	
isAuthenticationEnabled	
IMO Name—IREPService	
version	
administrativeVlan	
notificationEnabled	
IMO Name—IREPSegmentInfo	
segmentId	
segmentComplete	
IMO Name—IREPPortInfo	
portName	
portKey	
segmentId	
portType	
portRole	
operStatus	
blockedVlans	
preemptTimer	
lslAgeoutTimer	
remoteDeviceName	

Table 10-7 Ethernet Attribute Support on Generic Devices—Cisco Prime Network 3.9 (continued)

Attribute	Generic
remoteDeviceMac	
remotePortName	
IMO Name—IBridgeILan	
Id	
IMO Name—IIBBridgeEntry	
IS Id	
IBridge	
BBridge	

Hardware

Table 10-8 Hardware Attribute Support on Generic Devices—Cisco Prime Network 3.9

Attribute	Generic
IMO Name—IChassis	
Description	
Equipment Holder Type	
Contained Equipment Holders	
Contained Equipments	
Serial Number	
IMO Name—IShelf	
Description	
Status	
Equipment Holder Type	
Contained Equipment Holders	
Contained Equipments	
Serial Number	
IMO Name—IModule	
Module Name	
Module Description	
Software Version	
Operational Status	
Hardware Type + Version	
Managed IP Address	

Table 10-8 Hardware Attribute Support on Generic Devices—Cisco Prime Network 3.9

Attribute	Generic
Redundant Equipment	
Configured Redundancy	
Redundancy Status	
Operational Status Last Changed	
Supported Physical Termination Points	
Serial Number (soft property)	
Slots Number	
IMO Name—IManagedElement	
IP Address	Y
Communication State	Y
Investigation State	Y
Element Category	Y
Element Type and Key	Y
Device Name	Y
System Name	Y
System Description	Y
Up Time	Y
Software Version	Y
Vendor Identity	
Memory and CPU Usage	
DRAM Free	
DRAM Used	
Flash Device Size	
NVRAM Size	
Processor DRAM	
Sys Contact	
Sys Location	
Serial Number	
File Systems	
IMO Name—IContext	
Name	
Bounded Connections	
IP Address Pools	
Forwarding Components List	

Table 10-8 Hardware Attribute Support on Generic Devices—Cisco Prime Network 3.9

Attribute	Generic
Traffic Descriptors List	
Tunnel Containers List	
Data Link Aggregation Containers List	
IMO Name—ISystemService	
Type	
Status	
Up Time	
IMO Name—IBridge	
Bridge Table	
Type	
MAC Address	
IP Interface	
Name	
Logical Sons	
Vlan Type	
IMO Name—IBridgeEntry	
Destination MAC	Y
Outgoing Interface	Y

Serial

Table 10-9 Serial Attribute Support on Generic Devices—Cisco Prime Network 3.9

Attribute	Generic
IMO Name—IPhysicalLayer	
Media Type	
Clocking Source	
Maximum Speed	Y
Is Internal Port	
Discarded Bandwidth	
Dropped Bandwidth	
Input Bandwidth	
Output Bandwidth	

Table 10-9 Serial Attribute Support on Generic Devices—Cisco Prime Network 3.9 (continued)

Attribute	Generic
Discarded and Received Input Data Counters	Y
Dropped and Forward Output Data Counters	Y
Administrative Status	Y
Operational Status	Y
Last Changed	Y
IANA Type	
Containing CTPs	
Contained CTPs	
Port Alias	
Location	
Sending Alarms	
Connector Description	
Part ID	
Connector Serial Num	
Product	
Status	
Managed	



PART 2

Technology Support



CHAPTER 11

Supported Technologies

This chapter outlines the technologies supported in Prime Network 3.9. Supported technologies are listed in Table 11-1. Technology support that was introduced in Prime Network 3.9 is marked as such in the table. The fact that a specific technology is listed in Table 11-1 does not imply that every aspect of every relevant standard is represented and supported. In addition, the specific level of support provided for a particular technology on individual network elements can vary. For details on technology support on individual VNEs, see Part 1—Cisco VNEs.

The supported technologies table indicates the level of support that Prime Network provides for the various technologies, as follows:

- Element modeling—Device-level inventory, support for events.
- Network modeling—Support for flows (correlation, path trace).
- Topology view—Technologies for which links are auto-discovered, and technologies that can be viewed in the context of topological links in a map.

Note Please refer to the Prime Network Technology Center on Cisco Developer Network (CDN) for information about technology IMOs and their attributes.

Table 11-1 Supported Technologies

Technology Family	Technology Group	Technology	Element Modeling	Network Modeling	Topology View
Network (Layer 3)	IP	IP (including IPv6)	Yes	Yes	
		Address Resolution Protocol (ARP)	Yes	Yes	
		Hot Standby Router Protocol (HSRP)	Yes		
		Generic Routing Encapsulation (GRE)	Yes	Yes	Yes
		Carrier Grade NAT	Yes		
		IP SLA Responder	Yes		
		6PE	Yes	Yes	
		6RD	Yes		
		X-LAT	Yes		
		Access Control Lists (ACLs)	Limited		
		VRRP	Yes		
	Routing Protocols	Border Gateway Protocol (BGP), Multiprotocol extensions (MP-BGP), external BGP (eBGP), internal BGP (iBGP)	Yes	Yes	Yes
		Open Shortest Path First (OSPF) and OSPFv3	Yes		
		Intermediate System to Intermediate System (IS-IS)	Yes		
	VPN and VRF	Virtual Routing and Forwarding (VRF)	Yes	Yes	Yes
		VRF-Lite (Multi-VRF)	Yes	Yes	
		VPN		Yes	Yes
		CSCVPN	Yes		
		6VPE	Yes	Yes	Yes
	BFD	Bidirectional Forwarding Detection	Yes		Yes
	SBC	Session Border Controller	Yes		

Table 11-1 Supported Technologies (continued)

Technology Family	Technology Group	Technology	Element Modeling	Network Modeling	Topology View
Hybrid Network/ Data Link (Layers 3 and 2)	MPLS	Multiprotocol Label Switching (MPLS)	Yes	Yes	Yes
		Label Distribution Protocol (LDP)	Yes		
	MPLS TP	MPLS TP	Yes	Yes	Yes
	MPLS TE	Multiprotocol Label Switching Traffic Engineering (MPLS TE)	Yes	Yes	Yes
		P2MP (Point-to-Multipoint) TE			
		MPLS TE Fast Reroute (MPLS TE FRR)	Yes		
	Pseudowire	Pseudowire Emulation Edge to Edge (PWE3)	Yes	Yes	Yes
		VCCV	Yes		
		Pseudowire Redundancy	Yes		
		Static Pseudowire	Yes		
		TDM Pseudowire	Yes	Yes	Yes
		Multi-segment Pseudowire	Yes	Yes	Yes
		ATM over Pseudowire (ATM PW)	Yes	Yes	Yes
		PW-to-TP Tunnel Mapping	Yes	Yes	
		PW-to-TE Tunnel Mapping	Yes	Yes	
	Clocking	IE1588	Yes		
		SyncE	Yes		
		ACR	Yes		

Table 11-1 Supported Technologies (continued)

Technology Family	Technology Group	Technology	Element Modeling	Network Modeling	Topology View
Data Link/MAC (Layer 2)	Ethernet	Ethernet (IEEE 802.3)	Yes	Yes	Yes
		VLAN (IEEE 802.1Q)	Yes	Yes	Yes
		QinQ (IEEE 802.1ad)	Yes	Yes	
		LAG (IEEE 802.3ad)	Yes	Yes	Yes
		Ethernet Channel	Yes	Yes	Yes
		STP (IEEE 802.1D)	Yes		Yes
		RSTP (IEEE 802.1w)	Yes		Yes
		PvSTP	Yes		Yes
		MST (IEEE 802.1s)	Yes		Yes
		SVI	Yes		
		VTP	Yes		
		REP	Yes		Yes
		VPLS	Yes	Yes	Yes
		H-VPLS	Yes	Yes	Yes
		VSI	Yes	Yes	Yes
		PBB	Yes		
		EFP	Yes	Yes	Yes
		Access Gateway	Yes		
		mLACP (Iccp Redundancy Group)	Yes		
	Ethernet OAM	CFM (Cisco and Draft 8.1)	Yes		
		Link OAM	Yes		
		Ethernet LMI	Yes		
	ATM	ATM	Yes	Yes	
		IMA	Yes	Yes	
		ATM Cross-Connect	Yes	Yes	
		ATM OAM	Yes		
		IP over ATM (MPoA 1483R)	Yes	Yes	
		Ethernet over ATM (MPoA 1483B)	Yes	Yes	
	Frame Relay	Frame Relay	Yes	Yes	
	ISDN	Integrated Services Digital Network (ISDN)	Minimal		
	PPP	Point To Point Protocol (PPP)	Yes	Yes	
		PPPoA, PPPoE, PPPoFR	Yes		

Table 11-1 Supported Technologies (continued)

Technology Family	Technology Group	Technology	Element Modeling	Network Modeling	Topology View
Data Link/MAC (Layer 2)	Discovery Protocols	CDP, LLDP	Yes		
	L2TP	L2TP	Minimal		
	Local Switching	Local Switching	Yes	Yes	
Physical Layer (Layer 1)	xDSL	Digital Subscriber Line (xDSL)	Yes		
	IPoDWDM	Internet Protocol over Dense Wave Division Multiplexing (IPoDWDM)	Yes	Yes	
	SONET/SDH	SONET/SDH	Yes		
	TDM/DSx	TDM	Yes		
		DSx	Yes		
		CEM	Yes		
		T3/E3	Yes		
		Channelized T3, OC3, DS3 interface	Yes		
	Serial	Serial	Yes		
	Hardware	Pluggable Transceiver	Yes		
Mobility (3.9)	GGSN	GGSN	Yes		
	APN	APN	Yes		
	GTPU	GTPU	Yes		



CHAPTER 12

Prime Network VNE Topology

This chapter describes the types of topologies Prime Network supports and how Prime Network discovers and displays them, as follows:

- Supported Topology Types, page 12-1
- Discovery Techniques, page 12-6

Supported Topology Types

The following topology types are supported by Prime Network 3.9:

- ATM
- BFD
- BGP
- Business
- Ethernet
- LAG
- Frame Relay
- MPLS
- PPP or HDLC
- MLPPP
- VLAN
- Physical Layer
- Pseudowire
- GRE Tunnel
- VPN
- VLAN Service Links
- MPLS-TE Tunnel
- MPLS-TP Tunnel

ATM

ATM topology represents a link between two ATM ports which are connected in the network. In the VNE model, the endpoints of the link are ATM IMOs (ATM Interface (IAtm)) which represent the ATM port or interface.

Link type: ATM or PNNI

Discovery technique for ATM link:

- ATM VC Counters
- CDP (Cisco Discovery Protocol)
- Static

Verification Technique: Physical Layer Counters

Discovery technique for PNNI link:

- PNNI Information

BFD

BFD topology represents a BFD session with verified BFD connectivity between two endpoints in the network. In the VNE model, the endpoints of the link are the BFD Service IMOs (BFD Service (IBfdService)), which represent the BFD service running on the router.

Link type: BFD

Discovery and verification technique: BFD Session Source and Destination

BGP

BGP topology represents a TCP connection between two BGP entities which facilitate the “BGP neighborhood” in the network. In the VNE model, the endpoints of the link are the MPBgp IMOs (Multi Protocol BGP Entity), which represent the BGP service running on the router.

Link type: BGP

Discovery and verification technique: BGP Information

Business

Business topology does not represent any specific link or relationship in the network. It can represent the relationship between any two objects in the model, which can be business objects or network objects. These links are created in the Prime Network gateway.

Ethernet

Ethernet topology represents a link between two Ethernet ports which are connected in the network. In the VNE model the endpoints of the link are Ethernet IMOs (Ethernet Interface (IEthernet)), which represent the Ethernet ports.

Prime Network conducts discovery of Ethernet data link layer topology by using various types of data. This includes information from, for example, OAM, CDP, LLDP, STP, and can include MAC learning information. All types of data are collected and, based on priority, used to verify the adjacency between two ports.

Many service providers configure customer access to VLAN ports using L2PT. This avoids the need to process Layer 2 protocols such as CDP. In these scenarios, discovery may create links between ports which are not directly connected, because the Layer 2 protocol information is tunneled and does not reflect the actual physical links. This problem can be overcome by configuring static links on these ports. These static links will override any incorrect dynamically discovered links.

Link type: Ethernet

Discovery techniques:

- OAM
- MAC
- CDP (Cisco Discovery Protocol)
- LLDP (Link Layer Discovery Protocol)
- STP (Spanning Tree Protocol)
- REP
- Static

Verification Technique: All of the above discovery techniques and Physical Layer Counters.

LAG

LAG topology represents a link between two LAG or EtherChannel ports which are connected in the network. The underlying physical links do not have to be discovered for the LAG link to be discovered.

In the VNE model the endpoints of the link are indicated in the Data Link Aggregation Container (IDataLinkAggregationContainer) IMO, which points to the LAG or EtherChannel ports.

Link type: LAG

Discovery and verification techniques:

- MAC
- STP (Spanning Tree Protocol)
- REP
- LACP
- Static

Frame Relay

Frame Relay topology represents a link between two Frame Relay ports which are connected in the network. In the VNE model the endpoints of the link are FrameRelay IMOs (Frame Relay Interface (IFrameRelay/IFrTrunk)), which represent the Frame Relay ports.

Frame Relay links between Cisco devices with CDP enabled can be discovered dynamically. For all other cases, static or manual configuration can be used.

Link type: Frame Relay

Discovery techniques:

- CDP (Cisco Discovery Protocol)
- Static

Verification Techniques: The above discovery techniques and Physical Layer Counters.

MPLS

MPLS topology represents adjacent MPLS interfaces in the network. These MPLS interfaces forward MPLS (labeled) traffic between them. Labels may be learned using discovery protocols, such as LDP or TDP (Cisco), or may be manually configured. In the VNE model the endpoints of the link are MPLS IMOs (MPLS Interface (IMpls)), which represent the MPLS interfaces.

Prime Network discovers MPLS network layer topology by searching for the existence of the local IP subnet in any one-hop-away remote side's MPLS Interface. In particular, it compares the local and remote IP subnets gathered from the upper IP network layers.

Link type: MPLS

Discovery and verification techniques: IP Testing

PPP or HDLC

PPP or HDLC topology represents a link between two PPP or HDLC ports which are connected in the network. In the VNE model the endpoints of the link are PPP and HDLC IMOs (HDLC Encapsulation (IEncapsulation)), which represent the ports.

Prime Network performs discovery of PPP or HDLC topologies by searching for the local IP subnet in any one-hop-away remote side's PPP or HDLC interface. In particular, it compares the local and remote IP subnets gathered from the upper IP Network layers.

Discovery techniques:

- IP Testing
- CDP (Cisco Discovery Protocol)
- Static

Verification Techniques: The above discovery techniques and Physical Layer Counters.

MLPPP

The Multilink PPP Interface object models a multilink PPP bundle, which is a named virtual interface with multiple member links.

Discovery and Verification Technique: MLPPP Endpoint Identifier.

VLAN

Discovery and Verification Technique: VLAN ID Matching.

Physical Layer

Physical Layer topology represents a link between the physical layers of two ports connected in the network. In the VNE model the endpoints are IMOs which inherit from the physical layer (Layer 1) IMOs (Serial Interface (IPhysicalLayer)), such as SONET/SDH Physical (ISonetSdh) and DS3 Channelized Interface (IDS3PdhChannelized), which represent physical layers of a port.

In Prime Network's topology discovery implementation, physical layer (Layer 1) discovery is coupled with data link layer (Layer 2) discovery. By default, the physical layer does not have techniques for discovery, but rather complements the discovery of Layer 2, in the following ways:

- Ports from the same device are not connected (this validation is done in the physical layer).
- If static topology is configured, it is used in the physical layer.

Pseudowire

Pseudowire topology represents a link between the endpoints of an MPLS-based pseudowire tunnel in the network. In the VNE model the endpoints of the link are PTP Layer 2 MPLS tunnel IMOs (PTP Layer 2 MPLS Tunnel Interface (IPTPLayer2MplsTunnel)), which represent the pseudowire tunnel endpoints.

Prime Network discovers PWE3 Network layer topology by searching for matches between the local and remote router IP addresses in any one-hop-away remote side's PTP Layer 2 MPLS tunnel interface. In particular, it compares the local and remote router IP addresses and tunnel identifications.

Link type: Tunnel

Discovery and verification technique: Pseudowire Information.

GRE Tunnel

GRE Tunnel topology represents a link between the endpoints of a GRE tunnel in the network. In the VNE model the endpoints of the link are TunnelGre IMOs (Generic Routing Encapsulation (GRE) Tunnel Interface (ITunnelGRE)), which represent the GRE tunnel endpoints.

Link type: GRE tunnel

Discovery and verification technique: GRE Tunnel Information.

VPN

VPN topology represents a link between two VRFs that are part of a VPN, meaning that VPN traffic can pass between customer sites connected to these VRFs. In the VNE model the endpoints of the link are VRF IMOs (Virtual Routing Forwarding (VRF) Entity (IVrf)), which represent the VRF forwarding entities in the network element.

Prime Network discovers MPLS-BGP-based VPN network topology by searching for the existence of the local VRF entity's imported route targets in any remote side's VRF entity exported route targets.

Link type: VPN or VPNv6

Discovery and verification techniques: Route Targets for either IPv4 or IPv6 address families.

VLAN Service Links

A VLAN service link represents either an Ethernet or a LAG link in the context of a specific VLAN. It connects two Ethernet Flowpoint entities, which represent Ethernet or LAG ports in the context of a specific VLAN.

The two Ethernet Flowpoints can reside in the same Layer 2 domain, or connect between two different Layer 2 domains when a VLAN TAG manipulation is used.

VLAN service links are not discovered via the standard topology mechanism which resides in the VNE layer, but rather by the Carrier Ethernet discovery. The discovery mechanism uses Ethernet and LAG links, VNE inventory modeling information of the Ethernet/LAG interfaces, and Ethernet Flowpoint entities as inputs for the VLAN service link discovery process.

MPLS-TE Tunnel

MPLS-TE Tunnel topology represents a unidirectional link between the TE tunnel interface, which is the head of the TE tunnel, and the Label Switching Entity (LSE), which is the tail of the TE tunnel. The head of the TE tunnel is represented by the IMplsTETunnel IMO, and the tail of the TE tunnel is represented by the ILSE IMO, which is the MPLS forwarding component on the destination VNE.

MPLS TE tunnels also have mid-points, which are not represented in the MPLS-TE tunnel topology.

Link type: MPLS TE. The link is unidirectional and represents a flow from the head to the tail of the TE tunnel.

Discovery and verification techniques: Source IP, Dest IP and Tunnel ID on the head (taken from the MplsTETunnel) is compared with Dest IP, Source IP and Tunnel ID on the tail (taken from the MplsTeTunnelSegments of the LSE).

MPLS-TP Tunnel

MPLS-TP Tunnel topology represents a bidirectional link between two TP tunnel interfaces, which represent the two edges of the TP tunnel.

A TP tunnel interface is represented by the IMPLSTPTunnelEP IMO.

MPLS-TP tunnels also have mid-points, which are not represented as part of the MPLS-TP tunnel topology.

Link type: MPLS-TP. The link is bidirectional.

Discovery and verification techniques: The local information including Global ID, Router ID and TP tunnel ID of one MPLS-TP tunnel edge is compared with the remote Global ID, remote Router ID and remote TP tunnel ID information of another MPLS-TP tunnel edge.

The information is taken from the MPLSTPTunnelEP IMO.

Discovery Techniques

Discovery takes place in two phases:

1. Discovery of existing links.
2. For discovered links, verification that the links still exist.

This section describes the various discovery techniques used by Prime Network, as follows:

- ATM VC Counters
- CDP (Cisco Discovery Protocol)
- LLDP (Link Layer Discovery Protocol)
- PNNI Information
- BFD Session Source and Destination
- BGP Information
- MAC
- REP
- LACP
- OAM
- MLPPP Endpoint Identifier
- GRE Tunnel Information
- Pseudowire Information
- VLAN ID Matching
- Route Targets
- Physical Layer Counters
- IP Testing
- STP (Spanning Tree Protocol)

Note All the supported discovery techniques are enabled by default. Only MAC discovery can be disabled using the registry. See the *Cisco Prime Network 3.9 Administrator Guide* for more information.

ATM VC Counters

Same Active VCs

In this technique, each side identifies a set of active ATM Virtual Connections (VCs) and looks for a match with the same set on another port in the network. An active VC is a VC that has a configured level of traffic.

This technique supports configurations that have either the same VCs or the same VPs on both sides. It does not support a mixture of VCs on one side and VPs on the other side.

VC Traffic Signature

Traffic signature is based on traffic pattern analysis. The underlying assumption of traffic pattern analysis is that network traffic variety ensures that every active link or active ATM VC in the network maintains a differential traffic “fingerprint”.

Consequently, any two connected ports or VCs will have similar trend functions, which can be matched within reliable statistical significance.

CDP (Cisco Discovery Protocol)

For Cisco devices, if CDP is enabled, its information will be used for discovery and verification. This includes any upper layer techniques, such as VC-related techniques in ATM or MAC in Ethernet. In this technique, the matching criteria is the CDP neighbor information.

Please note the following limitations:

- If the port has more than one CDP neighbor, no links will be created.
- Ports in a multi chassis device will not be connected by CDP if there is no entry for them in the CDP neighbors table.

LLDP (Link Layer Discovery Protocol)

If LLDP is enabled, its information will be used for discovery and verification. In this technique, the matching criteria is the LLDP neighbor information.

PNNI Information

In this technique, each port in the ATM switch is identified with two values:

- Node ID.
- Port ID.

BFD Session Source and Destination

In this technique, the BFD session's source and destination addresses are verified by matching them against the source and destination addresses of the potential adjacent neighbors. The matching is session source to neighbor destination and session destination to neighbor source, respectively, as one side's source is the other side's destination. This method assumes that multiple BFD sessions running on the same router cannot have the same source and destination address.

BGP Information

In this technique, for each BGP Neighbor Entry the local BGP identifier is compared to the remote BGP identifier or a potential neighbor. This topology technique assume uniqueness of the BGP identifier in the network.

MAC

In this technique, the Ethernet port MAC is checked to see if it is the only one learned on the other Ethernet port (using bridge and ARP tables).

This technique discovers links between two routers and links between the router and switch, but not between two switches (includes the generic VNE).

REP

If REP is enabled between switches, the information that is provided by the 'show REP topology' command is used to connect the topology according to the REP configuration.

LACP

If the LAG is configured as LACP, actor and partner system ID are compared between the two devices (local actor = remote partner and vice versa).

OAM

If OAM is configured between two devices, local and remote OAM MACs are compared between the two devices (local OAM MAC = remote OAM MAC and vice versa).

This protocol has the highest priority and hence will be the first to be checked if it is enabled.

MLPPP Endpoint Identifier

In this technique, the Local and the Remote MLPPP End Point Identifier are verified by matching them against the Remote and the Local MLPPP End Point Identifier of the potential adjacent neighbors.

The matching is from the Local MLPPP End Point Identifier to the neighbor Remote MLPPP End Point Identifier respectively.

GRE Tunnel Information

GRE Tunnel Information—In this technique, each GRE tunnel is identified by the following criteria:

1. Source IP.

2. Destination IP.

Matching between two tunnels T1 and T2 is done by comparing the T1 source to the T2 destination and the T1 destination to the T2 source.

Pseudowire Information

In this technique, each pseudowire is identified by the following criteria:

- Local and Remote router IP.
- Tunnel ID.

Matching between two pseudowire tunnels Pw1 and Pw2 is conducted by comparing:

- The Pw1 local IP to the Pw2 remote IP and the Pw1 remote IP to the Pw2 local IP.
- Tunnel ID.

VLAN ID Matching

In this technique, the VLAN configuration aspects of each pair of VLAN-enabled physically connected Ethernet ports will be inspected to identify which VLAN tagged traffic crosses this link. The type of VLAN configurations that are inspected include:

- Switchport in all configuration modes (Access, Trunk, Dot1q_Tunnel), including the VLAN allowed and VLAN mapping.
- L2 sub-interfaces/service instances configured on the Ethernet port, specifically the VLAN tag matching criteria.
- L3 sub-interfaces configured on the Ethernet port, specifically the VLAN tag matching criteria.

Route Targets

Route Targets—In this technique, each VRF is identified with the set of its import and export route targets (for either IPv4 or IPv6 address families).

The matching criteria between two VRF entities will be matching at least one pair of import or export route targets of the one VRF to the export or import route targets of the other VRF.

Physical Layer Counters

The physical layer is used for topology verification (that is, if a link has already been discovered, it is tested periodically). This verification is done in the physical layer using counters. Physical layer counters are based on the port traffic signature, using octet-based or octet- and packet–based traffic.

IP Testing

Prime Network uses IP testing (IPv4) to discover the topology for PPP/HDCL and MPLS technologies. In both cases, the IP test checks the IP configuration on the relevant interface(s) and verifies that there is a match. In this context, finding a match means that the IP configuration is compared using the *primary* IP subnet configured on the local and remote interfaces, and the local IP subnet is equal to or contained in the remote IP subnet.

Note that there is an inherent limitation in using only the primary address and mask to define the IP subnet to be compared. This can cause issues if two interfaces are connected but have more than one address and, in either or both cases, the primary is from a different subnet. For example: We have two devices, Device1 and Device2. POS2/1 on Device1 is connected to POS1/1 on Device2. Device1's configuration is:

```
interface POS2/1
 description Connected to POS1/1 on Device2
 encapsulation ppp ip address 10.0.0.1 255.255.255.252
 ip address 11.0.0.1 255.255.255.252 secondary
```

Device2's configuration is:

```
interface POS1/1 description Connected to POS2/1 on Device1
 encapsulation ppp ip address 11.0.0.2 255.255.255.252
 ip address 10.0.0.2 255.255.255.252 secondary
```

In this case, the two devices will *not* be connected.

STP (Spanning Tree Protocol)

If STP is enabled between switches, the STP port information is used in the following way: bridge ID, designated bridge, and port identifier are compared with the relevant remote information. If a match is found, a link is created.

This STP discovery technique will work correctly only when the same STP protocol is running on both ports.



PART 3

Alarms and Events



CHAPTER 13

System Events

This section describes the Prime Network system events. System events appear in the Prime Network Events System tab. They include a variety of events pertaining to the system activities, from alarm thresholds to disk space and AVMs. Prime Network system events and system event messages are listed in the following tables:

- System events—Table 13-1 on page 13-1
- System event messages—Table 13-2 on page 13-12

For definitions of system event terms and acronyms, see Table 13-3 on page 13-13. For information about Prime Network Events, see the *Cisco Prime Network 3.9 User Guide.*

Table 13-1 Prime Network System Events

Source OID	Message	Severity	Cause	Action
Category: MCReachability				
IMC	Agent *vne_name, agent_ip* is reachable: DNA Unit = *unit_ip* AVM =*avm_id*	CLEARED	The VNE is reachable.	None needed.
IMC	Agent *vne_name,agent_ip* is unreachable: DNA Unit = *unit_ip* AVM = *avm_id*	MINOR	Various causes; system or network failure.	Contact Cisco Support.
IAvm	AVM *unit_ip: avm_id* (*avm_key*) is reachable	CLEARED	The AVM is reachable.	None needed.
IAvm	AVM *unit_ip:avm_id* (*avm_key*) is unreachable	MINOR	Network or machine failure.	Contact Cisco Support.
IMC	Unit *unit_ip* reachable	CLEARED	The MC is reachable.	None needed.
IMC	Unit *unit_ip* unreachable	MINOR	System, network, or machine failure.	Contact Cisco Support.
Category: alarm threshold				
IAvm	Ticket archiving initiated - Maximum ticket limit exceeded **Long Description** About to archive tickets *active tickets*. Removed tickets OIDs detailed in Archiving tickets system events.	CRITICAL	There are too many tickets open in the system.	Remove (archive) tickets.

Table 13-1 Prime Network System Events (continued)

Source OID	Message	Severity	Cause	Action
IAvm	Approaching maximum ticket limit **Long Description** Active tickets passed threshold of *threshold*.	WARNING	The number of open tickets is approaching the limit.	None needed.
IAvm	Ticket archiving as a result of exceeding maximum ticket limit has completed **Long Description** Following tickets exceeded the ticket threshold and have been archived:*tickets*.	INFO	System has finished archiving the tickets.	None needed.
Category: backup				
IAvm	Unable to back up the database because the database is not in archive mode	MAJOR	The database is not configured to work in archive log mode so the database cannot be backed up.	Change the database to archive log mode.
IAvm	Unable to delete directory:*path*	MAJOR	Permission problems.	Check the directory permissions.
IAvm	Unable to delete file:*name*	MAJOR	Permission problems.	Check the file permissions.
IAvm	Error deleting files from:*path*	MAJOR	Permission problems.	Check the permissions of the directory that contains the files and the permissions on the files.
IAvm	Error deleting files from:*path*	MAJOR	Permission problems.	Check the file permissions.
Category: bad alarms				
IAvm	Found alarms that do not refer to any network element in the system. Deleting *count* alarms.	MINOR	Element removed without first removing its alarms.	The system is removing the relevant alarms.
Category: bad oid				
IAvm	*count* bad oids found in table businessObject	CRITICAL	Bad business objects were inserted into the database.	The system is removing the bad business objects that were inserted into the database.

Table 13-1 Prime Network System Events (continued)

Source OID	Message	Severity	Cause	Action
Category: bos misconfiguration				
IElementManagement	*duplicate_value* is configured as *existing_element* in Unit *unit_ip* AVM *avm_id* and also as *new_element* in Unit *new_unit_ip* AVM *new_avm_id*	MAJOR	XML files were edited manually and incorrectly. Note: The existing element is a VNE. The duplicate value is either the name or the IP address of the VNE.	Fix the XML file. Remove conflicting entry.
Category: drop affected				
IAvm	Dropping affected Message of size:*size* the total affected waiting to be saved is:*count*	CRITICAL	The system was shut down while removing affected messages.	The system removes the remaining affected messages.
Category: free space				
IAvm	No room for tablespace *tablespace_name* on the disk	CRITICAL	There is no free space on the disk partition that the database occupies.	Free some space on the disk partition.
IAvm	No room for *object_name* in tablespace *tablespace_name*	MINOR	There is not enough free table space to accommodate growth in the table space.	The system will increase the table space when the table needs to grow.
Category: license				
MCNetwork	No license file exists (Evaluation system).	WARNING	Prime Network is installed without a license file; it is an evaluation system. The message occurs whenever the license file is: • Missing. • Invalid signature. • Locked on another MAC or host. • All features are expired.	Contact your Cisco representative to get a license file.
MCNetwork	Exceeding feature usage (Limited license. Either counted or expired).	WARNING	The license for some feature is either expired or usage exceeded.	Contact your Cisco representative to renew or modify the license for this feature.
IAvm	Prime Network is unlicensed **Long Description** The *x*-day evaluation period is over. To use Prime Network, a valid license must be acquired. The client will now close.	CRITICAL	You are using a Prime Network client without a license. The evaluation period is expired.	Purchase a valid Prime Network license.

Table 13-1 Prime Network System Events (continued)

Source OID	Message	Severity	Cause	Action
IAvm	Evaluation Usage **Long Description** Prime Network is in evaluation mode with *x* of *y* days remaining. A valid license must be acquired before the end of the evaluation period in order to continue working with Prime Network.	WARNING	You are using a Prime Network evaluation license that expires in *x* days.	Purchase a valid Prime Network license before the end of the evaluation period.
IAvm	UI Violation **Long Description** The number of concurrent UI client windows exceeds the license. Current violations count *x*.	WARNING	The number of concurrent UI client windows exceeded the allowance.	Purchase an additional UI license.
IAvm	UHS Violation **Long Description** The number of hot standby units exceeds the license. Current violations count *x*.	WARNING	The number of hot standby units exceeded the license.	Purchase an additional Unit Hot Standby (UHS) license.
IAvm	RTM Device Usage feature violation **Long Description** The following device groups are missing counted license: Device group *device group*.	WARNING	The number of devices in use exceeded the allowance of the device group or a device in the group attempted to perform a function for which it has no functional tier license.	Purchase an additional RTM license.
IAvm	RTM File Violation **Long Description** RTM file violation detected. Reason: *reason*.	WARNING	The RTM file is missing or not properly signed (for example, if someone manually edited the license file).	Purchase additional licenses or rectify the problem.
IAvm	Lab Usage	WARNING	The installation of Prime Network is compliant only for lab usage and cannot be used in production network.	None needed.
Category: no stacktrace				
IAvm	Session discard a msg due to an exception *exception_msg*	MAJOR	An exception occurred while handling an internal message.	If this event recurs frequently, check the logs for the exception type.
Category: partitioning				
IAvm	EMPTY partition contains data.	CRITICAL	EMPTY partition of *TABLE_NAME* table contains data.	Contact Prime Network Support team.

Table 13-1 Prime Network System Events (continued)

Source OID	Message	Severity	Cause	Action
IAvm	Query of EMPTY partition failed.	CRITICAL	Prime Network is unable to determine whether EMPTY partition of *TABLE_NAME* table contains data.	Contact Prime Network Support team.
Category: session timeout				
IAvm	Session creator *creator* has timed out (session XID=*session_xid*)	MINOR	The response to the last ping message was longer than the threshold time. This can result from delays and errors in the network or the application.	Notify Cisco Support (low priority).
Category: tickets capacity				
IAvm	Excessively large tickets detected **Long Description** The system contains the following *tickets* ticket(s) with more than 150 events per alarm. You can manually archive these tickets or the system will automatically archive them in: 15 minutes.	WARNING	System has discovered large tickets. A large ticket is a ticket raised with 150 events per alarm.	You can manually archive the tickets. If you do not respond within 15 minutes, Prime Network archives the tickets.
IAvm	Limit of excessively large tickets reached **Long Description** There are more than *x* excessively large tickets in the system (tickets with more than 150 events per alarm).	CRITICAL	System found more than *x* large tickets.	You can manually archive the tickets. If you do not respond within 15 minutes, Prime Network archives the tickets.
Category: user disabled				
IAvm	Too many failed login, user disabled *username*	MINOR	Too many failed login attempts caused Prime Network to disable the username.	Investigate the reason for the user login failures. If the reason was legitimate, reset the user profile to enabled.
Category: Device System Events				
IElement Management	Agent *agent_ip* is not loading because of incorrect polling group. BOS Unit = *unit_ip* AVM = *avm_id*	MINOR	The polling group defined while adding the agent does not exist or is corrupt.	Verify the polling group definition and specify the correct polling group.

Table 13-1 Prime Network System Events (continued)

Source OID	Message	Severity	Cause	Action
IElement Management	Configuration Error - Duplicate IP [*existing_ip*]. Will unload device.	CRITICAL	The error can occur when: • A duplicate agent IP was added by mistake, even if the management IP address on the device is different; or • Two devices have a duplicate management IP address and two agents for these two devices were added.	Remove the agent with the duplicate IP, rectify that on the device, and then add the agent again.
IElement Management	Configuration Error - Duplicate Key [*existing_key*]. Will unload device.	CRITICAL	Prime Network found a duplicate device key and will unload the device.	Assign a unique key to the device, then reload it.
IElement Management	Agent *agent_ip* is starting. BOS Unit = *unit_ip* AVM = *avm_id*	MINOR	The specified VNE is starting.	None needed.
IElement Management	Agent *agent_ip* is shutting down. BOS Unit = *unit_ip* AVM = *avm_id*	MINOR	The specified VNE is shutting down.	None needed.
IElement Management	Agent *agent_ip* not responding: BOS Unit = *unit_ip* AVM = *avm_id*	MAJOR	The specified VNE is not responding.	Check AVM logs for any errors or memory issues.
IElement Management	Agent *agent_ip* suppressed: BOS Unit = *unit_ip* AVM = *avm_id*	MAJOR	The specified VNE is not responding. Efforts to restart the VNE have failed, so Prime Network is now suppressing the VNE.	Check the VNE and restart manually.
IElement Management	Out of Memory	CRITICAL	The AVM memory is insufficient.	Increase the amount of memory allocated to the AVM.
Category: AVM System Events				
IAvm	AVM *avm_id* is starting. BOS Unit = *unit_ip*	MINOR	The specified AVM is starting.	None needed.
IAvm	AVM *avm_id* is shutting down.BOS Unit = *unit_ip*	MINOR	The specified AVM is shutting down.	None needed.
IAvm	AVM *avm_id* suppressed: BOS Unit = *unit_ip* AVM = *avm_id*	MINOR	The specified AVM is not responding and the efforts to restart it have failed multiple times. Prime Network is now permanently suppressing the AVM.	Check AVM logs for any evident errors, rectify those errors, and restart manually.
IAvm	AVM *avm_id* not responding: BOS Unit = *unit_ip* AVM = *avm_id*	MAJOR	The specified AVM is not responding.	Check AVM logs for any evident errors, rectify those errors, and restart manually.

Table 13-1 Prime Network System Events (continued)

Source OID	Message	Severity	Cause	Action
IAvm	Memory usage normal	CLEARED	The amount of memory the AVM consumes has returned to normal (occurs only after usage was set to HIGH).	None needed.
IAvm	Memory usage high	WARNING	The amount of memory the AVM consumes exceeded the HIGH threshold (set as a percentage of total memory; default is 85%).	Consider increasing the amount of memory for this AVM.
IAvm	AVM *avm_id* started. BOS Unit = *unit_ip*	MINOR	The specified AVM has started.	None needed.
IAvm	AVM *avm_id* shut down.BOS Unit = *unit_ip*	MINOR	The specified AVM has shut down.	None needed.
IAvm	An outgoing *frame_type* frame to *port_peer_description* was dropped	MAJOR	There is insufficient buffer space for outgoing transport frames.	Note the CPU usage of the machine and then contact Cisco Support.
IAvm	*repeat_count_frames* were dropped in the last *time* seconds - for example an outgoing *frame_type* frame to *port_peer_description*	MAJOR	There is insufficient buffer space. Repeated events were suppressed to avoid an event storm.	Note the CPU usage of the machine and then contact Cisco Support.
IAvm	A deserialization error occurred: class version error while deserializing a *frame_type_name* frame from *transport_string* to *transport_string*:*class_name*	MAJOR	Code incompatibility exists between the source's AVM and the target's AVM.	Contact Cisco Support.
IAvm	*deserialization_error_repeat_count* deserialization errors occurred in the last *time* seconds - for example: class version error while deserializing a *frame_type_name* frame from *transport_string* to *transport_string*:*class_name*	MAJOR	A code incompatibility exists; repeated events were suppressed.	Contact Cisco Support.
Category: Unit System Events				
IMC	Server *unit_ip* manual failover initiated. Raising Redundant machine = *redundant_unit_ip*	CRITICAL	A manual failover was requested for unit *unit_ip*. Prime Network is attempting to start the specified standby machine.	None needed.
IMC	Server *unit_ip* not responding. Raising Redundant machine = *redundant_unit_ip*	CRITICAL	A manual failover was requested for unit *unit_ip*. Prime Network is attempting to start the specified standby machine.	None needed.
IMC	Server *unit_ip* manual failover initiated. No Redundant machine available.	CRITICAL	The High Availability service cannot service the failover request because it cannot find an assigned standby machine.	Assign a machine to serve as a standby unit.

Table 13-1 Prime Network System Events (continued)

Source OID	Message	Severity	Cause	Action
IMC	Server *unit_ip* not responding. No Redundant machine available.	MAJOR	The High Availability service cannot service the failover request because the assigned standby machine *unit_ip* is not responding and there is no machine assigned to replace it.	Assign a machine to serve as a standby unit.
IMC	Registry Possibly out of Sync.	WARNING	The Registry service has detected that the registry is not synchronized with the golden source.	Reload the unit.
IMC	BOS Unit *unit_ip* is starting.	MINOR	The specified unit is starting.	None needed.
IMC	BOS Unit *unit_ip* is shutting down.	MINOR	The specified unit is shutting down.	None needed.
IMC	Uplink to *peer_host_address/peer_AVM_id* disabled	MINOR	The administrator disabled the uplink to the specified host or peer AVM.	None needed.
IMC	Uplink to *peer_host_address/peer_AVM_id* enabled	MINOR	The administrator disabled the uplink to the specified host or peer AVM.	None needed.
IMC	Uplink to *peer_host_address/peer_AVM_id* connected	MINOR	The uplink connection with the specified host or peer AVM was established.	None needed.
IMC	Uplink to *peer_host_address/peer_AVM_id* down	MINOR	The uplink to the specified host or peer AVM was lost.	Look for IP connectivity problems.
Category: CE-Service Discovery				
MCVM	*Service has been stopped* **Long Description** *Timeout occurred while retrieving data from the database.*	MAJOR	Discovery service was stopped due to multiple timeouts of a database query.	Fix the database timeouts root cause. Manually restart the discovery service.
Category: Topology Discovery				
MCVM	Physical Link discovery inconsistent **Long Description** Physical Link discovery of Port *ipPort* using *connectTechnology* information conflicts with verification based on *disconnectTechnology* information. You are strongly recommended to wait until the link disappears and then create a static link from Port *ipPort* to its neighbor.	MAJOR	A flickering link connected, disconnected, and reconnected due to conflicting topology information.	Disconnect the link, wait until the link disappears, and then create a static link.
Category: PortConnector				

Table 13-1 Prime Network System Events (continued)

Source OID	Message	Severity	Cause	Action
IManaged Element	Pluggable transceiver out	MAJOR	Pluggable transceiver was removed.	None needed.
Category: FanTray				
IManaged Element	Fan-tray down	MAJOR	Status of Fan-Tray was changed to down.	None needed.
IManaged Element	Fan-tray out	MAJOR	Fan-Tray was removed.	None needed.
Category:PowerSupply				
IManaged Element	Power-supply down	MAJOR	Status of power-supply card was changed to down.	Change the status of the power-supply card.
IManaged Element	Power-supply Out	MAJOR	Power-supply card was removed	Provide the power supply.
Category: Others				
IAvm	VNE definitions did not load properly **Long Description** VNE definitions did not load properly. Reason: *reason*	CRITICAL	Prime Network was unable to load VNEs.	Check the AVM logs for any evident errors, rectify those errors, and restart manually.
MCVM	Replication Success	INFORMATION	Replication process success.	None needed.
IAvm	*Event number* raw events were dropped.	MAJOR	Network events were dropped due to buffer overflow.	Check the network for the root cause of the event burst.
IAvm	*Event number* network events were dropped.	MAJOR	Database raw events were dropped.	Check the network for the root cause of the event burst.
IAvm	Cannot bind to discovery port.	MAJOR	Prime Network was unable to listen to the specified port.	Remove the link and connect again.
Port OID	REP port role failed. **Long description** REP port *port number* switched from Open to Failed.	MAJOR	Prime Network was unable to listen to the REP port.	Remove the link and connect again.
Port OID	REP port role OK. **Long description** REP port *port number* switched from Failed to Open.	CLEARED	Prime Network was able to listen to the REP port.	None needed.
MCVM	Replication failure - File replication failed	MAJOR	Prime Network was unable to replicate file.	None needed.
MCVM	Replication failure - Database replication failed	MAJOR	Prime Network was unable to replicate database.	None needed.

Table 13-1 Prime Network System Events (continued)

Source OID	Message	Severity	Cause	Action
IAvm	Snmp V3 discovery port bind failure	MAJOR	Prime Network has an SNMP V3 discovery port bind failure.	None needed.
IAvm	Query of EMPTY partition failed. Long description Unable to determine whether EMPTY partition of *TABLE_NAME* table contains data. Please contact your Prime Network administrator	CRITICAL	Prime Network is unable to determine whether empty partition of *TABLE_NAME* table contains data.	Contact Cisco Support.
IAvm	Event Notification Service connection error. Long description Failed to establish *PROTOCOL* connection: Destination DESTINATION. Stopping service *SERVICE_NAME*. The service can be restarted after connection issues are resolved.	MINOR	Prime Network failed to establish protocol connection.	Restart the service after resolving the connection issues.
IAvm	Raw events were dropped	MAJOR	Some network events were not written to the raw events database tables.	None Needed
IAvm	Network events were dropped	MAJOR	Some network events were dropped due to buffer overflow in Eventcollector. This can be caused when incoming event rate is too high for the specs or a mismatch in the configuration of the Eventcollector.	None Needed
IAvm	System Load Change. Long description Subsystem %subsystem% returned to NORMAL operation.	CLEARED	A system load change occured.	None Needed
IAvm	System Load Change Long description Subsystem %subsystem% is operating in running level %level% in order to prevent the system from overloading.	MAJOR	A system load change occured.	None Needed
IAvm	Automatic Overload Prevention - Reports Were Canceled Long description Reports were canceled in order to prevent the system from overloading	MAJOR	An automatic overload prevention has occured and reports were cancelled.	None Needed

Table 13-1 Prime Network System Events (continued)

Source OID	Message	Severity	Cause	Action
IAvm	Automatic Overload Prevention - Network events were dropped Long description Events were dropped in order to prevent the system from overloading: Running level 1 - %running_level_1_drops% events Running level 2 - %running_level_2_drops% events Running level 3 - %running_level_3_drops% events Running level 4 - %running_level_4_drops% events Running level 5 - %running_level_5_drops% events Running level 6 - %running_level_6_drops% events	WARNING	An automatic overload prevention has occured and network events were dropped.	None Needed
IAvm	Event Global Filter Update **Long description** Updated by user:%user%New Configuration:%configuration%	WARNING	An event global filter update has occured.	None Needed
IAvm	The table EVENTSUBTYPEINFO was not able to be loaded. **Long description** The table EVENTSUBTYPEINFO was not able to be loaded due to: %exception%.	MAJOR	Prime Network is unable to load the table EVENTSUBTYPEINFO.	None Needed
IMCVM	Rebuilding unusable index %index name%	INFO	Prime Network is rebuilding unusable index named *index*.	None Needed
IMCVM	Rebuilding index %index name% for partition %partition name%	INFO	Prime Network is rebuilding unusable index named *index* for partition *partition name*.	None Needed
IAvm	Analyzed Test was failed. Please refer to AVM11 log for further troubleshooting	MINOR	Analyzing the database tables statistics has failed.	Refer the AVM11 log for further troubleshooting.

Table 13-1 Prime Network System Events (continued)

Source OID	Message	Severity	Cause	Action
IAvm	%table name% table, partition 'nonarchived' is missing statistics. Please refer to the Cisco Prime Network Administrator guide	MINOR	%table name% table, partition 'nonarchived' is missing statistics.	Follow instructions specified in the *Cisco Prime Network Installation Guide, 3.9.*
IAvm	%table name% table, partition 'nonarchived' statistics are from %analyze date%. Please refer to the Cisco Prime Network Administrator guide.	WARNING	%table name% table, partition 'nonarchived' is missing statistics.	Follow instructions specified in the *Cisco Prime Network Installation Guide, 3.9.*
IAvm	%table name% table, partition 'nonarchived' statistics are from %analyze date%. Please refer to the Cisco Prime Network Administrator guide.	WARNING	%table name% table, partition 'nonarchived' statistics are too old.	Follow instructions specified in the *Cisco Prime Network Installation Guide, 3.9.*
IAvm	%table name% table, partition 'nonarchived' statistics are from %analyze date%. Please refer to the Cisco Prime Network Administrator guide.	MINOR	%table name% table is missing statistics.	Follow instructions specified in the *Cisco Prime Network Installation Guide, 3.9.*

Table 13-2 Error and Event Messages

Description	Cause	Action
The key of AVM *unit_ip:avmid* (*avmeap*) was changed to *newkey*	The Administrator changed the AVM key.	None needed.
Full GC max time exceeded (reached *seconds* seconds)	The system moved some of the heap to the swap.	Increase the amount of physical memory or reduce the amount of memory allocated to the AVM.
AVM not responding, DNA Unit: *unit_ip*, AVM: *avm_id*	The High Availability service determined that the AVM *avm_id* on unit *unit_ip* is not responding.	None needed.
AVM suppressed, DNA Unit: *unit_ip*, AVM: *avm_id*	The High Availability service has suppressed AVM *avm_id* on unit *unit_ip*. This means that the AVM will not be started again automatically.	Resolve the problem that caused the suppression, then restart the AVM manually.
Out Of Memory, DNA Unit: *unit_ip*, AVM: *avm_id*	The specified AVM exceeded its allocated memory.	Assign more memory to the AVM, then restart the AVM.

Table 13-2 Error and Event Messages (continued)

Description	Cause	Action
A message was dropped from *vne_xid*'s mailbox: *message_class* from *XID* to *XID*	There is insufficient buffer space in the message queue of the specified VNE.	Contact Cisco Support.
number messages were dropped in the last *number* seconds – for example this message from *vne_xid*'s mailbox: *message_class* from *XID* to *XID*	There has been insufficient buffer space in the message queue of the specified VNE for the specified time, and repeated events are being suppressed.	Contact Cisco Support.
Cannot bind to discovery port.	Prime Network cannot listen on the specified port. The port is used for SnmpV3 outgoing and incoming engine discovery requests. Hence, incoming SnmpV3 traps might be discarded for some of the devices, and Snmp Inform requests might not work.	None needed.
Raw events were dropped.	Some network events were not written to the raw events database tables. This usually happens due to database connectivity or performance.	None needed.
Network events were dropped.	Some network events were dropped due to buffer overflow in Eventcollector. This can be caused when incoming event rate is too high for the specs or a mismatch in the configuration of the Eventcollector.	None needed.

Table 13-3 defines some common system event acronyms.

Table 13-3 System Event Terms and Acronyms

Term	Definition
AVM	A Prime Network Java process that provides the necessary distribution support platform for executing and monitoring multiple VNEs.
avm_id	AVM identifier
avm_key	AVM key
BOS	Prime Network
DNA	Prime Network
MC	Prime Network unit
VNE	Virtual Network Element



CHAPTER 14

Security Events

This section describes the Prime Network security events. Security events are related to client logins and user activities when managing Prime Network and the Prime Network environment. Table 14-1 lists Prime Network security events. Security events are displayed in the Security tab in Prime Network Events.

For definitions of terms and acronyms used in Table 14-1, see Table 14-2 on page 14-7. For information about Prime Network Events, see the *Cisco Prime Network 3.9 User Guide.*

Table 14-1 Prime Network Security Events

Event Name	Source OID	Short Description	Severity	Cause	Action
Category: Administrator Action					
avm-added	IAvm	AVM <ip>:<avmid> (<avmkey>) was added.	CLEARED	Administrator action.	None needed.
avm-classesjar-changed	IAvm	The class JAR list of AVM <ip>:<avmid> (<avmkey>) was changed to <classesjar>.	CLEARED	Administrator action.	None needed.
avm-disabled	IAvm	AVM <ip>:<avmid> (<avmkey>) was disabled.	CLEARED	Administrator action.	None needed.
avm-enabled	IAvm	AVM <ip>:<avmid> (<avmkey>) was enabled.	CLEARED	Administrator action.	None needed.
avm-high-availability-disabled	IAvm	High availability was disabled for AVM <ip>:<avmid> (<avmkey>).	CLEARED	Administrator action.	None needed.
avm-high-availability-enabled	IAvm	High availability was enabled for AVM <ip>:<avmid> (<avmkey>).	CLEARED	Administrator action.	None needed.
avm-key-changed	IAvm	The key of AVM <ip>:<avmid> (<avmkey>) was changed to <newkey>.	CLEARED	Administrator action.	None needed.
avm-maxmem-changed	IAvm	The maximum heap size of AVM <ip>:<avmid> (<avmkey>) was changed to <maxmem>.	CLEARED	Administrator action.	None needed.
avm-moved	IAvm	AVM <ip>:<avmid> (<avmkey>) was moved to <newip>.	CLEARED	Administrator action.	None needed.
avm-patchjar-changed	IAvm	The patch JAR list of AVM <ip>:<avmid> (<avmkey>) was changed to <patchjar>.	CLEARED	Administrator action.	None needed.

Table 14-1 Prime Network Security Events (continued)

Event Name	Source OID	Short Description	Severity	Cause	Action
avm-removed	IAvm	AVM <ip>:<avmid> (<avmkey>) was removed.	CLEARED	Administrator action.	None needed.
avm-restarted	IAvm	AVM <ip>:<avmid> (<avmkey>) was restarted.	CLEARED	Administrator action.	None needed.
client-license-added	IClient License Management	Client license <key> was added.	CLEARED	Administrator action.	None needed.
client-license-removed	IClient License Management	Client license <key> was removed.	CLEARED	Administrator action.	None needed.
element-added	IElement Management	Element <key> was added to AVM <unitip>:<avmid>.	CLEARED	Administrator action.	None needed.
element-alias-added	IElement Management	The alias <alias> was added to element <key> (in AVM <unitip>:<avmid>).	CLEARED	Administrator action.	None needed.
element-alias-removed	IElement Management	The alias <alias> was removed from element <key> (in AVM <unitip>:<avmid>).	CLEARED	Administrator action.	None needed.
element-disabled	IElement Management	Element <key> (in AVM <unitip>:<avmid>) was disabled.	CLEARED	Administrator action.	None needed.
element-enabled	IElement Management	Element <key> (in AVM <unitip>:<avmid>) was enabled.	CLEARED	Administrator action.	None needed.
element-moved	IElement Management	Element <key> was moved from AVM <unitip>:<avmid> to AVM <newip>:<newavmid>.	CLEARED	Administrator action.	None needed.
element-removed	IElement Management	Element <key> was removed from AVM <unitip>:<avmid>.	CLEARED	Administrator action.	None needed.
mc-network-high-availability-disabled	IMC Network	High availability was disabled for the BOS network.	CLEARED	Administrator action.	None needed.
mc-network-high-availability-enabled	IMC Network	High availability was enabled for the BOS network.	CLEARED	Administrator action.	None needed.
permission-added	IPermission	User <username> was granted permission for scope <scope> with role <role>.	CLEARED	Administrator executed grant permission to user command.	None needed.
permission-deleted	IPermission	User <username>'s permission for scope <scope> was revoked (previous role: <role>).	CLEARED	Administrator executed revoke permission to user command.	None needed.
permission-role-changed	IPermission	User <username>'s role in scope <scope> was changed to <role>.	CLEARED	Administrator executed change role to user command.	None needed.

Table 14-1 Prime Network Security Events (continued)

Event Name	Source OID	Short Description	Severity	Cause	Action
polling-group-added	IPolling Group Management	Polling group <name> (description: <description>) was added.	CLEARED	Administrator action.	None needed.
polling-group-description-changed	IPolling Group Management	The description of polling group <name> was changed to <description>.	CLEARED	Administrator action.	None needed.
polling-group-removed	IPolling Group Management	Polling group <name> (description: <description>) was removed.	CLEARED	Administrator action.	None needed.
polling-interval-added	IPolling Interval	Polling interval <group>/<name> (interval: <interval>) was added.	CLEARED	Administrator action.	None needed.
polling-interval-changed	IPolling Interval	Polling interval <group>/<name> was changed to <interval>.	CLEARED	Administrator action.	None needed.
polling-interval-removed	IPolling Interval	Polling interval <group>/<name> (interval: <interval>) was removed.	CLEARED	Administrator action.	None needed.
protection-group-added	IProtection Group	Protection group <key> (description: <description>) was added.	CLEARED	Administrator action.	None needed.
protection-group-description-changed	IProtection Group	The description of protection group <key> was changed to <description>.	CLEARED	Administrator action.	None needed.
protection-group-removed	IProtection Group	Protection group <key> (description: <description>) was removed.	CLEARED	Administrator action.	None needed.
redundant-unit-added	IMC	DNA Redundant Unit <ip> was added.	CLEARED	Administrator action.	None needed.
scope-created	IScope	Scope <scope> was created.	CLEARED	Administrator executed create scope command.	None needed.
scope-deleted	IScope	Scope <scope> was deleted.	CLEARED	Administrator executed delete scope command.	None needed.
scope-elements-added	IScope	The following elements were added to scope <scope>: <elements>.	CLEARED	Administrator executed add elements to scope command.	None needed.
scope-elements-removed	IScope	The following elements were removed from scope <scope>: <elements>.	CLEARED	Administrator executed remove elements from scope command.	None needed.

Table 14-1 Prime Network Security Events (continued)

Event Name	Source OID	Short Description	Severity	Cause	Action
static-link-added	IStatic Topology Management	A static topology link from <source> to <destination> was added.	CLEARED	Administrator action.	None needed.
static-link-removed	IStatic Topology Management	The static topology link from <source> to <destination> was removed.	CLEARED	Administrator action.	None needed.
transport-uplink-added	IMC Network	A transport uplink was added between <sourceaddress> (local name: <sourcename>) and <destinationaddress> (local name: <destinationname>).	CLEARED	Administrator action.	None needed.
transport-uplink-disabled	IMC Network	The transport uplink between <sourceaddress> (local name: <sourcename>) and <destinationaddress> (local name: <destinationname>) was disabled.	CLEARED	Administrator action.	None needed.
transport-uplink-enabled	IMC Network	The transport uplink between <sourceaddress> (local name: <sourcename>) and <destinationaddress> (local name: <destinationname>) was enabled.	CLEARED	Administrator action.	None needed.
transport-uplink-removed	IMC Network	The transport uplink between <sourceaddress> (local name: <sourcename>) and <destinationaddress> (local name: <destinationname>) was removed.	CLEARED	Administrator action.	None needed.
unit-added	IMC	DNA Unit <ip> was added.	CLEARED	Administrator action.	None needed.
unit-high-availability-disabled	IMC	High availability was disabled for BOS Unit <ip>.	CLEARED	Administrator action.	None needed.
unit-high-availability-enabled	IMC	High availability was enabled for BOS Unit <ip>.	CLEARED	Administrator action.	None needed.
unit-manual-failover	IMC	Manual failover was started in BOS Unit <ip>.	CLEARED	Administrator action.	None needed.
unit-protection-group-changed	IMC	The protection group of BOS Unit <ip> was changed to <protectiongroup>.	CLEARED	Administrator action.	None needed.
unit-removed	IMC	BOS Unit <ip> was removed.	CLEARED	Administrator action.	None needed.
unit-restart	IMC	BOS Unit <ip> was restarted.	CLEARED	Administrator action.	None needed.
unit-restarted	IMC	BOS Unit <ip> was restarted	CLEARED	Administrator action.	None needed.

Table 14-1 Prime Network Security Events (continued)

Event Name	Source OID	Short Description	Severity	Cause	Action
user-created	IBOSUser	User <username> was created	CLEARED	Administrator executed create user command.	None needed.
user-deleted	IBOSUser	User <username> was deleted.	CLEARED	Administrator executed delete user command.	None needed.
user-map-added	IBOSUser	User <username> was granted permission to use map <map>.	CLEARED	Administrator action.	None needed.
user-map-removed	IBOSUser	User <username>'s permission to use map <map> was revoked.	CLEARED	Administrator action.	None needed.
user-password-changed	IBOSUser	User <username>'s password was changed.	CLEARED	Administrator executed change password command.	None needed.
user-property-changed	IBOSUser	The property <property> of user <username> was changed to <value>.	CLEARED	Administrator executed change user property command.	None needed.
execute command	IBOSUser	Unit <ip> was connected.	CLEARED	Administrator connected a Prime Network unit.	None needed.
Category: Insufficient Permissions					
execute command	IAvm	User <user> authenticated successfully.	MAJOR	A user executed a command is successfully authenticated.	None Needed.
execute command	IAvm	Session for user <user> was closed.	MAJOR	A user executed a command with insufficient permissions. Might be a security attack.	Examine the log and identify the user and the command. Take the appropriate action according to organizational security policies.

Table 14-1 Prime Network Security Events (continued)

Event Name	Source OID	Short Description	Severity	Cause	Action
Category: License					
license_cap_exceeded	IAvm	License capacity exceeded for user = <username>, ip = <ip>.	MAJOR	User attempted to log in but is already using the maximum number of connections.	Close some of the user connections to the application.
license_expired	IAvm	License expired for user = <username>, ip = <ip>.	MAJOR	The user's license has expired.	Buy a license or log in as another user.
no_license	IAvm	No license exists for user = <username>, ip = <ip>.	MAJOR	The user does not have a license to use the application.	Buy a license.
Category: Login					
invalid password	IAvm	Invalid password. Couldn't authenticate user <username>.	MINOR	User entered an invalid password.	Enter the password correctly.
invalid user	IAvm	Invalid login. Unknown user <username>.	MINOR	User entered invalid login name.	Enter the login name correctly.
session number exceeded	IAvm	Number of open sessions for user <username> exceeded.	MINOR	User has opened more sessions than allowed.	Increase the number of allowed sessions for this user or do not open so many.
success	IAvm	Successful login <username>.	CLEARED	User entered the correct login information.	None needed.
total number session exceeded	IAvm	Maximum open sessions number exceeded (<maxOpenSessions>).	MINOR	The users of the system have opened too many connections.	Close some of the connections to the system.
user disabled	IAvm	User <username> is disabled.	MINOR	User tried too many times to log in with an incorrect password; the account is disabled.	Enable the account.

Table 14-1 Prime Network Security Events (continued)

Event Name	Source OID	Short Description	Severity	Cause	Action
user successfully authenticated	IAvm	User <username> authenticated successfully.	MINOR	The user of the system is succesfully authenticated.	None needed.
Category: Logoff					
user logoff	IAvm	User <username> logged off.	CLEARED	User closed the application that was connected to the system.	None needed.
Category: Password Changed					
password changed	IAvm	User <username> changed password.	CLEARED	The user changed their password.	None needed.
Category: Password Expired					
authenticate	IAvm	Password expired. Couldn't authenticate user <username>.	MINOR	User password expiration date has arrived.	Update user password.
disabled	IAvm	Account inactivity timeout expired. Account disabled. Couldn't authenticate user <username>.	MINOR	The user has not logged in within the specified time period and the account is disabled.	Enable user account.
Category: User Disabled					
disabled	IAvm	Too many failed logins, user disabled <username>	MAJOR	User had too many failed logins.	None needed.

Table 14-2 defines terms and acronyms that appear in the security events table.

Table 14-2 Security Event Terms and Acronyms

Term	Definition
avmid	AVM identifier
avmkey	AVM key
BOS	Prime Network
DNA	Prime Network
MC	Prime Network unit
VNE	Virtual Network Element



CHAPTER 15

Service Alarms

This section describes the Prime Network service alarms (events). Service alarms appear in the Prime Network Events Service tab. For information about Prime Network Events, see the *Cisco Prime Network 3.9 User Guide.* These topics describe the Prime Network service alarms, registry parameters, and source OIDs:

- Service Alarms
- Registry Parameters
- Alarm Source OIDs

Each alarm is described in a section containing:

- A short description, including background about the network state or system (Prime Network) state that caused the alarm. The short description of the service alarm is what appears in the ticket, in the Service tab of Cisco Prime Network Events. The short description for each type and subtype can be viewed in Registry Parameters.

  When a flapping event occurs, the short description is changed.

Note The name of the service alarm is the same as the short description.

- A table of all the subtype events that represent one of the states the alarm can be in, and a description of when they are issued. For example, the Link Down alarm can have multiple subtype events (states) which include Link Down Due to Admin Down, Link Down Due to Oper Down, and Link Up. The description also shows if the event is a clearing event.
- Information related to the correlation of the alarm, mainly:
  - The alarm issue correlation process and location (local or network).
  - If other alarms can correlate to this alarm.
  - The keys that are used in the correlation process.
  - The specific correlation filters in use for the alarm, if any. The filter indicates if a specific event cannot be selected as the root cause event in the correlation process.
- By default, any new event filters the following events: Cloud Problem, BGP Process Down, LDP Neighbor Down, MPLS Interface Removed, the event itself, and events with lower or equal correlation weight.

Each section describes a group of alarms sharing the same event type.

Service Alarms

The following service alarms are supported in Prime Network:

- Adaptive Polling
- All IP Interfaces Down
- ATM IMA Service
- BFD Connectivity Down
- BFD Neighbor Loss
- BGP Link Down
- BGP Neighbor Loss
- BGP Process Down
- Broken LSP Discovered
- Card Down
- Card Out
- CFM Domain Fault
- Carrier Grade NAT Translations Create Rate
- Carrier Grade NAT Translations Delete Rate
- Carrier Grade NAT Inside-to-Outside Forward Rate
- Carrier Grade NAT Outside-to-Inside Forward Rate
- Carrier Grade NAT Inside-to-Outside Drops Port Limit Exceeded
- Carrier Grade NAT Inside-to-Outside Drops System Limit Reached
- Carrier Grade NAT Inside-to-Outside Drops Resource Depletion
- Chassis Disconnected
- Cloud Problem
- Component Unreachable
- CPU Utilization
- Device Unsupported
- Discard Packets
- Dropped Packets
- DS0 Bundle Service Alarm
- DS1 Path Link Down
- DS1 Path Port Down
- DS3 Path Link Down
- DS3 Path Port Down
- Dual Stack IP Changed
- DWDM Controller Down
- DWDM G709 Status Down
- EFP Down

- ESMC Process Down
- Fan-Tray Down
- Fan-Tray Out
- GRE Keepalive
- GRE Tunnel Down
- HSRP Group Status Changed
- Interface Status
- Investigation State
- L2TP Peer Not Established
- L2TP Sessions Threshold
- Lag Down
- Lag Link Down
- Layer 2 Tunnel Down
- LDP Neighbor Loss
- Link Down
- Link Utilization
- Log Archive is Disabled on the Device
- Local Switching Down
- Logical Port Down
- LSP Down
- Members Changed
- Memory Utilization
- MLPPP Bundle
- MPLS Black Hole Found
- MPLS TP Bandwidth Mismatch
- MPLS Interface Removed
- MPLS TE FRR State Changed
- MPLS TE Tunnel Down
- MPLS TP Tunnel Down
- Network-Clock Synchronization
- OSPF Neighbor State Change
- Port Down
- Power Supply Down
- Power Supply Out
- Pluggable Transceiver Out
- REP Port Role Change
- Rx Dormant
- Rx Utilization

- Shelf Out
- SONET Path Link Down
- SONET Path Port Down
- Subinterface Down
- Tx Dormant
- Tx Utilization
- VSI Down

Adaptive Polling

Adaptive polling is a mechanism that handles situations in which the device CPU is crossing a predefined, configurable threshold. It reduces the polling when the CPU reaches high threshold values for a configurable sample, and returns the polling to a normal rate when the CPU reaches the lower threshold. Where the CPU stays high for several samplings, the VNE is automatically moved to the maintenance state to avoid continuous polling of the device.

In all cases, alarms are issued when the device or the VNE state changes.

Table 15-1 Adaptive Polling—Subtype Events

Subtype Event Name	Description
VNE Switched to Low Polling Rate Due to CPU High Usage	Issued when the CPU level has been above the high threshold (configurable, default=90%) for several samplings (configurable, default=5). The polling rate of the device is lowered by adding a delay between requests (default delay is 500 msec).
VNE Switched Back to Regular Polling Rate	Clearing event. Issued when the CPU level has been below the lower threshold (configurable, default=70%) for several samplings (configurable, default=2). The polling rate of the device is changed back to normal (no delay between requests).
VNE Switched to a Limited Investigation Mode Due to High CPU Usage	Issued when the CPU level raises above a threshold and the VNE stops polling the device. The VNE starts polling the device automatically once the CPU usage decreases.

Correlation

The alarm correlates to other alarms using the local correlation mechanism with the ManagedElement key. No other alarms can correlate to it.

Impact Analysis

No impact analysis is performed for this alarm.

Source OID

See Managed Element OID (IManagedElementOid).

All IP Interfaces Down

The All IP Interfaces Down alarm is used when *all* IP interfaces configured on the same port are down, and implies that another fault has occurred in lower layers (such as the physical layer). In this case, one alarm is issued, and all IP interface status alarms are correlated to it.

Table 15-2 All IP Interfaces Down—Subtype Events

Subtype Event Name	Description
All IP Interfaces Down	Issued when all the IP interfaces configured above a physical interface change their state to down.
Active IP Interfaces Found	Clearing event. Issued when at least one of the IP interfaces changes its state to up.

Correlation

The alarm correlates to other alarms using the local correlation mechanism with the PortLayer1 key representing the physical layer. The PortLayer1 key is the port that all the IP interfaces were configured on.

Other alarms might correlate to this alarm using the physical port key, in particular the Interface Status Down alarm.

Impact Analysis

No impact analysis is performed for this alarm.

Source OID

See Physical Layer OID (IPhysicalLayerOid).

ATM IMA Service

The ATM IMA Service alarm is generated by the IMA group. IMA Group Down events are generated when the number of IMA group members is reduced by a user-defined percentage configured in the registry. The severity depends on the percentage of member removed. To avoid false correlations, the events are combined with the IMA group status. An IMA group down generates the highest severity. Other severities are user-defined.

Table 15-3 ATM IMA Service Alarm

Subtype Event Name	Description
IMA Admin Down	Generated when the IMA group is administratively shut down. All the members are correlated to this event.
IMA Oper Down	Generated when the IMA group is operationally down.

Correlation

The IMA Admin Down alarm can be the root cause of other events, but other ATM IMA events cannot be root cause of other events. No events are correlated.

Impact Analysis

No impact analysis is performed for this alarm.

Source OID

See IMA Service (IIMAGroupOid).

BFD Connectivity Down

The BFD Connectivity Down Alarm is generated when the connectivity is lost between two BFD neighbors.

Table 15-4 BFD Connectivity Down

Subtype Event Name	Description
BFD Connectivity Down	Generated when BFD connection is lost.
BFD Connectivity Up	Clearing Event. Generated when BFD connection is found.

Correlation

BFD Connectivity Down alarm uses flow based correlation.

The VNE with flow based correlation mechanisim uses an active correlation flow that traverses among three layers of the network (Layer 1,Layer 2, and Layer 3) and tries to correlate along a specified network path to an alarm. Based on the alarm that could occur in any one of the layers, it will try to find the root cause alarm. BFD Connectivity Down alarm can corrleate to alarms that are found upto Layer 3.

Impact Analysis

No impact analysis is performed for this alarm.

Source OID

See BFD Connectivity Down OID.

BFD Neighbor Loss

A BFD Neighbor Loss alarm is triggered when the status of BFD changes. When the status of a BFD is changed, an alarm will be issued by each neighbor as a separate event. These alarms will remain displayed until the parent ticket is cleared, that is until the status of the BFD neighbor changes to its previous state.

A BFD Neighbor Found alarm is a clearing event for the BFD Neighbor Loss alarm. It is triggered when the alarm state changes from down to up.

Table 15-5 BFD Neighbor Loss

Subtype Event Name	Description
BFD Neighbor Loss	Generated when the connection to BFD neighbor is lost.
BFD Neighbor Found	Clearing Event.Generated when the BFD Neighbor is found.

Correlation

BFD Neighbor Loss alarm uses flow based correlation.

The VNE with flow based correlation mechanisim uses an active correlation flow that traverses among three layers of the network (Layer 1,Layer 2, and Layer 3) and tries to correlate along a specified network path to an alarm. Based on the alarm that could occur in any one of the layers, it will try to find the root cause alarm. BFD Neighbor loss alarm can corrleate upto Layer 3.

Impact Analysis

No impact analysis is performed for this alarm.

Source OID

See BFD Neighbor Loss OID.

BGP Link Down

When a connection between two BGP peers is lost, no route information is exchanged between the two peers. This situation affects the network connectivity because route entries which are not refreshed start to be dropped from the routing table, causing packets to be dropped.

In this scenario, when a BGP neighbor has an adjacent peer (meaning that it is connected to another BGP neighbor with a discovered link), a BGP Link Down alarm is issued. When the adjacent peer is not managed, a BGP Neighbor Loss alarm is issued. A VNE identifies this situation based on changes in the BGP neighbor table of the device.

Due to the nature of this fault, it is possible that one of the devices may be unreachable. In this case, the respective VNE does not identify the changes in the BGP neighbor table of the unreachable device, but a BGP Link Down is still issued.

A negotiation process between the two link edges is issued when the BGP neighbor entry state changes from Established, indicating that a BGP Link Down should be invoked.

Table 15-6 BGP Link Down—Subtype Events

Subtype Event Name	Description
BGP Link Down Due to Admin Down	Issued when a BGP neighbor entry has changed its state from Established to another state, or a BGP neighbor entry that had an Established state has been removed from the BGP neighbors table and the entry has an adjacent peer. BGP neighbor state complies with the definitions in BGP4-MIBBFDbgpPeerState (1.3.6.1.2.1.15.3.1.2). In the case of a state change, any state other than Established implies that the connection between the BGP peers is not fully functioning, which means the route information is not exchanged. This alarm is issued when a BGP link is administratively down.
BGP Link Down Due to Oper	Issued when a BGP neighbor entry has changed its state from Established to another state, or a BGP neighbor entry that had an Established state has been removed from the BGP neighbors table and the entry has an adjacent peer. BGP neighbor state complies with the definitions in BGP4-MIB::bgpPeerState (1.3.6.1.2.1.15.3.1.2). In the case of a state change, any state other than Established implies that the connection between the BGP peers is not fully functioning, which means the route information is not exchanged. This alarm is issued when a BGP link is operatively down.
BGP Link Down VRF Due to Admin	Issued in the same conditions as the BGP Link Down alarm except that the neighbor is defined in the context of a VRF (BGP connection between PE router and CE router). This alarm is issued when a BGP link is administratively down.
BGP Link Down VRF Due to Oper	Issued in the same conditions as the BGP Link Down alarm except that the neighbor is defined in the context of a VRF (BGP connection between PE router and CE router). This alarm is issued when a BGP link is operatively down.
BGP Link Up	Clearing event. Issued when one of the edge BGP neighbor entries has changed its state from any state other than Established to Established. This is the clearing alarm for both the BGP Link Down alarms previously described.

Correlation

The alarm correlates to other alarms using the network correlation mechanism that runs a forward IP flow to the BGP neighbor peer IP. This flow runs a forward flow from each of the BGP neighbors to its peer IP, and might collect the following alarms: Interface Status Down, Port Down, Link Down, Device Unreachable, and so on.

Other alarms might correlate to it using the MPBgp key or the MPBgp key concatenated with the neighbor peer IP. Furthermore, the relevant BGP Neighbor Down syslogs are correlated to the service alarm.

Note The BGP Link Down and BGP Link Down VRF alarms do not filter out the BGP Process Down alarm in the correlation process.

Impact Analysis

No impact analysis is performed for this alarm.

Source OID

See MPBGP OID (IMpBgpOid).

BGP Neighbor Loss

If BGP connectivity to a specific device in an MPLS VPN network is lost, VPN sites lose connectivity. The VNE models the BGP connection between routers and actively monitors its state. A BGP Neighbor Loss alarm is generated from both sides of the connection when a connectivity loss occurs. Alarms and tickets are issued and impact analysis information displayed.

The correlation engine identifies various faults that affect the BGP connection and reports them as the root cause for the BGP Neighbor Loss alarm, for example, Link Down, CPU Overutilized, and Link Data Loss.

Note BGP Neighbor Loss alarms are not correlated to each other. They are correlated to the root cause of the connectivity loss.

The BGP Neighbor Loss alarm is detected actively by the system, and service alarms are generated. The system also supports BGP neighbor down syslogs.

When the VNE BGP component polls the BGP neighbor status (expedite or normal polling) and finds that an entry for a neighbor no longer exists or its state changed from Established to another state, the BGP component issues a BGP Neighbor Loss alarm. This alarm causes the BGP component to issue a Root Cause Analysis (RCA) correlation flow to find the root cause. If RCA does not find an alarm to correlate, the VNE sends the alarm to the gateway as a ticket.

If a BGP neighbor loss occurs and the BGP component has no other BGP PE links, all VRFs with route entries to the PE as BGP next hops are true-affected. This information is sent as an update to the previous BGP Neighbor Loss alarm.

Table 15-7 BGP Neighbor Loss—Subtype Events

Subtype Event Name	Description
BGP Neighbor Loss Due to Admin	Issued when a BGP neighbor entry has changed its state from Established to another state due to admin, or when a BGP neighbor entry with the Established state has been removed from the BGP neighbors table. BGP neighbor state complies with the definitions in BGP4-MIB::bgpPeerState (1.3.6.1.2.1.15.3.1.2). In the case of a state change, any state other than Established implies that the connection between the BGP peers is not fully functioning, meaning that the route information is not exchanged.
BGP Neighbor Loss Due to Oper	Issued when a BGP neighbor entry has changed its state from Established to another state due to oper, or when a BGP neighbor entry with the Established state has been removed from the BGP neighbors table.
BGP Neighbor Loss VRF Due to Admin	Issued in the same conditions as the BGP Neighbor Loss Due to Admin alarm, except that the neighbor is defined in the context of a VRF (BGP connection between PE router and CE router).

Table 15-7 BGP Neighbor Loss—Subtype Events (continued)

Subtype Event Name	Description
BGP Neighbor Loss VRF Due to Oper	Issued in the same conditions as the BGP Neighbor Loss Due to Oper alarm, except that the neighbor is defined in the context of a VRF (BGP connection between PE router and CE router).
BGP Neighbor Found	Clearing event. Issued when a BGP neighbor entry has changed its state from any state other than Established to the Established state, or a new BGP neighbor entry that has an Established state has been discovered in the BGP neighbors table. This is the clearing alarm of both neighbor loss alarms previously described.

Correlation

The alarm correlates to other alarms using the network correlation mechanism that runs a forward IP flow to the BGP neighbor peer IP. This flow runs a forward flow from each of the BGP neighbors to its peer IP, and might collect the following alarms: Interface Status Down, Port Down, Link Down, Device Unreachable, and so on.

Other alarms might correlate to it using the MPBgp key or the MPBgp key concatenated with the neighbor peer IP. Furthermore, the relevant BGP Neighbor Down syslogs are correlated to the service alarm.

Note The BGP Neighbor Loss and BGP Neighbor Loss VRF alarms do not filter out the BGP Process Down alarm in the correlation process.

Impact Analysis

The alarm issues an impact analysis process that calculates the affected services of this fault. In this case, the affected service is represented as a pair of VRFs that cannot communicate due to this BGP Neighbor Loss fault.

The affected pair (service) can be marked as potentially affected or real affected. In this case, because the BGP reports on a neighbor loss only after a hold-time interval (default 180 sec), in which it did not get the hello message from its neighbor, it assumes that the connection was lost and cannot be recovered. The identified affected pairs are marked as real affected.

Source OID

See MPBGP OID (IMpBgpOid).

BGP Process Down

A Prime Network query checks the status of the BGP process when the VNE BGP component polls for the status and configuration of its BGP neighbors (expedite or normal polling). If the BGP process is not running, the VNE BGP component issues a BGP Process Down alarm. This alarm is always a ticket and does not try to correlate to other alarms. All BGP Neighbors Down alarms issued in response to the BGP Process Down alarm are correlated to the BGP Process Down ticket.

Table 15-8 BGP Process Down—Subtype Events

Subtype Event Name	Description
BGP Process Down	Issued when the BGP process/service is down after it was up. The BGP component in the VNE identifies this change, updates its state, and issues the alarm.
BGP Process Up	Clearing event. Issued when the BGP process/service changes its state back to up. The BGP component in the VNE identifies this change, updates its state, and issues the clearing alarm.

Correlation

Due to the nature of this alarm, it cannot be correlated to other alarms, thus this alarm does not try to run any correlation process.

Other alarms might correlate to it using the MPBgp key, in particular BGP Neighbor Loss alarms caused by this failure correlate to it.

Impact Analysis

No impact analysis is performed for this alarm.

Source OID

See MPBGP OID (IMpBgpOid).

Broken LSP Discovered

A Broken LSP Discovered alarm is issued as a companion to the MPLS Black Hole Found alarm (see MPLS Black Hole Found.)

A Broken LSP Discovered event means that an LSP, at some point, went through an MPLS black hole. Because of this, the MPLS labels were removed from the packet, and one of the following scenarios occurs:

- If the packet contains more than one MPLS label (data contained in the packet is VPN traffic), the packet is dropped or is forwarded to an incorrect destination. This happens because the IP header in the packet belongs to a different routing domain.
- If the packet contains only one MPLS label (data contained in the packet belongs to the same routing domain), the packet continues to be forwarded based on the IP header information instead of the MPLS labels. This is not a problem.

The following information applies to the Broken LSP Discovered alarm:

- This alarm does not have a clearing alarm, which means that after it is issued, its severity cannot be changed.
- To overcome the previous limitation, the alarm auto-clear flag is set to true. This means that this alarm severity does not have an impact on the severity of other alarms that it correlates to.
- Though the Broken LSP Discovered alarm is issued as a companion to the MPLS Black Hole Found, it does not imply that it is issued from the same device that issued the MPLS Black Hole Found alarm.

After an MPLS Black Hole Found alarm is issued, a process starts and looks for broken LSPs that go through this MPLS black hole. The process of discovering the broken LSPs is as follows:

1. At the VNE on which the MPLS Black Hole Found was issued, all label switching entries that were destined for the black hole have an untagged out label. All MPLS labels are removed from packets traversing using this label switching entry.
2. Each untagged label switching entry starts traversing the LSP using a backward flow.

Note The direction of a backward flow traversing the VNE model is opposite that of a standard packet flow traversing the network.

3. On each device traversed in the backward flow, Prime Network checks for configured MPLS-based services on the device. The following identification services are supported:
   - Existence of VRFs (BGP/MPLS VPN services based on RFC2547).
   - Existence of MPLS Layer2 tunnels (PWE3 services based on RFC4448).
4. If the device contains such services, a Broken LSP Discovered alarm is issued for each LSP traversed backward to that point.

   This means that only PE routers issue such alarms. It is possible that the same LSP has entry points in multiple devices, and thus multiple alarms are issued for it.
5. Information that is important for each broken LSP alarm issued is the entry point (label switching entry) and the exit point (the IP subnet destination).

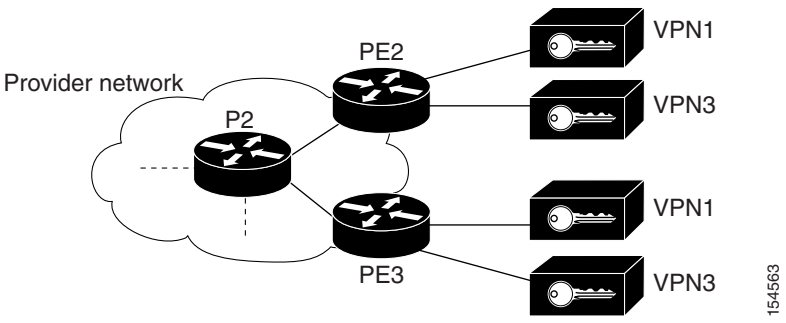
This information is used in the impact analysis process to identify the relevant affected pairs (services).

In the network described in Figure 15-1, the shortest path from PE2 to PE3 is PE2< >P2< >PE3. The link between P2 and PE3 is an MPLS link, meaning interfaces on both sides of the link are configured as MPLS interfaces. Also assume that for some reason, the MPLS configuration is incomplete or incorrect; for example:

- Only one interface is configured as an MPLS interface.
- The label distribution protocol is configured differently on both interfaces (protocol mismatch).

In this case, the label switching table on P2 and PE3 will have untagged entries for the LSPs between PE2 and PE3. If PE2 and PE3 have VPN services (for example VRFs and pseudowires), the outcome will be that the data flow between PE2 and PE3 will be affected.

Figure 15-1 Example of an MPLS Black Hole Scenario



In this case, Prime Network does the following:

- Identifies untagged label switching entries on P2 and PE3.
- Issues MPLS Black Hole Found alarms on the interfaces on both sides of the link (since the LSP is unidirectional).
- Initiates a backward flow starting from the link on the specific untagged entries and identifies the two LSPs traversing the link:
  - LSP from PE2 to PE3
  - LSP from PE3 to PE2
- Issues Broken LSP Discovered alarms on both LSPs in PE2 and PE3, which are correlated to the corresponding MPLS Black Hole Found alarm.

Note The clearing alarm does not activate flows to locate the LSPs that were passing through it in order to issue a clearing alarm for Broken LSPs, but rather uses the auto-clear functionality. The gateway periodically reviews the tickets and checks if all the alarms under each ticket are cleared or configured as auto-cleared alarms and whether the gateway correlation timeout has passed, in which case the gateway closes the ticket.

After the MPLS Black Hole alarm clears, and the configured gateway correlation timeout period is reached, the gateway can close the ticket because all the alarms correlated to MPLS Black Hole and Broken LSP are auto-cleared.

Note If an MPLS Network Link Down event causes an IP reroute and an LDP redistribution, new LSPs might be redirected through nonMPLS segments, which will create a black hole. In this case, Broken LSP Discovered alarms are issued. However, the discovered broken LSPs are correlated to the Link Down alarm and not to the MPLS Black Hole Found alarm.

Table 15-9 Broken LSP Discovered—Subtype Events

Subtype Event Name	Description
Broken LSP Discovered	Issued as a companion to the MPLS Black Hole Found alarm as described previously. For every LSP traversing the black hole, a Broken LSP Discovered alarm is issued. There is no clearing event.

Correlation

This alarm is correlated by definition to one of the following:

- The MPLS Black Hole Found that triggered the discovery of this broken LSP.
- Link Down alarm, if the link down caused the MPLS traffic to change its course and pass through the black hole.

No other alarms can correlate to it.

Impact Analysis

The alarm issues an impact analysis process that identifies the local affected services of this fault. In this case, affected services can be of two types:

- A pair of VRFs that cannot communicate due to this broken LSP (for BGP/MPLS VPN services).
- A pair of MPLS Layer 2 tunnel edges representing a PWE3 service endpoint.

The affected pairs in this alarm are marked as potentially affected.

Note The system can be configured to present the affected pairs for BGP/MPLS VPN services as pairs of VRF IP interfaces instead of just the VRFs. This creates, in most cases, additional pairs that might cause a load on the system. Configuring them as IP interfaces is disabled by default.

Source OID

See Managed Element OID (IManagedElementOid) (the LSE entry that is the entry point to the broken LSP).

Card Down

The Card Down alarm represents a state in which a card is not operational. This can be caused by a hardware failure, or by changing the administrative state of the card.

Table 15-10 Card Down—Subtype Events

Subtype Event Name	Description
Card Down	Issued when the operational state of a card is changed to down. This can be caused by a hardware failure, or by changing the administrative state of the card
Card Up	Clearing event. Issued when the operational state of the card changes back to up.

Correlation

Due to the nature of this alarm, the event does not try to correlate to another event, and creates a new ticket in the gateway where the event is the root cause alarm of the ticket.

Other alarms might correlate to it using the Card key.

Impact Analysis

No impact analysis is performed for this alarm.

Source OID

See Module OID (IModuleOid).

Card Out

The Card Out alarm represents a state where a card is removed from the device. The Card Out alarm is also issued when a device stops reporting on the existence of a card due to another failure, even if the card is actually still in the device. It is assumed that any functionality that was implemented by the card is not working anymore if the card had no redundancy configuration.

Note When a Card Out alarm occurs, Prime Network Vision displays an alarm icon next to the affected card in the inventory display. Even though the card has been physically removed, it is still displayed in Prime Network Vision so that you can identify which network element is generating the alarm.

Table 15-11 Card Out—Subtype Events

Subtype Event Name	Description
Card Out	Issued when a card is removed from the device. It is possible that some card failures are identified as Card Out because the device does not report on the card's existence after a failure.
Subcard Out	Issued when a card that is contained in another card is removed from the device. When a card that contains other cards is removed, in addition to the Card Out alarm issued on the main card, a Subcard Out alarm is issued for each of its subcards. It is possible that some failures of cards that contain subcards are identified as Card Down on the parent card and Subcard Out for the subcards, because the device stops reporting on the existence of the subcards.
Card Out due to Chassis Disconnected	Issued when a chassis is removed from the network element corresponding to which the cards in the chassis are unavailable in the network element. It is possible that some card failures are identified as Card Out because the device does not report on the card's existence after a failure.
Card In	Clearing event. Issued when the card is inserted back into the device.

Correlation

Due to the nature of the Card Out alarm, the event does not try to correlate to another event, and creates a new ticket in the gateway where the event is the root cause alarm of the ticket. The Subcard Out alarm correlates to other alarms using the local correlation mechanism with Subcard key and its parent Card key.

Other alarms might correlate to it using the Card and Subcard keys.

Impact Analysis

No impact analysis is performed for this alarm.

Source OID

See Module OID (IModuleOid).

CFM Domain Fault

The CFM Domain Fault service alarm is created for every CFM domain having at least one event attached to an entity belonging to that domain (Maintenance Association, Maintenance Endpoint, and Remote Maintenance Endpoint). The CFM Domain Fault service alarm is cleared after all the correlated events are cleared.

Events can be aggregated as long as they have a common source OID.

The CFM application is used to aggregate the different CFM syslogs and traps by domain.

The domain OID is contained in the MEP OID.

Table 15-12 CFM Domain Fault

Subtype Event Name	Description
CFM Domain Aggregation Down	Created for every domain that has at least one event attached to an entity belonging to the domain: Maintenance Association, Maintenance Endpoint (MEP), or Remote MEP.
CFM Domain Aggregation Up	Issued after all correlated events are cleared.

Correlation

Because Prime Network does not discover CFM topologies, CFM event correlation is not available.

Impact Analysis

No impact analysis is performed for this alarm.

Source OID

IMaintenanceDomainOID

Carrier Grade NAT Translations Create Rate

When data packets traverse from the private to public network, the Cisco CRS-1 routers (configured with Carrier Grade NAT) translate many private IPv4 addresses into fewer public IPv4 addresses. Similarly, when data packets traverse from the public to private network, many public IPv4 addresses are translated into fewer private IPv4 addresses.

Carrier Grade NAT Translations Create Rate represents the number of translation entries that are created in the last one second. Alarms are issued when the number of translations exceeds or drops below the threshold value. The threshold values can be changed by the user.

Table 15-13 Carrier Grade NAT Translations Create Rate

Subtype Event Name	Description
Carrier Grade NAT Translations Create Rate Higher Threshold Exceeded	Alarm is triggered when the number of translations created exceeds the higher threshold value. The default higher threshold value is 80.
Carrier Grade NAT Translations Create Rate Lower Threshold Exceeded	Alarm is triggered when the number of translations created is lower than the lower threshold value. The default lower threshold value is 40.
Carrier Grade NAT Translations Create Rate Threshold Normal	Alarm triggered when the number of translations created is equal to the normal threshold value.

Correlation

Carrier Grade NAT Translations Create Rate service alarm does not try to correlate with any other alarm.

No other alarms can correlate to this alarm.

Impact Analysis

No impact analysis is performed for this alarm.

Source OID

See Carrier Grade NAT OID (ICgnServiceOid).

Carrier Grade NAT Translations Delete Rate

When data packets traverse from the private to public network, the Cisco CRS-1 routers (configured with Carrier Grade NAT) translate many private IPv4 addresses into fewer public IPv4 addresses. Similarly, when data packets traverse from the public to private network, many public IPv4 addresses are translated into fewer private IPv4 addresses.

Carrier Grade NAT Translations Delete Rate represents the number of translation entries that are deleted in the last one second. Alarms are issued when the number of translations exceeds or drops below the threshold value. The threshold values can be changed by the user.

Table 15-14 Carrier Grade NAT Translations Delete Rate

Subtype Event Name	Description
Carrier Grade NAT Translations Delete Rate Higher Threshold Exceeded	Alarm is triggered when the number of translations deleted exceeds the higher threshold value. The default higher threshold value is 80.
Carrier Grade NAT Translations Delete Rate Lower Threshold Exceeded	Alarm is triggered when the number of translations deleted is lower than the lower threshold value. The default lower threshold value is 40.
Carrier Grade NAT Translations Delete Rate Threshold Normal	Alarm triggered when the number of translations deleted is equal to the normal threshold value.

Correlation

Carrier Grade NAT Translations Delete Rate service alarm does not try to correlate with any other alarm.

No other alarms can correlate to this alarm.

Impact Analysis

No impact analysis is performed for this alarm.

Source OID

See Carrier Grade NAT OID (ICgnServiceOid).

Carrier Grade NAT Inside-to-Outside Forward Rate

Data packets enter the Cisco CRS-1 routers (configured with Carrier Grade NAT) from the private network. The destination address of the packet is changed to a global address and is forwarded to the public network.

Carrier Grade NAT Inside-to-Outside Forward Rate represents the number of packets that have been forwarded from the private to the public network in the last one second. Alarms are issued when the number of forwarded packets, exceeds or drops below the threshold value. The threshold values can be changed by the user.

Table 15-15 Carrier Grade NAT Inside-to-Outside Forward Rate

Subtype Event Name	Description
Carrier Grade NAT Inside-to-Outside Forward Rate Higher Threshold Exceeded	Alarm is triggered when the number of packets forwarded exceeds the higher threshold value. The default higher threshold value is 80.
Carrier Grade NAT Inside-to-Outside Forward Rate Lower Threshold Exceeded	Alarm is triggered when the number of packets forwarded is lower than the lower threshold value. The default lower threshold value is 40.
Carrier Grade NAT Inside-to-Outside Forward Rate Threshold Normal	Alarm triggered when the number of packets forwarded is equal to the normal threshold value.

Correlation

Carrier Grade NAT Inside-to-Outside Forward Rate service alarm does not try to correlate with any other alarm.

No other alarms can correlate to this alarm.

Impact Analysis

No impact analysis is performed for this alarm.

Source OID

See Carrier Grade NAT OID (ICgnServiceOid).

Carrier Grade NAT Outside-to-Inside Forward Rate

Data packets enter the Cisco CRS-1 routers (configured with Carrier Grade NAT) from the public network. The destination address of the packet is changed to a private address and the packet is forwarded to the private network.

Carrier Grade NAT Outside-to-Inside Forward Rate represents the number of packets that have been forwarded from the private to the public network in the last one second. Alarms are issued when the number of forwarded packets, exceeds or drops below the threshold value. The threshold values can be changed by the user.

Table 15-16 Carrier Grade NAT Outside-to-Inside Forward Rate

Subtype Event Name	Description
Carrier Grade NAT Outside-to-Inside Forward Rate Higher Threshold Exceeded	Alarm is triggered when the number of packets forwarded exceeds the higher threshold value. The default higher threshold value is 80.
Carrier Grade NAT Outside-to-Inside Forward Rate Lower Threshold Exceeded	Alarm is triggered when the number of packets forwarded is lower than the lower threshold value. The default lower threshold value is 40.
Carrier Grade NAT Outside-to-Inside Forward Rate Threshold Normal	Alarm is triggered when the number of packets forwarded is equal to the normal threshold value.

Correlation

Carrier Grade NAT Outside-to-Inside Forward Rate service alarm does not try to correlate with any other alarm.

No other alarms can correlate to this alarm.

Impact Analysis

No impact analysis is performed for this alarm.

Source OID

See Carrier Grade NAT OID (ICgnServiceOid).

Carrier Grade NAT Inside-to-Outside Drops Port Limit Exceeded

When data packets traverse from the private network to public network, Cisco CRS-1 routers (configured with Carrier Grade NAT) translates the private addresses into global addresses. Data packets can get dropped during the inside-to-outside translations, when the port limit is exceeded.

Carrier Grade NAT Inside-to-Outside Drops Port Limit Exceeded alarm is issued when the number of dropped packets, exceeds or drops below the threshold value. The threshold values can be changed by the user.

Table 15-17 Carrier Grade NAT Inside-to-Outside Drops Port Limit Exceeded

Subtype Event Name	Description
Carrier Grade NAT Inside-to-Outside Drops Port Limit Higher Threshold Exceeded	Alarm is triggered when the number of packets dropped exceeds the higher threshold value. The default higher threshold value is 80.

Table 15-17 Carrier Grade NAT Inside-to-Outside Drops Port Limit Exceeded (continued)

Subtype Event Name	Description
Carrier Grade NAT Inside-to-Outside Drops Port Limit Lower Threshold Exceeded	Alarm is triggered when the number of packets dropped is lower than the lower threshold value. The default lower threshold value is 40.
Carrier Grade NAT Inside-to-Outside Drops Port Limit Threshold Normal	Alarm is triggered when the number of packets dropped is equal to the normal threshold value.

Correlation

Carrier Grade NAT Inside-to-Outside Drops Port Limit Exceeded service alarm does not try to correlate with any other alarm.

No other alarms can correlate to this alarm.

Impact Analysis

No impact analysis is performed for this alarm.

Source OID

See Carrier Grade NAT OID (ICgnServiceOid).

Carrier Grade NAT Inside-to-Outside Drops System Limit Reached

When data packets traverse from the private network to public network, Cisco CRS-1 routers (configured with Carrier Grade NAT) translates the private addresses into global addresses. Data packets can get dropped during the inside-to-outside translations, when the system limit is reached.

Carrier Grade NAT Inside-to-Outside Drops System Limit Reached alarm is issued when the number of dropped packets, exceeds or drops below the threshold value. The threshold values can be changed by the user.

Table 15-18 Carrier Grade NAT Inside-to-Outside Drops System Limit Reached

Subtype Event Name	Description
Carrier Grade NAT Inside-to-Outside Drops System Limit Reached Higher Threshold Exceeded	Alarm is triggered when the number of packets dropped exceeds the higher threshold value. The default higher threshold value is 80.
Carrier Grade NAT Inside-to-Outside Drops System Limit Reached Lower Threshold Exceeded	Alarm is triggered when the number of packets dropped is lower than the lower threshold value. The default lower threshold value is 40.
Carrier Grade NAT Inside-to-Outside Drops System Limit Reached Threshold Normal	Alarm is triggered when the number of packets dropped is equal to the normal threshold value.

Correlation

Carrier Grade NAT Inside-to-Outside Drops System Limit Reached service alarm does not try to correlate with any other alarm.

No other alarms can correlate to this alarm.

Impact Analysis

No impact analysis is performed for this alarm.

Source OID

See Carrier Grade NAT OID (ICgnServiceOid).

Carrier Grade NAT Inside-to-Outside Drops Resource Depletion

When data packets traverse from the private network to public network, Cisco CRS-1 routers (configured with Carrier Grade NAT) translates the private addresses into global addresses. Data packets can get dropped during the inside-to-outside translations, when no ports are available.

Carrier Grade NAT Inside-to-Outside Drops Resource Depletion alarm is issued when the number of dropped packets, exceeds or drops below the threshold value. The threshold values can be changed by the user.

Table 15-19 Carrier Grade NAT Inside-to-Outside Drops Resource Depletion

Subtype Event Name	Description
Carrier Grade NAT Inside-to-Outside Drops Resource Depletion Higher Threshold Exceeded	Alarm is triggered when the number of packets dropped exceeds the higher threshold value. The default higher threshold value is 80.
Carrier Grade NAT Inside-to-Outside Drops Resource Depletion Lower Threshold Exceeded	Alarm is triggered when the number of packets dropped is lower than the lower threshold value. The default lower threshold value is 40.
Carrier Grade NAT Inside-to-Outside Drops Resource Depletion Threshold Normal	Alarm is triggered when the number of packets dropped is equal to the normal threshold value.

Correlation

Carrier Grade NAT Inside-to-Outside Drops Resource Depletion service alarm does not try to correlate with any other alarm.

No other alarms can correlate to this alarm.

Impact Analysis

No impact analysis is performed for this alarm.

Source OID

See Carrier Grade NAT OID (ICgnServiceOid).

Chassis Disconnected

The Chassis Disconnected represents a state where a chassis is removed from a network element. The Chassis Disconnected alarm is also issued when a port connecting the chassis is removed from the network element, even if the chassis is actually still in the network element. As the port is removed, the corresponding cards in the chassis are also disconnected from the network element. The system administrator would need to manually connect the chassis or the port to the network element.

Note When a Chassis Disconnected alarm occurs, Prime Network Vision displays an alarm icon next to all the affected cards of the chassis in the inventory display. This enables you to identify which network element is generating the alarm.

Table 15-20 Chassis Disconnected—Subtype Events

Subtype Event Name	Description
Chassis Disconnected	Issued when a chassis is removed from a network element.
Chassis Connected	Clearing event. Issued when the chassis is inserted back into the network element.

Correlation

Due to the nature of the Chassis Disconnected alarm, the event does not try to correlate to another event, and creates a new ticket in the gateway where the event is the root cause alarm of the ticket. A clearance event is generated when the chassis is connected back into the network element.

Impact Analysis

No impact analysis is performed for this alarm.

Source OID

See Chassis Oid (ChassisId)

Cloud Problem

Cloud VNEs represent unmanaged network segments, so that operations such PathTracer and Root Cause Analysis (RCA) can be viewed or processed end-to-end. A Cloud VNE represents the unmanaged segment of a network as a single device to which two or more managed segments of the network can be connected.

In a network in which a segment of the network is unmanaged, Prime Network runs a correlation flow to find the root cause. If no root cause is found within the managed segment, a Cloud Problem service alarm is created, to which events are correlated.

Table 15-21 Cloud Problem—Subtype Events

Subtype Event Name	Description
Cloud Problem	An alarm might use network correlation using IP-based forward flow to a destination. During the flow, the alarm collects possible alarms with which to correlate. If it can find no such alarms, and the flow has traversed a Cloud VNE (a network segment unmanaged by Prime Network), at the end of the flow a Cloud Problem alarm is issued. The original alarm is correlated to it. This alarm does not have a clearing alarm, thus the severity of the Cloud Problem alarm is informational.

Correlation

Due to the nature of the Cloud Problem alarm, the event does not try to correlate to another event, but creates a new ticket in the gateway where the event is the root cause alarm of the ticket.

Note When required, a correlation filter filters the Cloud Problem alarm. This enables or disables the ability of an alarm to create a Cloud Problem alarm and to correlate to it. The default value is false for all alarms in the system, meaning that an alarm does not correlate to the Cloud Problem alarm by default. However, there are several events that override the default configuration (these events are specific to Cisco devices) and are set to true, as follows:

- BGP Neighbor Down syslog
- OSPF Neighbor Loss syslog
- EIGRP Router Query to Neighbors Timeouted syslog

As described previously, other alarms might be correlated to it using the logic in the Cloud Problem subalarm. See Cloud Problem.

Note The Cloud Problem alarm does not filter the BGP Process Down alarm in the correlation process.

Impact Analysis

No impact analysis is performed for this alarm.

Source OID

See Managed Element OID (IManagedElementOid).

Component Unreachable

A VNE might be configured to poll its respective device in multiple network protocols (for example both SNMP and Telnet). In addition, each protocol can be configured for reachability testing. This means that when the VNE stops responding using a protocol, the device is considered unreachable.

Table 15-22 Component Unreachable—Subtype Events

Subtype Event Name	Description
Component Unreachable	Issued when the device is not responding to at least one of the network protocols that are configured for reachability. The VNE uses a retry mechanism to make sure the problem persists for a certain configurable duration before issuing an alarm. This means that it is resilient during short periods of network packet loss. **Note** Prime Network will generate Device Unreachable events, with corresponding SNMP Timeout messages in the AVM log file, for devices with nonunique SNMP engine identifiers. These identifiers are normally derived from the unique MAC address of the device and assigned automatically. You can also customized them. But then you must try to avoid custom SNMP engine identifiers. However if you do use them, ensure that they are unique.
Component Reachable	Clearing event issued when the device responds to all the network protocols that are configured for reachability.
Device Partially Managed	Warning event issued when the device is partially managed.

Source OID

See Managed Element OID (IManagedElementOid) (the managed element of the Cloud VNE).

Checking Reachability

Reachability used by the VNEs (to check the reachability between the VNEs and network elements) depends on the configuration of the VNE, and involves multiple connectivity tests using SNMP, Telnet/SSH, and ICMP, as appropriate.

The following table describes the various situations where an NE fails to respond to the protocols:

Table 15-23 Unreachable Network Elements

VNE Type	Protocol Used to Check Reachability	Action Taken When NE Fails to Respond	Action Taken When NE is Reachable
ICMP VNE	ICMP only. During the ICMP test, the unit pings the NE every configured interval.	ICMP ping is suspended, and a VNE Unreachable event is sent to the Prime Network Gateway. Thereafter, only the reachability tests are run to detect when the device is reachable again.	ICMP ping is restarted, and the alarm is cleared.

Table 15-23 Unreachable Network Elements (continued)

VNE Type	Protocol Used to Check Reachability	Action Taken When NE Fails to Respond	Action Taken When NE is Reachable
Generic VNE	• SNMP only (default). Polls the sysoid of the NE using an **SNMP get** command during the SNMP reachability test, and expects to receive a response; or • SNMP only (default), and adding an ICMP test.	General polling is suspended, and a VNE Unreachable event is sent to the Prime Network Gateway. Thereafter, only the reachability tests are run to detect when the device is reachable again. If more than one protocol is used, it is enough for one of them to become unreachable to generate the event. The event is generic to all the protocols.	• General polling is restarted, and all commands are sent to the device, smoothed across the polling interval. • The alarm is cleared.
Full VNE	• SNMP only (default). Polls the sysoid of the NE using an **SNMP get** command during the SNMP reachability test, and expects to receive a response; or • SNMP only (default), and adding ICMP and Telnet. During the Telnet test, the unit sends `Enter` via the open session and expects to get a prompt back.	General polling is suspended, and a VNE Unreachable event is sent to the Prime Network Gateway. Thereafter, only the reachability tests are run to detect when the device is reachable again. If more than one protocol is used, it is enough for one of them to become unreachable to generate the event. The event is generic to all the protocols.	• General polling is restarted, and all commands are sent to the device, smoothed across the polling interval. • The alarm is cleared.

Each of these scenarios has two possible settings in the registry:

- Track reachability (true/false). The default is true.

  When this parameter is true, reachability is tracked according to the specific protocol (ICMP, SNMP, Telnet, and so forth).

  When this parameter is false, the test is not performed.

- Lazy reachability (true/false). The default is false. This parameter determines whether there is a dedicated reachability command in charge of tracking reachability or whether reachability is determined by the regular polled commands.

  When this parameter is true, reachability is based on polling, and a dedicated command is not activated.

  When this parameter is false, a dedicated SNMP command is activated, and this test verifies the response from a specific SNMP OID (sysoid is the default that can be changed).

  After the first failure of a command and all its retries, the device is considered unreachable. At this point, Prime Network starts to poll the device using the dedicated reachability command (see Table 15-23). In normal track reachability mode (lazy=false), the reachability commands run all the time. When the reachability test succeeds for the first time, it stops running and the device is considered reachable again.

Note Changes to the registry should be performed only with the support of Cisco. For details, contact your Cisco account representative.

Correlation

The alarm correlates to other alarms using the network correlation mechanism, which runs a forward IP flow from the global routing entity to the management IP address (that is, to the IP address of the unit on which the VNE resides). This flow might collect the following alarms: Device Unreachable, Link Down, Port Down, Interface Status Down, BGP Neighbor Loss, and so forth.

Other alarms might correlate to it using the ManagedElement key.

Note The Device Unreachable alarm filters out the Link Down on Unreachable alarm in the correlation process. Events with the same weight are not filtered out.

Impact Analysis

No impact analysis is performed for this alarm.

Source OID

See Managed Element OID (IManagedElementOid).

CPU Utilization

VNEs are configured to trace their device CPU utilization. An alarm is issued when device CPU utilization crosses a configured threshold. The thresholds, as defined in the registry under the managed element, are:

- Upper threshold—80%
- Lower threshold—40%

Table 15-24 CPU Utilization—Subtype Events

Subtype Event Name	Description
CPU Overutilized	Issued when the device CPU usage is above the configured upper threshold.
CPU Normal Utilization	Clearing event. Issued when the device CPU usage returns to below the lower threshold.

Correlation

Due to the nature of CPU utilization alarms, the event does not try to correlate to another event; it creates a new ticket in the gateway where the event is the root cause alarm of the ticket.

No other alarm tries to correlate to this alarm.

Impact Analysis

No impact analysis is performed for this alarm.

Source OID

See Managed Element OID (IManagedElementOid).

Device Unsupported

A VNE identifies various loading situations that prevent regular operation of the VNE. When such a situation occurs, the VNE issues a Device Unsupported alarm.

Table 15-25 Device Unsupported—Subtype Events

Subtype Event Name	Description
Device Unsupported	Issued for the following scenarios: • The device type identified by its sysOid is not identified by the system. • The device software version is not supported, and the VNE is configured to react when a device is unsupported. Other possible actions are: use the default version, load generic VNE, or load ICMP VNE. • Registry problems occur when trying to load generic or ICMP VNEs. • The VNE failed to retrieve the device sysOid or software version.

Correlation

Due to the nature of the Device Unsupported alarm, the event does not try to correlate to another event and creates a new ticket in the gateway where the event is the root cause alarm of the ticket.

No other alarms can correlate to this alarm.

Impact Analysis

No impact analysis is performed for this alarm.

Source OID

See Managed Element OID (IManagedElementOid).

Discard Packets

VNEs are configured to trace the discarded packet counters on their device ports. An alarm is issued when the discarded counter for a port crosses the configured thresholds. The thresholds, as defined in the registry under PortLayer1, are:

- Upper threshold—500 packets per second.
- Lower threshold—50 packets per second.

Table 15-26 Discard Packets—Subtype Events

Subtype Event Name	Description
Discard Packets	Issued when the number of discarded packets on a device port is higher than the configured threshold.
Normal Discard Packets	Clearing alarm. Issued when the number of discarded packets on a devices port is lower than the configured threshold.

Correlation

Due to the nature of the Discard Packets alarm, the event does not try to correlate to another event, and creates a new ticket in the gateway where the event is the root cause alarm of the ticket.

No other alarms can correlate to this alarm.

Impact Analysis

By default, impact analysis is not supported for this alarm, but it can be enabled. If enabled, a flow starts to collect all the affected services passing this port. The endpoint of such services can be any termination point, such as an IP interface, VC, Port, VRF, and so on.

Source OID

See Physical Layer OID (IPhysicalLayerOid).

Dropped Packets

VNEs are configured to trace the dropped packet counters on their device ports. An alarm is issued when a dropped packet counter from a port crosses the configured thresholds. The thresholds, as defined in the registry under PortLayer1, are:

- Upper threshold—500 packets per second.
- Lower threshold—50 packets per second.

Table 15-27 Dropped Packets—Subtype Events

Subtype Event Name	Description
Dropped Packets on Port	Issued when the number of dropped packets on a device port is higher than the configured threshold.
Stopped Dropping Packets on Port	Clearing event. Issued when the number of dropped packets on a device port is lower than the configured threshold.

Correlation

Due to the nature of the Dropped Packets on Port alarm, the event does not try to correlate to another event. It creates a new ticket in the gateway where the event is the root cause alarm of the ticket.

No other alarms can correlate to this alarm.

Impact Analysis

By default, impact analysis is not supported for this alarm, but it can be enabled. If enabled, a flow starts to collect all the affected services passing this port. The endpoint of such services can be any termination point, such as an IP interface, VC, port, VRF, and so on.

Source OID

See Physical Layer OID (IPhysicalLayerOid).

DS0 Bundle Service Alarm

DS0 Bundle is a logical interface with an administration and operational status. The DS0Bundle Service alarm is generated when the administration or operational status changes.

Table 15-28 DS0 Bundle Service—Subtype Events

Subtype Event Name	Description
DS0 Bundle Admin Down	Generated when the DS0 Bundle status changes from OK to Admin Down.
DS0 Bundle Oper Down	Generated when the DS0 Bundle status changes from OK to Oper Down.
DS0 Bundle Up	Generated when the DS0 Bundle status changes from Not OK to OK.

Correlation

This alarm will be correlated to lower layer events, such as Port Down. Upper layer events can be correlated to this event.

Impact Analysis

No impact analysis is performed for this alarm.

Source OID

See DS0 Bundle OID (IDS0BundleOid).

DS1 Path Link Down

DS1 Path Link Down is generated when an administrative or operational path shutdown occurs.

Table 15-29 DS1 Path Link Down—Subtype Events

Subtype Event Name	Description
DS1 Path Link Down Due to Admin Down	Generated when the path is administratively shut down.
DS1 Path Link Down Due to Oper Down	Generated when the path is operatively shut down.
DS1 Path Link Down Due to Card	Generated when the card is down in the DS1 path.
DS1 Path Link Down on Unreachable	Generated when the path is not reachable.
DS1 Path Link Up	Generated when the DS1 path is up.

Correlation

DS1 Path Link Down can be correlated to lower level alarms, such as Port Down. It can be the root cause for higher level alarms.

Impact Analysis

No impact analysis is performed for this alarm.

Source OID

See Topological Link OID (ITopologicalLinkOid), where each endpoint is a DS1 Path OID (IDS1PathOid).

DS1 Path Port Down

DS1 Path Port Down is generated when an administrative or operational path shutdown occurs.

Table 15-30 DS1 Path Port Down—Subtype Events

Subtype Event Name	Description
DS1 Path Port Down Due to Admin	Generated when the DS1 port path is administratively down.
DS1 Path Port Down Due to Oper	Generated when the DS1 port path is operatively down.
DS1 Path Port Down Due to Card	Generated when the card is down in the DS1 port path.
DS1 Path Port Up	Generated when the DS1 port path is up.

Correlation

DS1 Path Port Down can be correlated to lower level alarms, such as Port Down. It can be the root cause for higher level alarms.

Impact Analysis

No impact analysis is performed for this alarm.

Source OID

See DS1 Path OID (IDS1PathOid).

DS3 Path Link Down

DS3 Path Link Down is generated due to administrative or operational shutdown of the path.

Table 15-31 DS3 Path Link Down—Subtype Events

Subtype Event Name	Description
DS3 Path Link Down Due to Admin Down	Generated when the path is administratively shut down.
DS3 Path Link Down Due to Oper Down	Generated when the path is operatively shut down.
DS3 Path Link Down Due to Card	Generated when the path is down due to card.
DS3 Path Link Down on Unreachable	Generated when the path is not reachable.
DS3 Path Link Up	Generated when the DS3 path is up.

Correlation

DS3 Path Link Down can be correlated to lower level alarms, such as Port Down. It can be the root cause for higher level alarms.

Impact Analysis

No impact analysis is performed for this alarm.

Source OID

See Topological Link OID (ITopologicalLinkOid), where each endpoint is a DS3 Path OID (IDS3PathOid).

DS3 Path Port Down

DS3 Path Port Down is generated when an administrative or operational path shutdown occurs.

Table 15-32 DS3 Path Port Down—Subtype Events

Subtype Event Name	Description
DS3 Path Port Down Due to Admin	Generated when the DS3 port path is administratively down.
DS3 Path Port Down Due to Oper	Generated when the DS3 port path is operatively shut down.
DS3 Path Port Down Due to Card	Generated when the DS3 port path is down due to card.
DS3 Path Port Up	Generated when the DS3 port path is up.

Correlation

DS3 Path Port Down can be correlated to lower level alarms, such as Port Down. It can be the root cause for higher level alarms.

Impact Analysis

No impact analysis is performed for this alarm.

Source OID

See DS3 Path OID (IDS3PathOid).

Dual Stack IP Changed

The dual stack IP interface alarm generates events when an interface goes from a dual IP address (IPv4 and IPv6) to a single stack, and when it goes from a single stack to a dual. That is, the event is generated when an IPv6 (global unicast address) or IPv4 address is removed from an interface. The event does not do any correlation but can be a root cause.

Table 15-33 Dual Stack IP Changed

Subtype Event Name	Description
Dual Stack IP Removed	Generated when all IPv6 (global unicast address) or all IPv4 addresses are removed from a dual-stack (two IP addresses) interface.
Dual Stack IP Added	Generated when an IPv6 (global unicast address) or IPv4 address is configured on a single-stack (one IP address) interface that was previously configured as a dual stack.

Correlation

No correlation is performed for this alarm.

Impact Analysis

No impact analysis is performed for this alarm.

Source OID

See IP Interface OID (IPInterfaceOid).

DWDM Controller Down

The DWDM controller has an Up and Admin-Down status. The DWDM Controller Down alarm is generated when the DWDM controller state changes. A DWDM Controller Down ticket is generated. The DWDM Controller Down alarm is based on polling results.

Table 15-34 DWDM Controller Down

Subtype Event Name	Description
DWDM Controller Down	The alarm trigger.
DWDM Controller Up	The clearing alarm.

Correlation

No correlation is performed for this alarm.

Impact Analysis

No impact analysis is performed for this alarm.

Source OID

See DWDM Controller OID (IDWDMOid).

DWDM G709 Status Down

The DWDM G709 wrapper has a status of up and down, The DWDM G709 Status Down alarm is generated when the G709 wrapper state changes, and the DWDM G709 Status Down ticket is generated. The alarm is based on the polling result; if the DWDM G709 wrapper status changes, the service alarm is triggered.

Table 15-35 DWDM G709 Status Down

Subtype Event Name	Description
DWDM G709 Status Down	The alarm trigger.
DWDM G709 Status Up	The clearing alarm.

Correlation

No correlation is performed for this alarm.

Impact Analysis

No impact analysis is performed for this alarm.

Source OID

See DWDM Controller OID (IDWDMOid).

EFP Down

The EFP Down alarm represents a state in which an Ethernet flow point (EFP) administrative or operational status changes from up to down. The alarm is cleared after the status value is set to up.

The polling of the status property can happen at every standard polling interval, or can be expedited following syslog handling.

The severity of the service alarms is Major, with the exception of EFP Up, which has the severity Cleared.

Table 15-36 EFP Down — Subtype Events

Subtype Event Name	Description
EFP Admin Down	EFP is in administrative status down.
EFP Down Due to Error Disabled	EFT is in operational status down and the error disabled property value is true.
EFP Oper Down	EFP is in operational status down.
EFP Up	Clearing event. Issued when the EFP status returns to up.

Correlation

The generated service alarm searches for its root cause through the correlation mechanism. In addition, the EFP Down alarm is the root cause for every relevant network event caused by the EFP Down event.

Impact Analysis

No impact analysis is performed for this alarm.

Source OID

See EFP OID (IEFPOID).

ESMC Process Down

The ESMC Process Down alarm is generated when an ESMC process is enabled or disabled. The alarm is cleared after the status value is set to up.

The polling of the status property can happen at every standard polling interval, or can be expedited following syslog handling.

Table 15-37 ESMC Process Down—Subtype Events

Subtype Event Name	Description
ESMC Process Down	The alarm triggering event when ESMC process is down.
ESMC Process Up	The alarm triggering event when ESMC process is up.

Correlation

No correlation is performed for this alarm.

Impact Analysis

No impact analysis is performed for this alarm.

Source OID

See ISyncEOID.

Fan-Tray Down

The Fan-Tray Down alarm is generated when the fan tray of the network element is powered down in the network elelment.

Table 15-38 Fan-Tray Down—Subtype Events

Subtype Event Name	Description
Fan-Tray Down	The alarm triggering event when fan tray is powered down.
Fan-Tray Up	The alarm triggering event when fan tray is powered up.

Correlation

No correlation is performed for this alarm.

Impact Analysis

No impact analysis is performed for this alarm.

Source OID

See Fan Tray OID.

Fan-Tray Out

The Fan-Tray Out alarm is generated when the fan tray of the network element is removed.

Table 15-39 Fan-Tray Out—Subtype Events

Subtype Event Name	Description
Fan-Tray Out	The alarm triggering event when fan tray is removed.
Fan-Tray In	The alarm triggering event when fan tray is available.

Correlation

No correlation is performed for this alarm.

Impact Analysis

No impact analysis is performed for this alarm.

Source OID

See Fan Tray OID.

GRE Keepalive

The GRE Keepalive alarm is generated when the GRE keepalive attribute is not configured or has been removed from a discovered GRE tunnel.

Table 15-40 GRE Keepalive—Subtype Events

Subtype Event Name	Description
Keepalive Not Set	The alarm triggering event when GRE Keepalive is not configured. The event is ticketable with a minor severity.
Keepalive Set	The clearing event.

Correlation

No correlation is performed for this alarm.

Impact Analysis

No impact analysis is performed for this alarm.

Source OID

See GRE Tunnel Endpoint OID Structure.

GRE Tunnel Down

Generic routing encapsulation (GRE) tunnels are basically stateless, meaning that when the tunnel is down, the tunnel edges might not identify this situation and continue reporting the tunnel as up. To overcome this, the GRE tunnel edge can be configured to send *keepalive* messages. If at some point a GRE tunnel edge does not receive keepalive messages, it can change its state to down.

The GRE Tunnel Down alarm is supported only on GRE tunnels that are configured with keepalive messages. When keepalive is configured on the GRE tunnel edge, if a failure occurs in the GRE tunnel at any point, both IP interfaces of the GRE tunnel edges change their state to down. This ensures that the alarm is identified. If keepalive is not configured on the GRE tunnel edge, because the alarm creation is triggered by the state change of the IP interface of the GRE tunnel, the GRE Tunnel Down alarm might not be generated.

Table 15-41 GRE Tunnel Down—Subtype Events

Subtype Event Name	Description
GRE Tunnel Down	Issued when a GRE link exists between the two tunnel edges and the state of the IP interface of one of the GRE tunnel edges changes to down. A simple negotiation procedure is done to avoid sending the event from both edges of the GRE tunnel, and a GRE Tunnel Down event is issued.
GRE Tunnel Up	Clearing event. Issued when the IP interface state changes back to up. The clearing event is issued even if the GRE link does not exist (for example, if you have chosen to clear and remove the event).

Correlation

The GRE Tunnel Down alarm tries to correlate to other alarms using the network correlation mechanism that runs a forward IP flow from the local GRE tunnel edge to the tunnel destination IP. This flow might collect the following alarms: Link Down, Port Down, Interface Status Down, and more.

Other alarms might correlate to it using the TunnelGre key.

Impact Analysis

No impact analysis is performed for this alarm.

Source OID

See Topological Link OID (ITopologicalLinkOid) (each endpoint is Layer 2 GRE Tunnel OID (ITunnelGreOid).

HSRP Group Status Changed

Hot Standby Router Protocol (HSRP) is used in IP networks and allows one router to automatically assume the function of the second router if the second router fails. The current support relates to the instance where only one backup router is configured in the HSRP group, though it is possible to configure more than one.

Table 15-42 HSRP Group Status Changed—Subtype Events

Subtype Event Name	Description
Primary HSRP Interface Is Not Active	Issued when the primary interface within an HSRP group has changed its state to down. This means that one of the other interfaces in the group becomes the active interface in the group. This alarm tries to correlate to other alarms using the network correlation mechanism that runs a forward IP flow from the local global routing entity to the HSRP group backup interface IP. Alarms can correlate to this alarm using the local IPInterface key.
Primary HSRP Interface Is Active	Clearing event for the Primary HSRP Interface Is Not Active alarm. Issued when the primary interface within a HSRP group has changed its state back to up after it was down. This means that if one of the other interfaces in the group was currently active it becomes secondary. This alarm is the clearing alarm for the Primary HSRP Interface Is Not Active alarm.
Secondary HSRP Interface Is Active	Issued when a secondary interface within an HSRP group has changed its state to up. This happens when the original active interface changes its state to down and the backup interface takes over. This alarm tries to correlate to other alarms using the network correlation mechanism that runs a forward IP flow from the local global routing entity to the HSRP group virtual IP. Alarms can correlate to this alarm using the local IPInterface key.
Secondary HSRP Interface Is Not Active	Clearing event for the Secondary HSRP Interface Is Active alarm. Issued when a secondary interface within a HSRP group has changed its state back to down after it was up. This means that the original active interface in that group has changed its state to up.

Correlation

For correlation to work, there must be a correlation path between the routers. Correlation details are described in the relevant subtype events in Table 15-42.

Impact Analysis

No impact analysis is performed for this alarm.

Source OID

See IP Interface OID (IPInterfaceOid) (IP interface of the active or secondary interface).

Interface Status

VNEs are configured to trace the operational state of their IP interfaces. When the status of an IP interface changes, the VNE issues the relevant alarm. There are multiple subtype events for Interface Status Down, and the subtype that is issued depends on the scenario. Each has a different behavior; these are described in Table 15-43.

Table 15-43 Interface Status—Subtype Events

Subtype Event Name	Description
Interface Status Down GRE Tunnel (GRE tunnel)	Issued when the IP interface on a GRE tunnel changes its state to down. Correlation—This alarm issues a local correlation process and tries to correlate to the GRE Tunnel Down alarm. If the GRE tunnel down does not exist (for example, in the case where no GRE link exists), the alarm is issued as the root cause. When the GRE tunnel is issued from the other edge of the tunnel, it uses the local alarm to correlate to it. Other alarms might correlate to it using the IPInterface key. This includes alarms such as Device Unreachable or any other alarms that perform network correlation and where the correlation flow traverses the IP interface.
Interface Status Down Connection (connection that is a point-to-point connection)	Issued when a point-to-point IP interface changes its state to down. The identification of this type of interface is done using the following: 1. The subnet mask is /30 or /31. 2. The IP interface is on one VC encapsulation. Correlation—The alarm correlates to other alarms using the network correlation mechanism that runs a forward down IP flow from the IP interface to other IP addresses in the IP interface's IP address subnet. This flow might collect the following alarms: Link Down, Port Down, and so on. Other alarms might correlate to it using the IPInterface or the physical port (PortLayer1) keys.
Interface Status Down Nonconnection (nonconnection that is a multipoint connection)	Issued when a point-to-point IP interface changes its state to down. The identification of this type of interface is done using the following: 1. The number of encapsulations under the IP interface/MPLS is greater than one. 2. Any other case not covered in the previously-described scenarios. Correlation—The alarm correlates to other alarms using the network correlation mechanism that runs a forward down flow from the IP interface to the physical port (PortLayer1) under this interface.
Interface Status Up	Clearing event. Issued when an IP interface changes its operational state from down to up.

Correlation

Correlation details are described in the relevant subtype events in Table 15-43.

Impact Analysis

No impact analysis is performed for this alarm.

Source OID

See IP Interface OID (IPInterfaceOid).

Investigation State

Situations might occur where one or more physical components (specifically modules) are not identified by the physical investigation component in a VNE. This is not an unusual scenario because many devices have large sets of supported modules, and not all of the modules may be supported by the VNE. The Investigation State alarm is issued in this scenario.

Table 15-44 Investigation State—Subtype Events

Subtype Event Name	Description
Investigation State	Issued when one or more modules are not identified by the physical investigation component of the VNE. There is no clearing event.

Correlation

Due to the nature of the Investigation State alarm, the event does not try to correlate to another event, and creates a new ticket in the gateway where the event is the root cause alarm of the ticket.

No other alarms can correlate to this alarm.

Impact Analysis

No impact analysis is performed for this alarm.

Source OID

See Managed Element OID (IManagedElementOid).

L2TP Peer Not Established

This alarm is specific to the Redback Networks implementation of Layer 2 Tunneling Protocol (L2TP), and is based on the state of an L2TP peer that is basically a logical entity from which L2TP tunnels are created. The L2TP peer is also used as a container for these L2TP tunnels. The alarm is issued when the L2TP peer has an incorrect tunnel configuration and the tunnels between the L2TP access concentrator (LAC) and the L2TP network server (LNS) cannot be created.

Table 15-45 L2TP Peer Not Established—Subtype Events

Subtype Event Name	Description
L2TP Peer Not Established	Issued when the L2TP peer has an incorrect configuration, and L2TP tunnels cannot be created between the LAC and the LNS. This is identified by querying the state of the L2TP peer tunnels that do not change to Established.
L2TP Peer Is Removed	Issued when the L2TP peer is removed from the L2TP peer list, or when the first tunnel in the peer changes its state from Established to another state.
L2TP Peer Established	Clearing event. Issued when at least one tunnel of the L2TP peer is in an Established state.

Correlation

The alarm correlates to other alarms using the network correlation mechanism that runs a forward down flow from the L2TP peer to the remote IP.

Other alarms can correlate to this alarm using the local L2TPpeer key.

Impact Analysis

No impact analysis is performed for this alarm.

Source OID

See L2TP Peer OID (IL2tpPeerOid).

L2TP Sessions Threshold

This alarm is specific to the Redback Networks implementation of L2TP and is implemented as a TCA of the number of sessions in a L2TP peer. The alarm is issued when the number of L2TP sessions related to the L2TP peer crosses a configurable threshold.

Table 15-46 L2TP Sessions Threshold—Subtype Events

Subtype Event Name	Description
L2TP Sessions Count Exceeds Maximum Threshold	Issued when the number of active sessions associated with the L2TP peer crosses a configurable threshold (the default is 80%). The calculation is done as follows: *active-sessions*/(*max-session-per-tunnel* * *max-tunnels-per-peer*) * 100.
L2TP Sessions Count Has Returned to Normal	Clearing event. Issued when the number of active sessions associated with the L2TP peer drops below the lower threshold (the default is 70%).

Correlation

Due to the nature of the L2TP Sessions Count Exceeds Maximum Threshold alarm, the event does not try to correlate to another event, and creates a new ticket in the gateway where the event is the root cause alarm of the ticket.

No other alarms can correlate to this alarm.

Impact Analysis

No impact analysis is performed for this alarm.

Source OID

See L2TP Peer OID (IL2tpPeerOid).

Note This alarm is implemented as TCA, which means that no information about this alarm is found in the standard event-related registry.

Lag Down

The Lag Down alarm is generated when the status of the Link Aggregation changes.

Table 15-47 Lag Down—Subtype Events

Subtype Event Name	Description
Lag Admin Down	Issued when the status changes due to administrative status change.
Lag Oper Down	Issued when the status changes due to oper status change.
Lag Up	Clearing Event. Issued when the status is up again.

Correlation

Lag Down alarm does not correlate to any alarm. No other alarms can correlate to this alarm.

Impact Analysis

No impact analysis is performed for this alarm.

Source OID

See Lag Down OID.

Lag Link Down

The Lag Link Down alarm is generated when the status of the Lag Link changes in the logical inventory.

Table 15-48 Lag Link Down—Subtype Events

Subtype Event Name	Description
Lag Link Admin Down	Generated when lag link is administratively down.
Lag Link Oper Down	Generated when lag link is operatively down.
Lag Link Down on Unreachable	Generated when lag link is not reachable.
Lag Link Down on Unreachable	Clearing Event. Issued when the status is up again.

Correlation

Lag Link Down alarm does not correlate to any alarm. No other alarms can correlate to this alarm.

Impact Analysis

No impact analysis is performed for this alarm.

Source OID

See Lag Link Down OID.

Layer 2 Tunnel Down

A Layer 2 tunnel represents a point-to-point pseudowire in the network, also known as an AToM. This alarm is issued when the operational state of a Layer 2 tunnel changes.

Table 15-49 Layer 2 Tunnel Down—Subtype Events

Subtype Event Name	Description
Layer 2 Tunnel Down	Issued when the operational state of the Layer 2 tunnel changes its state to down. This can happen due to a problem between the two edges of the tunnel or on the local tunnel interface. When the state changes on both edges, a simple negotiation procedure is done to avoid sending the alarm from both edges of the Layer 2 tunnel.
Layer 2 Tunnel Up	Clearing event. Issued when the Layer 2 tunnel changes its state back to up.

Correlation

Because this alarm can be caused by multiple conditions, it issues multiple network correlation flows, which run as follows:

- A network flow from the Layer 2 tunnel to the remote IP to identify problems that occur between the tunnel edges.

  This flow might collect the following alarms: Link Down, Port Down, MPLS alarms, and so on.

- A network flow from the local Layer 2 tunnel edge to the physical port on which it is configured, to identify problems that occur on the local physical interface.

  This flow might collect the following alarms: Link Down, Port Down, and so on.

- A network flow from the remote Layer 2 tunnel edge to the physical port on which it is configured, to identify problems that occur on the remote physical interface.

  This flow might collect the following alarms: Link Down, Port Down, and so on.

Any alarm can correlate to this alarm using the PTP Layer2 MPLS Tunnel (which represents the Layer 2 tunnel edge) key.

Note The Layer 2 Tunnel Down alarm does not filter out the LDP Neighbor Down alarm in the correlation process.

Impact Analysis

No impact analysis is performed for this alarm.

Source OID

See Topological Link OID (ITopologicalLinkOid) (each endpoint is Layer 2 MPLS Tunnel OID (IPTPMplsLayer2TunnelOid).

LDP Neighbor Loss

LDP enables neighboring P or PE routers acting as LSRs to discover peers in an MPLS network to which they can establish LDP sessions. The sessions allow the routers to negotiate and exchange labels used for forwarding packets.

If a session to an LDP neighbor goes down, an LDP Neighbor Down alarm is issued. This can happen as the result of a failure in the TCP connection used by the LDP session, or if the interface is no longer running MPLS. The LDP neighbor down alarm is cleared by a corresponding LDP Neighbor Up alarm.

The alarm is issued when a peer is removed from the table in the LDP Neighbors tab. The alarm runs a correlation flow to detect the network core triggering event. A root cause analysis is performed to find the root cause. The alarm initiates an IP-based flow toward the peer transport address destination. If an alarm is found during the flow, that alarm is correlated to the LDP Neighbor Down alarm.

Note The LDP Neighbor Down alarm can correlate to the MPLS Interface Removed alarm.

VNEs are configured to trace the state of the current LDP neighbor of their devices. The VNE issues the relevant alarm when it identifies that an existing LDP neighbor has been removed, or that an LDP neighbor that was removed has been restored.

The identification of this alarm is expedited by notifications such as syslogs or traps.

Table 15-50 LDP Neighbor Loss—Subtype Events

Subtype Event Name	Description
LDP Neighbor Down	Issued when an LDP neighbor of the device that was previously discovered is removed.
LDP Neighbor Up	Clearing event. Issued when the LDP neighbor that was previously removed is restored and is currently active.

Correlation

This alarm issues a network correlation flow that runs a forward down flow from the global routing entity to the LDP peer IP address.

This flow might collect the following alarms: MPLS Interface Removed, Link Down, Port Down, and so on.

Any alarm can correlate to this alarm using the LDPPeer or LDPpeerDiscoverySources keys.

Note The LDP Neighbor Down alarm does not filter out the MPLS Interface Removed alarm in the correlation process.

Impact Analysis

No impact analysis is performed for this alarm.

Source OID

See LSE OID (ILseOid) (Label Switching Entity with the differentiator object of the LDP peer).

Link Down

This is one of the basic service alarms supported in the system. When a port has an adjacent peer (that is, it is connected to another port and has a discovered link), and its operational state changes from up to down or from down to up, the alarm is issued. When the port is not adjacent, a Port Down alarm is issued instead of a Link Down alarm. See Port Down.

The negotiation process between the two link edges occurs when the port's operational state changes to down to identify the exact event that should be issued.

Table 15-51 Link Down—Subtype Events

Subtype Event Name	Description
Link Down Due to Admin Down	Issued when the admin state of at least one of the link ports changes to down. Correlation—Due to the nature of this alarm, the event does not try to correlate to another event, and creates a new ticket in the gateway that is the root cause alarm of the ticket.
Link Down Due to Oper Down	Issued when the admin state is up on both ports and none of the scenarios described below occur. Correlation—This alarm issues a local correlation process and tries to correlate to other alarms using the physical port (PortLayer1) key.
Link Down Due to Card Event	Issued when at least one of the ports is on a card that was removed from the device, or is currently in an operational down state. Correlation—This alarm issues a local correlation process and tries to correlate to other alarms (specifically Card Out or Card Down) using the Module key.
Link Down on Unreachable	Issued when at least one of the ports is on a device that is currently unreachable by its VNE. Correlation—This alarm issues a local correlation process in order to correlate to the Device Unreachable alarm (using the ManagedElement key).
Link Up	Clearing event. Issued when the port operational state changes back to up.

Link Down supports flapping with the following subevents:

- Link Down Flapping
- Link Down Flapping Update
- Link Down Stopped Flapping Cleared
- Link Down Stopped Flapping Noncleared

Note In Prime Network Events, these flapping subevent names are displayed in the event's short description field.

Correlation

Other alarms can try to correlate to any link down alarm using the physical port (PortLayer1) key.

Impact Analysis

No impact analysis is performed for this alarm.

Source OID

See Topological Link OID (ITopologicalLinkOid) where each endpoint is Physical Layer OID (IPhysicalLayerOid).

Link Utilization

VNEs are configured to trace the Rx and Tx counters on their device ports, where a port has an adjacent peer (that is, it is connected to another port), and it already issued a Rx Overutilized or Tx Overutilized alarm. (For more information on these alarms, see Rx Utilization and Tx Utilization.) This alarm has complementary functionality so that all the utilization alarms from both ports of the link correlate to it, instead of issuing multiple root cause alarms.

Table 15-52 Link Utilization—Subtype Events

Subtype Event Name	Description
Link Overutilized	Issued after Tx Overutilized or Rx Overutilized alarms are issued on a physical port, if the port has an adjacent peer to enable correlation of all port level utilizations alarms from the ports on both sides of the link to one link utilization alarm.
Link Utilization Normal	Clearing event. Issued if both sides of the link send clearing alarms on the Tx utilization and Rx utilization alarms.

Correlation

Due to the nature of this alarm, the event does not try to correlate to another event, and creates a new ticket in the gateway where the event is the root cause alarm of the ticket.

Other alarms can correlate to this alarm using the physical port (PortLayer1) key.

Impact Analysis

No impact analysis is performed for this alarm.

Source OID

See Topological Link OID (ITopologicalLinkOid) where each endpoint is Physical Layer OID (IPhysicalLayerOid).

Log Archive is Disabled on the Device

A VNE that is modeled in the reduced polling mode uses the device log archive feature to identify the changed configuration applied on the device to update the VNE in Prime Network. If the archive is disabled on device, Prime Network generates the service alarm. The Prime Network administrator must enable the archive on the selected device as a corrective action.

For more information on device specific settings required, see *Device Configuration Tasks for VNE Creation* in the *Cisco Prime Network 3.9 Administrator Guide*.

Correlation

No correlation.

Impact Analysis

No impact analysis is performed for this alarm.

Source OID

See Managed Element OID (IManagedElementOid).

Local Switching Down

The Local Switching Entry Down Alarm is issued when the status of the local switching entry changes.

Table 15-53 Logical Port Down—Subtype Events

Subtype Event Name	Description
Local Switching Entry Down	Generated when the status changes to down.
Local Switching Entry Up	Clearing event for the Local Switching Entry down alarm.

Correlation

Local Switching Entry Down alarm uses flow based correlation.

The VNE with flow based correlation mechanisim uses an active correlation flow that traverses among three layers of the network (Layer 1,Layer 2, and Layer 3) and tries to correlate along a specified network path to an alarm. Based on the alarm that could occur in any one of the layers, it will try to find the root cause alarm.

Impact Analysis

No impact analysis is performed for this alarm.

Source OID

See Local Switching Entry Down OID.

Logical Port Down

Logical ports are logical interfaces that are defined on physical ports. Logical ports are used to logically separate the traffic of the physical port, and to control the separated traffic in a different manner. Logical ports are currently implemented in Prime Network for specific VNE types (for example, Lucent WAN Switches) and specific technologies (such as ATM and Frame Relay). Each logical port has an independent administrative and operational state. When the operational state of a logical port changes, the VNE issues an alarm.

Table 15-54 Logical Port Down—Subtype Events

Subtype Event Name	Description
Logical Port Down	Issued when the operational state of a logical port changes to down.
Logical Port Up	Clearing event. Issued when the operational state of a logical port changes back to up.

Correlation

This alarm issues a local correlation process and tries to correlate to alarms on the physical port using the physical port (PortLayer1) key. Possible alarms that this alarm can correlate to are Link Down, Port Down, or any alarm on the physical port.

Other alarms might correlate to it using the logical port key, including alarms that perform network correlation, and the correlation flow traverses the logical port.

Note The Logical Port Down alarm does not filter out the BGP Process Down alarm in the correlation process.

Impact Analysis

No impact analysis is performed for this alarm.

Source OID

See Logical Port OID (ILogicalPortOid).

LSP Down

LSP down is generated from both the endpoints of the MPLS-TP tunnel if the endpoint status goes down. The alarm is cleared after the status value changes from down to up.

Table 15-55 LSP Down

Subtype Event Name	Description
LSP Down	Issued when LSP Endpoint goes down.
LSP Down Due to Label Mismatch	Issued when LSP Endpoint status goes down, it will start the flow to find out whether it is down due to label mismatch in the flow (out going label / in going label does not match). It can be generated for the first time when LSP endpoint discovers. It is not necessary to have LSP Status Transition from Up to Down.
LSP Down Due to Lock Out	Issued when user configures a lock out. It will be also generated without a state transition. It means that this service alarm will be generated first time, if LSP Endpoint status is locked out.
LSP Up	Issued when LSP Endpoint goes up.

Correlation

This alarm issues a local correlation process and tries to correlate to alarms on the physical port using the physical port (PortLayer1) key.

Impact Analysis

No impact analysis is performed for this alarm.

Source OID

See LSP Endpoint OID (LSP EndPoint OID).

Members Changed

Members Changed alarm is generated if there is a status change for any member of the aggregation entity such as Ethernet LAG, MLPPP or IMA Group. For example, if an Ethernet LAG group has 4 Ethernet links (members) configured as part of the group and if one link goes down, a low priority Members Changed is generated indicating that 1 out of 4 links (25% of links) are down. If three or all links go down (75% of links or all links), a high priority service alarm is generated. Based on the configuration of thresholds in the registry the aggregation service alarm is a low priority, medium priority or high priority service alarm.

Table 15-56 Members Changed

Subtype Event Name	Description
High Priority Member Down	Issued when the percentage of active links is greater than zero and less than or equal to the high priority threshold defined in the registry.
Medium Priority Member Down	Issued when the percentage of active links is less than or equal to the medium priority threshold and greater than the high priority threshold defined in the registry.
Low Priority Member Down	Issued when the percentage of active links is less than or equal to the low priority threshold and greater than the medium priority threshold defined in the registry.
All Members Operationally Up	Issued when all the member links are up.

Correlation

Members Changed service alarm does not try to correlate with any other alarm.

No other alarms can correlate to this alarm.

Impact Analysis

No impact analysis is performed for this alarm.

Source OID

Members Changed Alarms will have any one of the following OIDs based on the members that have changed.

- IMA Service (IIMAGroupOid)
- MLPPP OID (IMLPPPOid)
- Lag Down OID
- Members Changed OID (IDataLinkAggregationOid)

If the status of the IMA group members is changed, Source OID will be IIMAGroupOid.

If the status of the MLPPP members is changed, it will be IMLPPPOid.

If the status of the EthernetChannel or LAG members is changed, Source OID will be IDataLinkAggregationOid.

Memory Utilization

VNEs are configured to trace their device memory utilization. A memory utilization alarm is issued when the device memory utilization crosses a configured threshold. The thresholds, as defined in the registry under ManagedElement, are:

- Upper threshold—80%
- Lower threshold—40%

Table 15-57 Memory Utilization—Subtype Events

Subtype Event Name	Description
Memory Overutilized	Issued when the device memory usage is above the configured upper threshold.
Memory OK	Clearing event. Issued when the device memory usage is back below the lower threshold.

Correlation

Due to the nature of the Memory Utilization alarm, the event does not try to correlate to another event, and creates a new ticket in the gateway where the event is the root cause alarm of the ticket.

No other alarms can correlate to this alarm.

Impact Analysis

No impact analysis is performed for this alarm.

Source OID

See Managed Element OID (IManagedElementOid).

MLPPP Bundle

MLPPP Bundle does not generate a Service alarm for each endpoint; it generate the alarm for links. If a link is not available, the service alarm is generated for individual endpoints. MLPPP Bundle can be a root cause. However, it cannot be correlated to other service alarms; that is, another event cannot be the root cause of MLPPP Down. MLPPP Bundle is ticketable.

Table 15-58 MLPPP Bundle Service Alarm

Subtype Event Name	Description
MLPPP Down Due To Flapping	Generated when MLPPP is down due to flapping.
MLPPP Down Flapping Update	Generated when MLPPP flapping update occurs.
MLPPP Down Flapping Proxy	Generated when MLPPP is down due to flapping proxy.

Table 15-58 MLPPP Bundle Service Alarm

Subtype Event Name	Description
MLPPP Down Due To Admin Down	Generated when MLPPP is administratively shut down on either side.
MLPPP Down Due To Oper Down	Generated when MLPPP is down but neither endpoint is operatively shut down.
MLPPP Up	Generated when either side changes to up.

Correlation

MLPPP Down cannot be correlated to other events. However, other events can correlate to MLPPP Down.

Impact Analysis

No impact analysis is performed for this alarm.

Source OID

See MLPPP OID (IMLPPPOid) or Topological Link OID (ITopologicalLinkOid), where each endpoint is a MLPPP OID (IMLPPPOid).

MPLS Black Hole Found

An MPLS black hole is an abnormal termination of an MPLS path (an LSP) inside an MPLS network. An MPLS black hole exists when there are untagged entries destined for a known PE router on a specific interface. Note that the untagged interfaces might exist in the network in normal situations. For example, where the boundary of the MPLS cloud has untagged interfaces, this is still considered normal.

MPLS black hole cause the loss of all the MPLS labels on a packet, including the VPN information that lies in the inner MPLS label. Therefore, if a packet goes through an untagged interface, the VPN information is lost. The VPN information loss translates directly to VPN sites losing connectivity.

Black hole alarms are detected in either of the following situations:

- When the system is loaded for the first time and performs the initial discovery of the network.
- Changes in the network are identified through the ongoing discovery process.

Note MPLS black hole discovery is supported only when the PEs are managed by Prime Network.

Table 15-59 MPLS Black Hole Found—Subtype Events

Subtype Event Name	Description
MPLS Black Hole Found	Issued when an MPLS interface has at least one untagged LSP leading to a known PE router; in other words, an LSE entry changed to an Untagged action with a PE as a next hop. After an MPLS Black Hole Found alarm is issued, a process begins looking for broken LSPs that go through the MPLS black hole. See Broken LSP Discovered.
MPLS Black Hole Cleared	Clearing event. Issued when the MPLS interface that had untagged LSPs to a known PE router has no more untagged entries to any known PE neighbor.

Correlation

The MPLS Black Hole Found alarm can correlate to MPLS Interface Removed and LDP Neighbor Loss alarms. Broken LSP Discovered alarms can correlate to MPLS Black Hole Found alarms.

Note The MPLS Black Hole Found alarm does not filter out the MPLS Interface Removed and LDP Neighbor Down alarms in the correlation process.

Impact Analysis

No impact analysis is performed for this alarm.

Source OID

See LSE OID (ILseOid) (appended with a differentiator of the next hop interface name).

MPLS TP Bandwidth Mismatch

The MPLS TP bandwidth mismatch alarm is generated when there is a bandwidth mismatch in the two directions of the MPLS-TP tunnel.

Table 15-60 MPLS TP Bandwidth Mismatch

Subtype Event Name	Description
MPLS TP Bandwidth Mismatch	Issued when there is a bandwidth mismatch in the two directions of the MPLS-TP tunnel.

Correlation

There is no correlation for this alarm.

Impact Analysis

No impact analysis is performed for this alarm.

Source OID

See LSP Endpoint OID (LSP EndPoint OID)

MPLS Interface Removed

The MPLS interface is basically a representation of the MPLS sublayer in an interface configuration. The interface can be configured with or without MPLS capabilities. If this type of configuration change takes place while the VNE is loaded, it issues MPLS interface removed or added alarms.

Table 15-61 MPLS Interface Removed—Subtype Events

Subtype Event Name	Description
MPLS Interface Removed	Issued when an MPLS interface has at least one untagged LSP leading to a known PE router (that is, an LSE entry changed to an Untagged action with a PE as a next hop). After an MPLS Black Hole Found alarm is issued, a process that looks for broken LSPs that go through this MPLS black hole is started. See Broken LSP Discovered.
MPLS Interface Added	Clearing event. Issued when the MPLS capabilities of an interface are enabled after they were disabled.

Correlation

The alarm correlates to other alarms using the network correlation mechanism which runs a forward flow to the underlying physical port. This flow might collect the Card Out and Card Down alarms, because the only other cases in which it happens are due to other faults that are hardware related.

Other alarms might correlate to it using the MPLS key, including MPLS black hole alarms, MPLS TE Tunnel Down alarm, and so on.

Impact Analysis

No impact analysis is performed for this alarm.

Source OID

See LSE OID (ILseOid) (Label Switching Entity with differentiator object of the MPLS interface description).

MPLS TE FRR State Changed

The MPLS TE FRR State Changed service alarm is triggered when the backup MPLS TE FRR tunnel changes from Ready to Active, and from Active to Ready.

Table 15-62 MPLS TE FRR State Changed

Subtype Event Name	Description
MPLS TE FRR State Changed to Active	Generated when the status of the protecting MPLS TE FRR tunnel changes from Ready to Active because of a network failure in the primary tunnel segment.
MPLS TE FRR State Changed to Ready	Generated when the status of the protecting MPLS TE FRR tunnel changes back to Ready.

Correlation

Correlation is performed.

Impact Analysis

No impact analysis is performed for this alarm.

Source OID

See MPLS TE Tunnel OID (IMplsTETunnelOid).

MPLS TE Tunnel Down

MPLS TE tunnel alarms include:

- MPLS TE Tunnel Down
- MPLS TE Tunnel Flapping
- Tunnel Reoptimized

If a TE tunnel operational status changes to down, an MPLS TE Tunnel Down alarm is generated. The Prime Network correlation engine supports the MPLS TE Tunnel link between the head and tail ends of the network element. The engine also identifies the faults that affect the TE tunnel status and identifies the root cause for the MPLS TE Tunnel Down alarm. For example, a Link Down will cause a TE tunnel to go down. Multiple up and down alarms that are generated during a short time interval are suppressed and displayed as an MPLS TE Tunnel Flapping alarm (according to the specific flapping configuration).

MPLS TE Tunnel Down and MPLS TE Tunnel Flapping alarms are actively detected and service alarms are generated. The system also supports MPLS TE Tunnel Down syslogs, which are correlated to the service alarm.

For Cisco CRS-1 routers running Cisco IOS XR 3.6 software and using PBTS in MPLS or MPLS VPN networks, Prime Network supports the following subalarms for the MPLE TE Tunnel Down alarm:

- High Priority MPLS TE Tunnel Down
- Medium Priority MPLS TE Tunnel Down
- Low Priority MPLS TE Tunnel Down

The specific subalarm that is generated depends on the EXP bit specified for the traffic. Prime Network maps the specified EXP bit to tunnel priority and uses that mapping to generate the resultant subalarm. The alarm description includes information about the EXP bit.

VNEs are configured to trace the operational state of their MPLS TE tunnel interfaces. When the state of the tunnel changes, the VNE issues the relevant alarm.

Table 15-63 MPLS TE Tunnel Down—Subtype Events

Subtype Event Name	Description
MPLS TE Tunnel Rerouted	Issued when the tunnel changes it state to down. MPLS TE Tunnel Down alarm supports flapping with the following subevents: • MPLS TE Tunnel Flapping • MPLS TE Tunnel Update • MPLS TE Tunnel Stopped Flapping Cleared • MPLS TE Tunnel Stopped Flapping Noncleared **Note** In Prime Network Events, these flapping subevent names are displayed in the event's short description field.
High Priority MPLS TE Tunnel Down	This alarm is issued if the EXP bit is set to denote high priority. Prime Network maps the bit to a high priority alarm.

Table 15-63 MPLS TE Tunnel Down—Subtype Events (continued)

Subtype Event Name	Description
Medium Priority MPLS TE Tunnel Down	This alarm is issued if the EXP bit is set to denote medium priority. Prime Network maps the bit to a medium priority alarm.
Low Priority MPLS TE Tunnel Down	This alarm is issued if the EXP bit is set to denote low priority. Prime Network maps the bit to low priority alarm.
MPLS TE Tunnel Rerouted	This alarm is issued when the MPLS TE Tunnel is Rerouted.
MPLS TE Tunnel Reoptimized	Tunnel reoptimization occurs when a tunnel is up and its route changes but the tunnel continues to remain up. When a TE tunnel is reoptimized to take a different path, the system parses the tunnel reoptimized syslog, if such a syslog is available, and displays it as a ticket. The Tunnel Reoptimized alarm is generated from a syslog message sent by the router.
MPLS TE Tunnel Up	Clearing event. Issued when an MPLS TE tunnel changes its operational state from down to up.

Correlation

For all the down alarms, any other alarm can try to correlate to this alarm using the MPLS TE tunnel OID (IMplsTETunnelOid) key. The alarm correlates to other alarms using the network correlation mechanism that runs a forward down IP flow from the MPLS TE tunnel to its tunnel destination IP address. This flow might collect the following alarms: Link Down, Port Down, and so on.

The MPLS TE Tunnel Down alarm does not filter out the BGP Process Down alarm in the correlation process.

When MPLS TE Tunnel Down alarm is generated, the corresponding MPLS TE Tunnel link will have the same severity of MPLS TE Tunnel Down Ticket.

Impact Analysis

No impact analysis is performed for this alarm.

Source OID

See MPLS TE Tunnel OID (IMplsTETunnelOid).

MPLS TP Tunnel Down

An MPLS TP Tunnel Down alarm is triggered when one side of the tunnel is down or when both sides of the tunnel are down. This alarm is generated based on a negotiation.

The polling of the status property can happen at every standard polling interval, or can be expedited following syslog handling.

Table 15-64 MPLS TP Tunnel Down

Subtype Event Name	Description
TP Tunnel Down Due to Admin Down	Issued by VNEs when one side of the tunnel is down.
TP Tunnel Down Due to Oper Down	Issued by VNEs when both sides of the tunnel are down.

Correlation

This alarm by itself can be the root cause of the alarm; and also can find the root cause of the alarm.

Impact Analysis

No impact analysis is performed for this alarm.

Source OID

See TP Tunnel Endpoint OID (TP Tunnel EndPoint OID).

Network-Clock Synchronization

A network-clock synchronization alarm is triggered when network synchronization is enabled/disabled in the port. The alarm is cleared after the status value is changed from disabled to enabled.

The polling of the status property can happen at every standard polling interval, or can be expedited following syslog handling.

Table 15-65 OSPF Neighbor State Changed

Subtype Event Name	Description
Network-Clock Synchronization Enabled	Issued when the network clock synchroization is enabled in the port.
Network-Clock Synchronization Disabled	Issued when the network clock synchroization is disabled in the port.

Correlation

No correlation for these alarms.

Impact Analysis

No impact analysis is performed for this alarm.

Source OID

See ISyncEOID

OSPF Neighbor State Change

An OSPF Neighbor Down alarm is triggered when the status of an OSPF changes. When the status of an OSPF is changed, an alarm will be issued by each neighbor as a separate event. These alarms will remain displayed until the parent ticket is cleared, that is until the status of the OSPF neighbor changes to its previous state.

An OSPF Neighbor Up alarm is a clearing event for the OSPF Neighbor Down alarm. It is triggered when the alarm state changes from down to up.

Table 15-66 OSPF Neighbor State Changed

Subtype Event Name	Description
OSPF Neighbor Up	Issued by the neighboring VNEs after the OSPF device status has changed to up.
OSPF Neighbor Down	Issued by the neighboring VNEs after the OSPF device status has changed to down.

Correlation

The root cause for an OSPF Neighbor Down can be correlated by the correlation flow towards the neighbor's interface IP address. OSPF neighbor down key is the OID of the neighbor, and is used for correlating OSPF Neighbor Down syslogs and traps to OSPF Neighbor Down alarm.

Impact Analysis

No impact analysis is performed for this alarm.

Source OID

See OSPF Neighbor State Change OID

Port Down

When a physical port does not have an adjacent peer (that is, it is connected to another port) and its operational state changes from up to down, or from down to up, port down alarms are issued. When the port does have an adjacent peer, instead of a Port Down alarm, a similar Link Down alarm is issued.

Port Down supports flapping with the following subevents:

- Port Down Flapping
- Port Down Flapping Update
- Port Down Stopped Flapping Cleared
- Port Down Stopped Flapping Noncleared.

See Link Down.

Table 15-67 Port Down—Subtype Events

Subtype Event Name	Description
Port Down Due to Admin	Issued when the admin state of a physical port changes to down.
Port Down Due to Oper	Issued when the operational state of a physical port changes to down.

Table 15-67 Port Down—Subtype Events (continued)

Subtype Event Name	Description
Port Down Due to Card Event	Issued when the port is on a card that was removed from the device or is currently in an operational down state. Correlation—This alarm issues a local correlation process and tries to correlate to other alarms (specifically Card Out or Card Down) using the Module key.
Port Up	Clearing event. Issued when the operational state of a logical port changes back to up.

Correlation

For all the down alarms, any other alarm can try to correlate to this alarm using the physical port (PortLayer1) key.

Impact Analysis

No impact analysis is performed for this alarm.

Source OID

See Physical Layer OID (IPhysicalLayerOid).

Power Supply Down

The power supply down alarm is generated when the power supply unit is powered down.

Table 15-68 Power Supply Down

Subtype Event Name	Description
Power Supply Down	Issued when the power supply unit is powered down.
Power Supply Up	Issued when the power supply unit is powered up.

Correlation

There is no correlation for this alarm.

Impact Analysis

No impact analysis is performed for this alarm.

Source OID

See Power Supply OID.

Power Supply Out

The power supply down out alarm is generated when the power supply unit is removed.

Table 15-69 Pluggable Transceiver Out

Subtype Event Name	Description
Power Supply Out	Issued when power supply unit is removed.
Power Supply In	Issued when power supply unit is inserted.

Correlation

There is no correlation for this alarm.

Impact Analysis

No impact analysis is performed for this alarm.

Source OID

See Power Supply OID.

Pluggable Transceiver Out

A pluggable transceiver out alarm is generated when a pluggable transceiver is removed from the physical port of the network element.

Table 15-70 Pluggable Transceiver Out

Subtype Event Name	Description
Pluggable Transceiver In	Issued when pluggable transceiver is inserted back in the interface of the network element.
Pluggable Transceiver Out	Issued when pluggable transceiver is removed from the interface of the network element.

Correlation

This alarm will correlate to port\link down due to oper\admin.

Impact Analysis

No impact analysis is performed for this alarm.

Source OID

See Port OID.

REP Port Role Change

A REP Port Role Change alarm is generated when there is a port role change from failed to okay. The alarm is cleared after the status value is set to okay.

The polling of the status property can happen at every standard polling interval, or can be expedited following syslog handling.

Table 15-71 REP Port Role Change

Subtype Event Name	Description
REP Port Role Failed	Issued when REP port is failed.
REP Port Role Ok	Issued when REP port is okay.

Correlation

For all the alarms, any other alarm can try to correlate to this alarm using the physical port (PortLayer1) key.

Impact Analysis

No impact analysis is performed for this alarm.

Source OID

See Physical Layer OID (IPhysicalLayerOid).

Rx Dormant

VNEs are configured to trace the Rx packet counters on their device ports. An alarm is issued when the Rx counter on a port drops below the configured threshold.

Note This alarm is disabled by default.

Table 15-72 Rx Dormant—Subtype Events

Subtype Event Name	Description
Rx Dormant	Issued when the number of Rx packets on a device port is lower than the configured threshold.
Rx Dormant Normal	Clearing event. Issued when the number of Rx packets on a device port returns to a number lower than the configured threshold.

Correlation

The port Rx Dormant alarm does not start a correlation process and is always issued as a root cause alarm.

Impact Analysis

No impact analysis is performed for this alarm.

Source OID

See Physical Layer OID (IPhysicalLayerOid).

Rx Utilization

VNEs are configured to trace the Rx packet counters on their device ports. An alarm is issued when a the Rx counter for a port crosses the configured thresholds. The thresholds, as defined in the registry under PortLayer1, are:

- Upper threshold—75%
- Lower threshold—50%

When a port has an adjacent peer (that is, it is connected to another port) a Link Utilization alarm is also issued. For more information on these alarms, see Link Utilization.

Table 15-73 Rx Utilization—Subtype Events

Subtype Event Name	Description
Rx Overutilized	Issued when the number of Rx packets on a device port is higher than the configured threshold.
Rx Utilization Normal	Clearing event. Issued when the number of Rx packets on a device port returns to a number lower than the configured threshold.

Correlation

The Rx utilization alarms do not start a correlation process. No other alarms can correlate to this alarm, because there are no supported alarms that can be affected by the Rx utilization alarm.

Impact Analysis

By default, impact analysis is not supported for this alarm, but can be enabled. If it is enabled, a flow starts to collect all the affected services passing this port. The endpoint of such services can be any termination point, such as an IP interface, VC, port, VRF, and so on.

Source OID

See Physical Layer OID (IPhysicalLayerOid).

Shelf Out

The Shelf Out alarm represents a state in which the shelf is removed from the device. The Shelf Out alarm is also issued when the device stops reporting on the existence of a shelf due to another failure, even if the shelf is actually still in the device. It is assumed that any functionality that was implemented by the shelf is not working anymore if the shelf had no redundancy configuration.

Table 15-74 Shelf Out—Subtype Events

Subtype Event Name	Description
Shelf Out	Issued when a shelf is removed from the device. It is possible that some shelf failures are identified as Shelf Out, because the device does not report on the shelf's existence after the failure.
Shelf In	Clearing event. Issued when the shelf is inserted back into the device.

Correlation

Due to the nature of the Shelf Out alarm, it does not start a correlation process and is always issued as a root cause alarm.

Other alarms might correlate to it using the Shelf key, such as the Card Out alarm.

Impact Analysis

No impact analysis is performed for this alarm.

Source OID

See Shelf OID (IShelfOid).

SONET Path Link Down

The SONET Path Link Down Alarm is issued when the status of the SONET path link changes.

Table 15-75 SONET Path Link Down—Subtype Events

Subtype Event Name	Description
SONET Path Link Down Due to Admin Down	Issued when the administrative status changes.
SONET Path Link Down Due to Oper Down	Issued when the oper status changes.
SONET Path Link Down Due to Card	Issued when the path link is down due to card.
SONET Path Link Down on Unreachable	Issued when the path link is down due to unreachable status.
SONET Path Link Up	Clearing event. Issue when the path link down status changes from down to up.

Correlation

This alarm correlates to port down and link down alarms.

Impact Analysis

No impact analysis is performed for this alarm.

Source OID

See SONET Path Link Down OID.

SONET Path Port Down

The SONET Path Port Down is issued when the status of the SONET path port changes.

Table 15-76 SONET Path Link Down—Subtype Events

Subtype Event Name	Description
SONET Path Port Down Due to Admin Down	Issued when the administrative status changes.
SONET Path Port Down Due to Oper Down	Issued when the oper status changes.
SONET Path Port Down Due to Card	Issued when the path port is down due to card.
SONET Path Port Up	Clearing event. Issued when the path port down status changes from down to up.

Correlation

This alarm correlates to port down and link down alarms.

Impact Analysis

No impact analysis is performed for this alarm.

Source OID

See SONET Path Port Down OID.

Subinterface Down

QinQ technology refers to the nesting of a VLAN header in an Ethernet frame in an already existing VLAN header. Both VLAN headers must be of the type 802.1Q. When one VLAN header is nested within another VLAN header, they are often referred to as *stacked VLANs*. QinQ technology allows service provider networks to carry traffic with double-tagged, stacked VLAN (802.1Q-in-Q) headers of multiple customers while maintaining the VLAN and Layer 2 protocol configurations of each customer without impacting the traffic of other customers.

A subinterface is a logical division of traffic on an interface, such as multiple subnets across one physical interface. A subinterface name is represented as an extension to an interface name using dot notation, such as Interface Gigabit Ethernet 0/1/2/3.10. In this example, the main interface name is Gigabit Ethernet 0/1/2/3 and the subinterface is 10.

A Subinterface Down alarm is issued when the administrative or operational state of an Ethernet subinterface of a stacked VLAN changes. This state can be polled at standard polling intervals or can be expedited following syslog handling.

Table 15-77 Subinterface Down—Subtype Events

Subtype Event Name	Description
Subinterface Down	Issued when the operational status of the subinterface changes from up to down.

Table 15-77 Subinterface Down—Subtype Events (continued)

Subtype Event Name	Description
Subinterface Admin Down	Issued when the administrative status of the subinterface changes from up to down.
Subinterface Up	Clearing event. Issued when the operational or administrative status of the subinterface changes from down to up.

Correlation

The Subinterface Down event searches for the root cause through the correlation mechanism. The Subinterface Admin Down event does not search for the root cause through the correlation mechanism.

Subinterface Down is the root cause for every relevant network event caused by the Subinterface Down event.

Impact Analysis

No impact analysis is performed for this alarm.

Source OID

See VLAN Tagged Interface OID (IVlanTaggedInterfaceOID).

Tx Dormant

VNEs are configured to trace the Tx packet counters on their device ports. An alarm is issued when an Rx counter on a port drops below the configured thresholds. The upper and lower thresholds are defined in the registry under PortLayer1.

Note This alarm is disabled by default.

Table 15-78 Tx Dormant—Subtype Events

Subtype Event Name	Description
Tx Dormant	Issued when the number of Tx packets on a device port is lower than the configured threshold.
Tx Dormant Normal	Clearing event. Issued when the number of Tx packets on a device port returns to a number higher than the configured threshold.

Correlation

The port Tx Dormant alarm does not start a correlation process and is always issued as a root cause alarm.

Impact Analysis

No impact analysis is performed for this alarm.

Source OID

See Physical Layer OID (IPhysicalLayerOid).

Tx Utilization

VNEs are configured to trace the Tx packets counters on their device ports. An alarm is issued when a Rx counter on a port crosses the configured thresholds. The thresholds, as defined in the registry under PortLayer1, are:

- Upper threshold—75%
- Lower threshold—50%

When a port has an adjacent peer (that is, it is connected to another port), a Link Utilization alarm is also issued. For more information on these alarms, see Link Utilization.

Table 15-79 Tx Utilization—Subtype Events

Subtype Event Name	Description
Tx Overutilized	Issued when the number of Tx packets on a device port is higher than the configured threshold.
Tx Utilization Normal	Clearing event. Issued when the number of Tx packets on a device port returns to a number lower than the configured threshold.

Correlation

The port Tx Utilization alarm does not start a correlation process. No other alarm tries to correlate to this alarm, because there are no supported alarms that can be affected by the Tx Utilization on Port alarm.

Impact Analysis

By default, impact analysis is not supported for this alarm, but can be enabled. If impact analysis is enabled, a flow starts to collect all the affected services passing this port. The endpoint of such services can be any termination point, such as an IP interface, VC, port, VRF, and so on.

Source OID

See Physical Layer OID (IPhysicalLayerOid).

VSI Down

The VSI Down alarm represents a state in which a virtual switch instance (VSI) administrative or operational status changes from up to down. The alarm is cleared after the status value is set to up.

The polling of the status property can happen at every standard polling interval, but it can be expedited following the trap handling of one of the following:

- VLAN interface status change of a VLAN that is connected to a VSI.
- Pseudowire status change of a pseudowire configured on the VSI.

The severity of the service alarms is Major, except for VSI Admin Down alarm.

Table 15-80 VSI Down —Subtype Events

Subtype Event Name	Description
VSI Down	VSI is in operational status down.
VSI Admin Down	VSI is in administrative status down.
VSI Up	VSI status is up.

Correlation

The VSI Down alarm does not start a correlation process and is always issued as a root cause alarm.

Impact Analysis

No impact analysis is performed for this alarm.

Source OID

See VSI OID (IVSIOID).

Registry Parameters

The following registry parameters are included in this section:

- Adaptive Polling
- All IP Interfaces Down
- ATM IMA Down
- BGP Link Down
- BGP Neighbor Loss
- BGP Process Down
- BFD Connectivity Down
- BFD Neighbor Loss
- Broken LSP Discovered
- Card Down
- Card Out
- Carrier Grade NAT Translations Create Rate
- Carrier Grade NAT Translations Delete Rate
- Carrier Grade NAT Inside-to-Outside Forward Rate
- Carrier Grade NAT Outside-to-Inside Forward Rate
- Carrier Grade NAT Inside-to-Outside Drops Port Limit Exceeded
- Carrier Grade NAT Inside-to-Outside Drops System Limit Reached
- Carrier Grade NAT Inside-to-Outside Drops Resource Depletion
- CFM Domain Fault

- Chassis Disconnected
- Cloud Problem
- Component Unreachable
- CPU Utilization
- Device Unsupported
- Discard Packets
- Dropped Packets
- DS0 Bundle
- DS1 Path Link Down
- DS1 Path Port Down
- DS3 Path Link Down
- DS3 Path Port Down
- Dual Stack IP Changed
- DWDM Controller
- DWDM G709 Status
- EFP Down
- GRE Keepalive
- GRE Keepalive
- GRE Tunnel Down
- HSRP Group Status Changed
- Interface Status
- Investigation State
- L2TP Peer Not Established
- L2TP Sessions Threshold
- Lag Down
- Lag Link Down
- Layer 2 Tunnel Down
- LDP Neighbor Loss
- Link Down
- Link Utilization
- Local Switching Down
- Logical Port Down
- LSP Down
- Members Changed
- Memory Utilization
- MLPPP Bundle
- MPLS Black Hole Found
- MPLS Interface Removed

- MPLS TE FRR State Changed
- MPLS TE Tunnel Down
- MPLS TP Tunnel Down
- Network-Clock Synchronization
- OSPF Neighbor State Change
- Port Down
- Power Supply Down
- Pluggable Transceiver Out
- REP Port Role Change
- Rx Dormant
- Rx Utilization
- Shelf Out
- SONET Path Link Down
- SONET Path Port Down
- Subinterface Down
- Tx Dormant
- Tx Utilization
- VSI Down

Adaptive Polling

Table 15-81 VNE Switched to Low Polling Rate Due to CPU High Usage

Service Alarm Setting	Registry Parameter
Type	Adaptive Polling
Subtype	high polling interval
Correlation information	activate-flow=false
	correlate=true
	is-correlation-allowed=false
	weight=0
Northbound metadata	alarm-type=124
	auto-cleared=false
	auto-removed=true
	functionality-type=SERVICE
	severity=MAJOR
	is-ticketable=true
	send-to-gw=true
	short-description=VNE switched to low polling rate due to CPU high usage

Table 15-82 VNE Switched to a Limited Investigation Mode Due to High CPU Usage

Service Alarm Setting	Registry Parameter
Type	Adaptive polling
Subtype	maintenance
Correlation information	activate-flow=false
	correlate=true
	is-correlation-allowed=false
	weight=0
Northbound metadata	alarm-type=124
	auto-cleared=false
	auto-removed=true
	functionality-type=SERVICE
	severity=CRITICAL
	is-ticketable=true
	send-to-gw=true
	short-description=VNE switched to a limited investigation mode due to high CPU usage

Table 15-83 VNE Switched Back to Regular Polling Rate

Service Alarm Setting	Registry Parameter
Type	Adaptive polling
Subtype	regular polling interval
Correlation information	activate-flow=false
	correlate=false
	is-correlation-allowed=false
	weight=0
Northbound metadata	alarm-type=124
	auto-cleared=false
	auto-removed=true
	functionality-type=SERVICE
	severity=CLEARED
	is-ticketable=false
	send-to-gw=true
	short-description=VNE switched back to regular polling rate

All IP Interfaces Down

Table 15-84 Active IP Interfaces Found

Event Setting	Registry Parameter
Type	all ip interfaces down
Subtype	active ip interfaces found
Correlation information	activate-flow=false
	correlate=false
	is-correlation-allowed=false
	weight=0
Northbound metadata	alarm-type=837
	auto-cleared=false
	auto-removed=true
	functionality-type=SERVICE
	severity=CLEARED
	is-ticketable=false
	send-to-gw=true
	short-description=Active ip interfaces found
Flapping information	clear-interval=240000
	flapping-interval=60000
	flapping-threshold=5
	update-interval=200000
	update-threshold=20

Table 15-85 All IP Interfaces Down

Event Setting	Registry Parameter
Type	all ip interfaces down
Subtype	all ip interfaces down
Correlation information	activate-flow=false
	correlate=true
	is-correlation-allowed=true
	weight=750

Table 15-85 All IP Interfaces Down (continued)

Event Setting	Registry Parameter
Northbound metadata	alarm-type=837
	auto-cleared=false
	auto-removed=true
	functionality-type=SERVICE
	severity=MAJOR
	is-ticketable=true
	send-to-gw=true
	short-description=All ip interfaces down
Flapping information	clear-interval=240000
	flapping-interval=60000
	flapping-threshold=5
	update-interval=200000
	update-threshold=20

ATM IMA Down

Table 15-86 IMA Admin Down

Event Setting	Registry Parameter
Type	ima down
Subtype	ima admin down
Correlation information	activate-flow=false
	correlate=false
	is-correlation-allowed=true
	weight=110000

Table 15-86 IMA Admin Down (continued)

Event Setting	Registry Parameter
Northbound metadata	alarm-type=681
	auto-cleared=false
	auto-removed=true
	auto-removed-timeout=5000000
	duplication-counter=1
	functionality-type=SERVICE
	is-ticketable=true
	priority=0
	reduction-counter=1
	send-to-gw=true
	severity=CRITICAL
	short-description=ima administratively down

Table 15-87 IMA Oper Down

Event Setting	Registry Parameter
Type	ima down
Subtype	ima oper down
Correlation information	activate-flow=false
	correlate=false
	is-correlation-allowed=false
	weight=800
Northbound metadata	alarm-type=680
	auto-cleared=false
	auto-removed=true
	auto-removed-timeout=5000000
	duplication-counter=1
	functionality-type=SERVICE
	is-ticketable=true
	priority=0
	reduction-counter=1
	send-to-gw=true
	severity=MAJOR
	short-description=ima operationally down

Table 15-88 High Priority IMA Down

Event Setting	Registry Parameter
Type	ima down
Subtype	high priority ima down
Correlation information	activate-flow=false
	correlate=false
	is-correlation-allowed=false
	weight=800
Northbound metadata	alarm-type=680
	auto-cleared=false
	auto-removed=true
	auto-removed-timeout=5000000
	duplication-counter=1
	functionality-type=SERVICE
	is-ticketable=true
	priority=0
	reduction-counter=1
	send-to-gw=true
	severity=CRITICAL
	short-description=high priority ima down

Table 15-89 Medium Priority IMA Down

Event Setting	Registry Parameter
Type	ima down
Subtype	medium priority ima down
Correlation information	activate-flow=false
	correlate=false
	is-correlation-allowed=false
	weight=800

Table 15-89 Medium Priority IMA Down (continued)

Event Setting	Registry Parameter
Northbound metadata	alarm-type=680
	auto-cleared=false
	auto-removed=true
	auto-removed-timeout=5000000
	duplication-counter=1
	functionality-type=SERVICE
	is-ticketable=true
	priority=0
	reduction-counter=1
	send-to-gw=true
	severity=MAJOR
	short-description=medium priority ima down

Table 15-90 Low Priority IMA Down

Event Setting	Registry Parameter
Type	ima down
Subtype	low priority ima down
Correlation information	activate-flow=false
	correlate=false
	is-correlation-allowed=false
	weight=800
Northbound metadata	alarm-type=680
	auto-cleared=false
	auto-removed=true
	auto-removed-timeout=5000000
	duplication-counter=1
	functionality-type=SERVICE
	is-ticketable=true
	priority=0
	reduction-counter=1
	send-to-gw=true
	severity=MINOR
	short-description=low priority ima down

BFD Connectivity Down

Table 15-91 BFD Connectivity Down

Event Setting	Registry Parameter
Type	BFD connectivity down
Subtype	BFD connectivity down
Correlation information	activate-flow=true
	correlate=true
	is-correlation-allowed=true
	weight=840
Northbound metadata	alarm-type=1222
	auto-cleared=false
	auto-removed=true
	functionality-type=SERVICE
	severity=MAJOR
	is-ticketable=true
	send-to-gw=true
	short-description=BFD connectivity down

Table 15-92 BFD Connectivity Up

Event Setting	Registry Parameter
Type	BFD connectivity down
Subtype	BFD connectivity up
Correlation information	activate-flow=false
	correlate=false
	is-correlation-allowed=false
	weight=0
Northbound metadata	alarm-type=1222
	auto-cleared=false
	auto-removed=true
	functionality-type=SERVICE
	severity=CLEARED
	is-ticketable=false
	send-to-gw=true
	short-description=BFD connectivity up

BFD Neighbor Loss

Table 15-93 BFD Neighbor Loss

Event Setting	Registry Parameter
Type	BFD neighbor loss
Subtype	BFD neighbor loss
Correlation information	activate-flow=true
	correlate=true
	is-correlation-allowed=true
	weight=840
Northbound metadata	alarm-type=1234
	auto-cleared=false
	auto-removed=true
	functionality-type=SERVICE
	severity=MAJOR
	is-ticketable=true
	send-to-gw=true
	short-description=BFD neighbor loss

Table 15-94 BFD Neighbor Found

Event Setting	Registry Parameter
Type	BFD neighbor loss
Subtype	BFD neighbor found
Correlation information	activate-flow=false
	correlate=false
	is-correlation-allowed=false
	weight=0
Northbound metadata	alarm-type=1234
	auto-cleared=false
	auto-removed=true
	functionality-type=SERVICE
	severity=CLEARED
	is-ticketable=false
	send-to-gw=true
	short-description=BFD neighbor found

BGP Link Down

Table 15-95 BGP Link Down Due to Admin Down

Event Setting	Registry Parameter
Type	BGP link down
Subtype	BGP link down due to admin
Correlation information	activate-flow=false
	correlate=false
	is-correlation-allowed=true
	weight=0
Northbound metadata	alarm-type=1221
	auto-cleared=false
	auto-removed=true
	functionality-type=SERVICE
	severity=MINOR
	is-ticketable=true
	send-to-gw=true
	short-description=BGP link down due to admin

Table 15-96 BGP Link Down Due to Oper

Event Setting	Registry Parameter
Type	BGP link down
Subtype	BGP link down due to oper
Correlation information	activate-flow=true
	correlate=true
	is-correlation-allowed=true
	weight=599
Northbound metadata	alarm-type=1221
	auto-cleared=false
	auto-removed=true
	functionality-type=SERVICE
	severity=MAJOR
	is-ticketable=true
	send-to-gw=true
	short-description=BGP link down due to oper

Table 15-97 BGP Link Down VRF Due to Admin

Event Setting	Registry Parameter
Type	BGP link down
Subtype	BGP link down vrf due to admin
Correlation information	activate-flow=false
	correlate=false
	is-correlation-allowed=true
	weight=0
Northbound metadata	alarm-type=1221
	auto-cleared=false
	auto-removed=true
	functionality-type=SERVICE
	severity=MINOR
	is-ticketable=true
	send-to-gw=true
	short-description=BGP link down vrf due to admin

Table 15-98 BGP Link Down VRF Due to Oper

Event Setting	Registry Parameter
Type	BGP link down
Subtype	BGP link down vrf due to oper
Correlation information	activate-flow=true
	correlate=true
	is-correlation-allowed=true
	weight=400
Northbound metadata	alarm-type=1221
	auto-cleared=false
	auto-removed=true
	functionality-type=SERVICE
	severity=MAJOR
	is-ticketable=true
	send-to-gw=true
	short-description=BGP link down vrf due to oper

Table 15-99 BGP Link Up

Event Setting	Registry Parameter
Type	BGP link down
Subtype	BGP link up
Correlation information	activate-flow=false
	correlate=false
	is-correlation-allowed=false
	weight=0
Northbound metadata	alarm-type=1221
	auto-cleared=false
	auto-removed=true
	functionality-type=SERVICE
	severity=CLEARED
	is-ticketable=false
	send-to-gw=true
	short-description=BGP link up

BGP Neighbor Loss

Table 15-100 BGP Neighbor Found

Event Setting	Registry Parameter
Type	BGP neighbor loss
Subtype	BGP neighbor found
Correlation information	activate-flow=false
	correlate=false
	is-correlation-allowed=false
	weight=0
Northbound metadata	alarm-type=127
	auto-cleared=false
	auto-removed=true
	functionality-type=SERVICE
	severity=CLEARED
	is-ticketable=false
	send-to-gw=true
	short-description=BGP neighbor found

Table 15-101 BGP Neighbor Loss Due to Admin

Event Setting	Registry Parameter
Type	BGP neighbor loss
Subtype	BGP neighbor loss due to admin
Correlation information	activate-flow=false
	correlate=false
	is-correlation-allowed=true
	weight=0
Northbound metadata	alarm-type=127
	auto-cleared=false
	auto-removed=true
	functionality-type=SERVICE
	severity=MINOR
	is-ticketable=true
	send-to-gw=true
	short-description=BGP neighbor loss due to admin

Table 15-102 BGP Neighbor Loss Due to Oper

Event Setting	Registry Parameter
Type	BGP neighbor loss
Subtype	BGP neighbor loss due to oper
Correlation information	activate-flow=true
	correlate=true
	is-correlation-allowed=true
	weight=601
Northbound metadata	alarm-type=127
	auto-cleared=false
	auto-removed=true
	functionality-type=SERVICE
	severity=MAJOR
	is-ticketable=true
	send-to-gw=true
	short-description=BGP neighbor loss due to oper

Table 15-103 BGP Neighbor Loss VRF Due to Admin

Event Setting	Registry Parameter
Type	BGP neighbor loss
Subtype	bgp-neighbor-loss-vrf due to admin
Correlation information	activate-flow=flase
	correlate=false
	is-correlation-allowed=true
	weight=0
Northbound metadata	alarm-type=127
	auto-cleared=false
	auto-removed=true
	functionality-type=SERVICE
	severity=MINOR
	is-ticketable=true
	send-to-gw=true
	short-description=BGP neighbor loss vrf due to admin

Table 15-104 BGP Neighbor Loss VRF Due to Oper

Event Setting	Registry Parameter
Type	BGP neighbor loss
Subtype	bgp-neighbor-loss-vrf
Correlation information	activate-flow=true
	correlate=true
	is-correlation-allowed=true
	weight=400
Northbound metadata	alarm-type=127
	auto-cleared=false
	auto-removed=true
	functionality-type=SERVICE
	severity=MAJOR
	is-ticketable=true
	send-to-gw=true
	short-description=BGP neighbor loss vrf due to oper

BGP Process Down

Table 15-105 BGP Process Down

Event Setting	Registry Parameter
Type	bgp-process-down
Subtype	bgp-process-down
Correlation information	activate-flow=false
	correlate=false
	is-correlation-allowed=true
	weight=850
Northbound metadata	alarm-type=1501
	auto-cleared=false
	auto-removed=true
	functionality-type=SERVICE
	severity=CRITICAL
	is-ticketable=true
	send-to-gw=true
	short-description=BGP process down

Table 15-106 BGP Process Up

Event Setting	Registry Parameter
Type	bgp-process-down
Subtype	bgp-process-up
Correlation information	activate-flow=false
	correlate=false
	is-correlation-allowed=false
	weight=0
Northbound metadata	alarm-type=1501
	auto-cleared=false
	auto-removed=true
	functionality-type=SERVICE
	severity=CLEARED
	is-ticketable=false
	send-to-gw=true
	short-description=BGP process up

Broken LSP Discovered

Table 15-107 Broken LSP Discovered

Event Setting	Registry Parameter
Type	Broken LSP discovered
Subtype	Broken LSP discovered
Correlation information	activate-flow=false
	correlate=true
	is-correlation-allowed=false
	weight=0
Northbound metadata	alarm-type=129
	auto-cleared=true
	auto-removed=true
	functionality-type=SERVICE
	severity=MAJOR
	is-ticketable=true
	send-to-gw=true
	short-description=Broken LSP discovered

Card Down

Table 15-108 Card Down

Event Setting	Registry Parameter
Type	card down
Subtype	card down
Correlation information	activate-flow=false
	correlate=false
	is-correlation-allowed=true
	weight=100000
Northbound metadata	alarm-type=11
	auto-cleared=false
	auto-removed=true
	functionality-type=SERVICE
	severity=MAJOR
	is-ticketable=true
	send-to-gw=true
	short-description=Card down

Table 15-109 Card Up

Event Setting	Registry Parameter
Type	card down
Subtype	card up
Correlation information	activate-flow=false
	correlate=false
	is-correlation-allowed=false
	weight=0
Northbound metadata	alarm-type=11
	auto-cleared=false
	auto-removed=true
	functionality-type=SERVICE
	severity=CLEARED
	is-ticketable=false
	send-to-gw=true
	short-description=Card up

Card Out

Table 15-110 Card In

Event Setting	Registry Parameter
Type	card out
Subtype	card in
Correlation information	activate-flow=false
	correlate=false
	is-correlation-allowed=false
	weight=0
Northbound metadata	alarm-type=3
	auto-cleared=false
	auto-removed=true
	functionality-type=SERVICE
	severity=CLEARED
	is-ticketable=false
	send-to-gw=true
	short-description=Card in

Table 15-111 Card Out

Event Setting	Registry Parameter
Type	card out
Subtype	card out
Correlation information	activate-flow=false
	correlate=false
	is-correlation-allowed=true
	weight=100000
Northbound metadata	alarm-type=3
	auto-cleared=false
	auto-removed=true
	functionality-type=SERVICE
	severity=MAJOR
	is-ticketable=true
	send-to-gw=true
	short-description=Card out

Table 15-112 Subcard Out

Event Setting	Registry Parameter
Type	card out
Subtype	subcard out
Correlation information	activate-flow=false
	correlate=true
	is-correlation-allowed=true
	weight=1000
Northbound metadata	alarm-type=3
	auto-cleared=false
	auto-removed=true
	functionality-type=SERVICE
	severity=MAJOR
	is-ticketable=true
	send-to-gw=true
	short-description=Card out

Carrier Grade NAT Translations Create Rate

Table 15-113 Carrier Grade NAT Translations Create Rate Higher Threshold Exceeded

Event Setting	Registry Parameter
Type	cgn statistics translationsCreate
Subtype	cgn statistics translationsCreate higher threshold exceeded
Correlation information	activate-flow=false
	correlate=false
	is-correlation-allowed=false
	weight=0
Northbound metadata	alarm-type=5001
	auto-cleared=false
	auto-removed=true
	functionality-type=SERVICE
	severity=MAJOR
	gw-correlation-timeout=1200000
	is-ticketable=true
	send-to-gw=true
	short-description=cgn statistics translationsCreate higher threshold exceeded

Table 15-114 Carrier Grade NAT Translations Create Rate Lower Threshold Exceeded

Event Setting	Registry Parameter
Type	cgn statistics translationsCreate
Subtype	cgn statistics translationsCreate lower threshold exceeded
Correlation information	activate-flow=false
	correlate=false
	is-correlation-allowed=false
	weight=0
Northbound metadata	alarm-type=5001
	auto-cleared=false
	auto-removed=true
	functionality-type=SERVICE
	severity=MINOR
	is-ticketable=true
	send-to-gw=true
	short-description=cgn statistics translationsCreate lower threshold exceeded

Table 15-115 Carrier Grade NAT Translations Create Rate Threshold Normal

Event Setting	Registry Parameter
Type	cgn statistics translationsCreate
Subtype	cgn statistics translationsCreate threshold normal
Correlation information	activate-flow=false
	correlate=false
	is-correlation-allowed=false
	weight=0
Northbound metadata	alarm-type=5001
	auto-cleared=false
	auto-removed=true
	functionality-type=SERVICE
	severity=CLEARED
	is-ticketable=false
	send-to-gw=true
	short-description=cgn statistics translationsCreate threshold normal

Carrier Grade NAT Translations Delete Rate

Table 15-116 Carrier Grade NAT Translations Delete Rate Higher Threshold Exceeded

Event Setting	Registry Parameter
Type	cgn statistics translationsDelete
Subtype	cgn statistics translationsDelete higher threshold exceeded
Correlation information	activate-flow=false
	correlate=false
	is-correlation-allowed=false
	weight=0
Northbound metadata	alarm-type=5002
	auto-cleared=false
	auto-removed=true
	functionality-type=SERVICE
	severity=MAJOR
	is-ticketable=true
	send-to-gw=true
	short-description=cgn statistics translationsDelete higher threshold exceeded

Table 15-117 Carrier Grade NAT Translations Delete Rate Lower Threshold Exceeded

Event Setting	Registry Parameter
Type	cgn statistics translationsDelete
Subtype	cgn statistics translationsDelete lower threshold exceeded
Correlation information	activate-flow=false
	correlate=false
	is-correlation-allowed=false
	weight=0
Northbound metadata	alarm-type=5002
	auto-cleared=false
	auto-removed=true
	functionality-type=SERVICE
	severity=MINOR
	is-ticketable=true
	send-to-gw=true
	short-description=cgn statistics translationsDelete lower threshold exceeded

Table 15-118 Carrier Grade NAT Translations Delete Rate Threshold Normal

Event Setting	Registry Parameter
Type	cgn statistics translationsDelete
Subtype	cgn statistics translationsDelete threshold normal
Correlation information	activate-flow=false
	correlate=false
	is-correlation-allowed=false
	weight=0
Northbound metadata	alarm-type=5002
	auto-cleared=false
	auto-removed=true
	functionality-type=SERVICE
	severity=CLEARED
	is-ticketable=false
	send-to-gw=true
	short-description=cgn statistics translationsDelete threshold normal

Carrier Grade NAT Inside-to-Outside Forward Rate

Table 15-119 Carrier Grade NAT Inside-to-Outside Forward Rate Higher Threshold Exceeded

Event Setting	Registry Parameter
Type	cgn statistics fwdIn2Out
Subtype	cgn statistics fwdIn2Out higher threshold exceeded
Correlation information	activate-flow=false
	correlate=false
	is-correlation-allowed=false
	weight=0
Northbound metadata	alarm-type=5003
	auto-cleared=false
	auto-removed=true
	functionality-type=SERVICE
	severity=MAJOR
	is-ticketable=true
	send-to-gw=true
	short-description=cgn statistics fwdIn2Out higher threshold exceeded

Table 15-120 Carrier Grade NAT Inside-to-Outside Forward Rate Lower Threshold Exceeded

Event Setting	Registry Parameter
Type	cgn statistics fwdIn2Out
Subtype	cgn statistics fwdIn2Out lower threshold exceeded
Correlation information	activate-flow=false
	correlate=false
	is-correlation-allowed=false
	weight=0
Northbound metadata	alarm-type=5003
	auto-cleared=false
	auto-removed=true
	functionality-type=SERVICE
	severity=MINOR
	is-ticketable=true
	send-to-gw=true
	short-description=cgn statistics fwdIn2Out lower threshold exceeded

Table 15-121 Carrier Grade NAT Inside-to-Outside Forward Rate Threshold Normal

Event Setting	Registry Parameter
Type	cgn statistics fwdIn2Out
Subtype	cgn statistics fwdIn2Out threshold normal
Correlation information	activate-flow=false
	correlate=false
	is-correlation-allowed=false
	weight=0
Northbound metadata	alarm-type=5003
	auto-cleared=false
	auto-removed=true
	functionality-type=SERVICE
	severity=CLEARED
	is-ticketable=false
	send-to-gw=true
	short-description=cgn statistics fwdIn2Out threshold normal

Carrier Grade NAT Outside-to-Inside Forward Rate

Table 15-122 Carrier Grade NAT Outside-to-Inside Forward Rate Higher Threshold Exceeded

Event Setting	Registry Parameter
Type	cgn statistics fwdOut2In
Subtype	cgn statistics fwdOut2In higher threshold exceeded
Correlation information	activate-flow=false
	correlate=false
	is-correlation-allowed=false
	weight=0
Northbound metadata	alarm-type=5004
	auto-cleared=false
	auto-removed=true
	functionality-type=SERVICE
	severity=MAJOR
	is-ticketable=true
	send-to-gw=true
	short-description=cgn statistics fwdOut2In higher threshold exceeded

Table 15-123 Carrier Grade NAT Outside-to-Inside Forward Rate Lower Threshold Exceeded

Event Setting	Registry Parameter
Type	cgn statistics fwdOut2In
Subtype	cgn statistics fwdOut2In lower threshold exceeded
Correlation information	activate-flow=false
	correlate=false
	is-correlation-allowed=false
	weight=0
Northbound metadata	alarm-type=5004
	auto-cleared=false
	auto-removed=true
	functionality-type=SERVICE
	severity=MINOR
	is-ticketable=true
	send-to-gw=true
	short-description=cgn statistics fwdOut2In lower threshold exceeded

Table 15-124 Carrier Grade NAT Outside-to-Inside Forward Rate Threshold Normal

Event Setting	Registry Parameter
Type	cgn statistics fwdOut2In
Subtype	cgn statistics fwdOut2In threshold normal
Correlation information	activate-flow=false
	correlate=false
	is-correlation-allowed=false
	weight=0
Northbound metadata	alarm-type=5004
	auto-cleared=false
	auto-removed=true
	functionality-type=SERVICE
	severity=CLEARED
	is-ticketable=false
	send-to-gw=true
	short-description=cgn statistics fwdOut2In threshold normal

Carrier Grade NAT Inside-to-Outside Drops Port Limit Exceeded

Table 15-125 Carrier Grade NAT Inside-to-Outside Drops Port Limit Higher Threshold Exceeded

Event Setting	Registry Parameter
Type	cgn statistics dropsPortLimitIn2Out
Subtype	cgn statistics dropsPortLimitIn2Out Limit higher threshold exceeded
Correlation information	activate-flow=false
	correlate=false
	is-correlation-allowed=false
	weight=0
Northbound metadata	alarm-type=5005
	auto-cleared=false
	auto-removed=true
	functionality-type=SERVICE
	severity=MAJOR
	is-ticketable=true
	send-to-gw=true
	short-description=cgn statistics dropsPortLimitIn2Out Limit higher threshold exceeded

Table 15-126 Carrier Grade NAT Inside-to-Outside Drops Port Limit Lower Threshold Exceeded

Event Setting	Registry Parameter
Type	cgn statistics dropsPortLimitIn2Out
Subtype	cgn statistics dropsPortLimitIn2Out lower threshold exceeded
Correlation information	activate-flow=false
	correlate=false
	is-correlation-allowed=false
	weight=0
Northbound metadata	alarm-type=5005
	auto-cleared=false
	auto-removed=true
	functionality-type=SERVICE
	severity=MINOR
	is-ticketable=true
	send-to-gw=true
	short-description=cgn statistics dropsPortLimitIn2Out lower threshold exceeded

Table 15-127 Carrier Grade NAT Inside-to-Outside Drops Port Limit Threshold Normal

Event Setting	Registry Parameter
Type	cgn statistics dropsPortLimitIn2Out
Subtype	cgn statistics dropsPortLimitIn2Out threshold normal
Correlation information	activate-flow=false
	correlate=false
	is-correlation-allowed=false
	weight=0
Northbound metadata	alarm-type=5005
	auto-cleared=false
	auto-removed=true
	functionality-type=SERVICE
	severity=CLEARED
	is-ticketable=false
	send-to-gw=true
	short-description=cgn statistics dropsPortLimitIn2Out threshold normal

Carrier Grade NAT Inside-to-Outside Drops System Limit Reached

Table 15-128 Carrier Grade NAT Inside-to-Outside Drops System Limit Reached Higher Threshold Exceeded

Event Setting	Registry Parameter
Type	cgn statistics dropsSystemLimitIn2Out
Subtype	cgn statistics dropsSystemLimitIn2Out higher threshold exceeded
Correlation information	activate-flow=false
	correlate=false
	is-correlation-allowed=false
	weight=0
Northbound metadata	alarm-type=5006
	auto-cleared=false
	auto-removed=true
	functionality-type=SERVICE
	severity=MAJOR
	is-ticketable=true
	send-to-gw=true
	short-description=cgn statistics dropsSystemLimitIn2Out higher threshold exceeded

Table 15-129 Carrier Grade NAT Inside-to-Outside Drops System Limit Reached Lower Threshold Exceeded

Event Setting	Registry Parameter
Type	cgn statistics dropsSystemLimitIn2Out
Subtype	cgn statistics dropsSystemLimitIn2Out lower threshold exceeded
Correlation information	activate-flow=false
	correlate=false
	is-correlation-allowed=false
	weight=0
Northbound metadata	alarm-type=5006
	auto-cleared=false
	auto-removed=true
	functionality-type=SERVICE
	severity=MINOR
	is-ticketable=true
	send-to-gw=true
	short-description=cgn statistics dropsSystemLimitIn2Out lower threshold exceeded

Table 15-130 Carrier Grade NAT Inside-to-Outside Drops System Limit Reached Threshold Normal

Event Setting	Registry Parameter
Type	cgn statistics dropsSystemLimitIn2Out
Subtype	cgn statistics dropsSystemLimitIn2Out threshold normal
Correlation information	activate-flow=false
	correlate=false
	is-correlation-allowed=false
	weight=0
Northbound metadata	alarm-type=5006
	auto-cleared=false
	auto-removed=true
	functionality-type=SERVICE
	severity=CLEARED
	is-ticketable=false
	send-to-gw=true
	short-description=cgn statistics dropsSystemLimitIn2Out threshold normal

Carrier Grade NAT Inside-to-Outside Drops Resource Depletion

Table 15-131 Carrier Grade NAT Inside-to-Outside Drops Resource Depletion Higher Threshold Exceeded

Event Setting	Registry Parameter
Type	cgn statistics dropsResourceDepletionIn2Out
Subtype	cgn statistics dropsResourceDepletionIn2Out higher threshold exceeded
Correlation information	activate-flow=false
	correlate=false
	is-correlation-allowed=false
	weight=0
Northbound metadata	alarm-type=5007
	auto-cleared=false
	auto-removed=true
	functionality-type=SERVICE
	severity=MAJOR
	is-ticketable=true
	send-to-gw=true
	short-description=cgn statistics dropsResourceDepletionIn2Out higher threshold exceeded

Table 15-132 Carrier Grade NAT Inside-to-Outside Drops Resource Depletion Lower Threshold Exceeded

Event Setting	Registry Parameter
Type	cgn statistics dropsResourceDepletionIn2Out
Subtype	cgn statistics dropsResourceDepletionIn2Out lower threshold exceeded
Correlation information	activate-flow=false
	correlate=false
	is-correlation-allowed=false
	weight=0

Table 15-132 Carrier Grade NAT Inside-to-Outside Drops Resource Depletion Lower Threshold Exceeded (continued)

Event Setting	Registry Parameter
Northbound metadata	alarm-type=5007
	auto-cleared=false
	auto-removed=true
	functionality-type=SERVICE
	severity=MINOR
	is-ticketable=true
	send-to-gw=true
	short-description=cgn statistics dropsResourceDepletionIn2Out lower threshold exceeded

Table 15-133 Carrier Grade NAT Inside-to-Outside Drops Resource Depletion Threshold Normal

Event Setting	Registry Parameter
Type	cgn statistics dropsResourceDepletionIn2Out
Subtype	cgn statistics dropsResourceDepletionIn2Out threshold normal
Correlation information	activate-flow=false
	correlate=false
	is-correlation-allowed=false
	weight=0
Northbound metadata	alarm-type=5007
	auto-cleared=false
	auto-removed=true
	functionality-type=SERVICE
	severity=CLEARED
	is-ticketable=false
	send-to-gw=true
	short-description=cgn statistics dropsResourceDepletionIn2Out threshold normal

CFM Domain Fault

Table 15-134 CFM Domain Aggregation Down

Event Setting	Registry Parameter
Type	CFM Domain Fault
Subtype	CFM Domain Aggregation Down

Table 15-134 CFM Domain Aggregation Down (continued)

Event Setting	Registry Parameter
Correlation information	activate-flow=false
	correlate=false
	is-correlation-allowed=true
	weight=2
Northbound metadata	alarm-type=3016
	auto-cleared=false
	auto-removed=true
	auto-removed-timeout=5000000
	duplication-counter=1
	functionality-type=SERVICE
	is-ticketable=true
	priority=0
	reduction-counter=1
	send-to-gw=true
	severity=INFO
	short-description=CFM Domain fault

Table 15-135 CFM Domain Aggregation Up

Event Setting	Registry Parameter
Type	CFM Domain Fault
Subtype	CFM Domain Aggregation Up
Correlation information	activate-flow=false
	correlate=false
	is-correlation-allowed=false
	weight=0

Table 15-135 CFM Domain Aggregation Up (continued)

Event Setting	Registry Parameter
Northbound metadata	alarm-type=3016
	auto-cleared=false
	auto-removed=true
	auto-removed-timeout=5000000
	duplication-counter=1
	functionality-type=SERVICE
	is-ticketable=false
	priority=0
	reduction-counter=1
	send-to-gw=true
	severity=CLEARED
	short-description=CFM Domain fault cleared

Chassis Disconnected

Table 15-136 Chassis Disconnected

Event Setting	Registry Parameter
Type	Chassis Disconnected
Subtype	Chassis Disconnected
Correlation information	activate-flow=false
	correlate=false
	is-correlation-allowed=true
	weight=100000
Northbound metadata	alarm-type=3
	auto-cleared=false
	auto-removed=true
	functionality-type=SERVICE
	severity=MAJOR
	is-ticketable=true
	send-to-gw=true
	short-description=Chassis disconnected

Table 15-137 Card Out due to Chassis Disconnected

Event Setting	Registry Parameter
Type	Chassis Disconnected
Subtype	Card Out due to Chassis Disconnected
Correlation information	activate-flow=false
	correlate=true
	is-correlation-allowed=true
	weight=100000
Northbound metadata	alarm-type=3
	auto-cleared=false
	auto-removed=true
	functionality-type=SERVICE
	severity=MAJOR
	is-ticketable=true
	send-to-gw=true
	short-description=Card out due to chassis disconnected

Table 15-138 Chassis Connected

Event Setting	Registry Parameter
Type	Chassis Disconnected
Subtype	Chassis Connected
Correlation information	activate-flow=false
	correlate=false
	is-correlation-allowed=false
	weight=0
Northbound metadata	alarm-type=3
	auto-cleared=false
	auto-removed=true
	functionality-type=SERVICE
	severity=CLEARED
	is-ticketable=false
	send-to-gw=true
	short-description=Chassis connected

Cloud Problem

Table 15-139 Cloud Problem

Event Setting	Registry Parameter
Type	cloud problem
Subtype	cloud problem
Correlation information	activate-flow=false
	correlate=false
	is-correlation-allowed=true
	weight=2000
Northbound metadata	alarm-type=122
	auto-cleared=false
	auto-removed=true
	functionality-type=SERVICE
	severity=INFO
	is-ticketable=true
	send-to-gw=true
	short-description=cloud problem

Table 15-140 Cloud Problem Fixed

Event Setting	Registry Parameter
Type	cloud problem
Subtype	cloud up
Correlation information	activate-flow=false
	correlate=false
	is-correlation-allowed=false
	weight=0
Northbound metadata	alarm-type=122
	auto-cleared=false
	auto-removed=true
	functionality-type=SERVICE
	severity=CLEARED
	is-ticketable=false
	send-to-gw=true
	short-description=cloud problem fixed

Component Unreachable

Table 15-141 Component Reachable

Event Setting	Registry Parameter
Type	component unreachable
Subtype	component reachable
Correlation information	activate-flow=false
	correlate=false
	is-correlation-allowed=false
	weight=0
Northbound metadata	alarm-type=5
	auto-cleared=false
	auto-removed=true
	functionality-type=SERVICE
	severity=CLEARED
	is-ticketable=false
	send-to-gw=true
	short-description=Device Reachable

Table 15-142 Component Unreachable

Event Setting	Registry Parameter
Type	component unreachable
Subtype	component unreachable
Correlation information	activate-flow=true
	correlate=true
	is-correlation-allowed=true
	weight=600
Northbound metadata	alarm-type=5
	auto-cleared=false
	auto-removed=true
	functionality-type=SERVICE
	severity=MAJOR
	is-ticketable=true
	send-to-gw=true
	short-description=Device Unreachable

Table 15-143 Device Partially Managed

Event Setting	Registry Parameter
Type	component unreachable
Subtype	device partially managed
Correlation information	activate-flow=false
	correlate=false
	is-correlation-allowed=false
	weight=0
Northbound metadata	alarm-type=5
	auto-cleared=false
	auto-removed=true
	functionality-type=SERVICE
	severity=WARNING
	is-ticketable=true
	send-to-gw=true
	short-description=Device reachable

CPU Utilization

Table 15-144 CPU Normal Utilization

Event Setting	Registry Parameter
Type	cpu utilization
Subtype	cpu normal use
Correlation information	activate-flow=false
	correlate=false
	is-correlation-allowed=false
	weight=0
Northbound metadata	alarm-type=17
	auto-cleared=false
	auto-removed=true
	functionality-type=SERVICE
	severity=CLEARED
	is-ticketable=false
	send-to-gw=true
	short-description=CPU utilization less than lower threshold

Table 15-145 CPU Overutilized

Event Setting	Registry Parameter
Type	cpu utilization
Subtype	cpu over utilized
Correlation information	activate-flow=false
	correlate=false
	is-correlation-allowed=false
	weight=0
Northbound metadata	alarm-type=17
	auto-cleared=false
	auto-removed=true
	functionality-type=SERVICE
	severity=MAJOR
	is-ticketable=true
	send-to-gw=true
	short-description=CPU utilization exceeded lower threshold

Device Unsupported

Table 15-146 Device Initializing

Event Setting	Registry Parameter
Type	device unsupported
Subtype	device initializing
Correlation information	activate-flow=false
	correlate=false
	is-correlation-allowed=false
	weight=0
Northbound metadata	alarm-type=16
	auto-cleared=false
	auto-removed=true
	functionality-type=SERVICE
	severity=CRITICAL
	gw-correlation-timeout=1200000
	is-ticketable=false
	send-to-gw=true
	short-description=Device initializing

Table 15-147 Device Unsupported

Event Setting	Registry Parameter
Type	device unsupported
Subtype	device unsupported
Correlation information	activate-flow=false
	correlate=false
	is-correlation-allowed=false
	weight=0
Northbound metadata	alarm-type=16
	auto-cleared=false
	auto-removed=true
	functionality-type=SERVICE
	severity=CRITICAL
	is-ticketable=true
	send-to-gw=true
	short-description=Device unsupported

Discard Packets

Table 15-148 Discard Packets

Event Setting	Registry Parameter
Type	discard packets
Subtype	discard packets
Correlation information	activate-flow=false
	correlate=true
	is-correlation-allowed=false
	weight=0
Northbound metadata	alarm-type=9
	auto-cleared=false
	auto-removed=true
	functionality-type=SERVICE
	severity=MINOR
	is-ticketable=true
	send-to-gw=true
	short-description=Discarded packet rate exceeded upper threshold

Table 15-149 Normal Discard Packets

Event Setting	Registry Parameter
Type	discard packets
Subtype	normal discard packets
Correlation information	activate-flow=false
	correlate=false
	is-correlation-allowed=false
	weight=0
Northbound metadata	alarm-type=9
	auto-cleared=false
	auto-removed=true
	functionality-type=SERVICE
	severity=CLEARED
	is-ticketable=false
	send-to-gw=true
	short-description=Discarded packet rate is below lower threshold

Dropped Packets

Table 15-150 Dropped Packets on Port

Event Setting	Registry Parameter
Type	dropped packets
Subtype	dropped packets
Correlation information	activate-flow=false
	correlate=false
	is-correlation-allowed=false
	weight=0
Northbound metadata	alarm-type=10
	auto-cleared=false
	auto-removed=true
	functionality-type=SERVICE
	severity=MINOR
	is-ticketable=true
	send-to-gw=true
	short-description=Dropped packet rate exceeded upper threshold

Table 15-151 Stopped Dropping Packets on Port

Event Setting	Registry Parameter
Type	dropped packets
Subtype	normal dropped packets
Correlation information	activate-flow=false
	correlate=false
	is-correlation-allowed=false
	weight=0
Northbound metadata	alarm-type=10
	auto-cleared=false
	auto-removed=true
	functionality-type=SERVICE
	severity=CLEARED
	is-ticketable=false
	send-to-gw=true
	short-description=Dropped packet rate is below lower threshold

DS0 Bundle

Table 15-152 DS0 Bundle Admin Down

Event Setting	Registry Parameter
Type	ds0 bundle down
Subtype	ds0 bundle admin down
Correlation information	activate-flow=false
	correlate=false
	is-correlation-allowed=true
	root-cause-timeout=420000
	weight=750

Table 15-152 DS0 Bundle Admin Down (continued)

Event Setting	Registry Parameter
Northbound metadata	alarm-type=660
	auto-cleared=false
	auto-removed=true
	auto-removed-timeout=5000000
	duplication-counter=1
	functionality-type=SERVICE
	is-ticketable=true
	priority=0
	reduction-counter=1
	send-to-gw=true
	severity=MAJOR
	short-description=ds0 bundle admin down

Table 15-153 DS0 Bundle Oper Down

Event Setting	Registry Parameter
Type	ds0 bundle down
Subtype	ds0 bundle oper down
Correlation information	activate-flow=true
	correlate=true
	is-correlation-allowed=true
	root-cause-timeout=420000
	weight=725
Northbound metadata	alarm-type=660
	auto-cleared=false
	auto-removed=true
	auto-removed-timeout=5000000
	duplication-counter=1
	functionality-type=SERVICE
	is-ticketable=true
	priority=0
	reduction-counter=1
	send-to-gw=true
	severity=MAJOR
	short-description=ds0 bundle oper down

Table 15-154 DS0 Bundle Up

Event Setting	Registry Parameter
Type	ds0 bundle down
Subtype	ds0 bundle up
Correlation information	activate-flow=false
	correlate=false
	is-correlation-allowed=false
	root-cause-timeout=420000
	weight=0
Northbound metadata	alarm-type=660
	auto-cleared=false
	auto-removed=true
	auto-removed-timeout=5000000
	duplication-counter=1
	functionality-type=SERVICE
	is-ticketable=false
	priority=0
	reduction-counter=1
	send-to-gw=true
	severity=CLEARED
	short-description=ds0 bundle up

DS1 Path Link Down

Table 15-155 DS1 Path Link Down Due to Admin Down

Event Setting	Registry Parameter
Type	ds1path link down
Subtype	ds1path link down due to admin down
Correlation information	activate-flow=false
	correlate=false
	is-correlation-allowed=true
	root-cause-timeout=420000
	weight=815

Table 15-155 DS1 Path Link Down Due to Admin Down (continued)

Event Setting	Registry Parameter
Northbound metadata	alarm-type=1344
	auto-cleared=false
	auto-removed=true
	auto-removed-timeout=5000000
	duplication-counter=1
	functionality-type=SERVICE
	is-ticketable=true
	priority=0
	reduction-counter=1
	send-to-gw=true
	severity=CRITICAL
	short-description=DS1 Path Link down due to admin down

Table 15-156 DS1 Path Link Down Due to Oper Down

Event Setting	Registry Parameter
Type	ds1path link down
Subtype	ds1path link down due to oper down
Correlation information	activate-flow=true
	correlate=true
	is-correlation-allowed=true
	root-cause-timeout=420000
	weight=810
Northbound metadata	alarm-type=1344
	auto-cleared=false
	auto-removed=true
	auto-removed-timeout=5000000
	duplication-counter=1
	functionality-type=SERVICE
	is-ticketable=true
	priority=0
	reduction-counter=1
	send-to-gw=true
	severity=CRITICAL
	short-description=DS1 Path Link down due to oper down

Table 15-157 DS1 Path Link Down Due to Card

Event Setting	Registry Parameter
Type	ds1path link down
Subtype	ds1path link down due to card
Correlation information	activate-flow=false
	correlate=true
	is-correlation-allowed=true
	root-cause-timeout=420000
	weight=815
Northbound metadata	alarm-type=1344
	auto-cleared=false
	auto-removed=true
	auto-removed-timeout=5000000
	duplication-counter=1
	functionality-type=SERVICE
	is-ticketable=true
	priority=0
	reduction-counter=1
	send-to-gw=true
	severity=CRITICAL
	short-description=DS1 Path Link down due to card event

Table 15-158 DS1 Path Link Down on Unreachable

Event Setting	Registry Parameter
Type	ds1path link down
Subtype	ds1path link down on unreachable
Correlation information	activate-flow=true
	correlate=true
	is-correlation-allowed=true
	root-cause-timeout=420000
	weight=810

Table 15-158 DS1 Path Link Down on Unreachable (continued)

Event Setting	Registry Parameter
Northbound metadata	alarm-type=1344
	auto-cleared=false
	auto-removed=true
	auto-removed-timeout=5000000
	duplication-counter=1
	functionality-type=SERVICE
	is-ticketable=true
	priority=0
	reduction-counter=1
	send-to-gw=true
	severity=CRITICAL
	short-description=DS1 Path Link down on unreachable

Table 15-159 DS1 Path Link Up

Event Setting	Registry Parameter
Type	ds1path link down
Subtype	ds1path link up
Correlation information	activate-flow=false
	correlate=false
	is-correlation-allowed=false
	root-cause-timeout=420000
	weight=0
Northbound metadata	alarm-type=1344
	auto-cleared=false
	auto-removed=true
	auto-removed-timeout=5000000
	duplication-counter=1
	functionality-type=SERVICE
	is-ticketable=false
	priority=0
	reduction-counter=1
	send-to-gw=true
	severity=CLEARED
	short-description=DS1 Path Link up

DS1 Path Port Down

Table 15-160 DS1 Path Port Down Due to Admin

Event Setting	Registry Parameter
Type	ds1path port down
Subtype	ds1path port down due to admin
Correlation information	activate-flow=true
	correlate=true
	is-correlation-allowed=true
	root-cause-timeout=420000
	weight=810
Northbound metadata	alarm-type=1381
	auto-cleared=false
	auto-removed=true
	auto-removed-timeout=5000000
	duplication-counter=1
	functionality-type=SERVICE
	is-ticketable=true
	priority=0
	reduction-counter=1
	send-to-gw=true
	severity=MAJOR
	short-description=DS1 Path down due to Admin

Table 15-161 DS1 Path Port Down Due to Oper

Event Setting	Registry Parameter
Type	ds1path port down
Subtype	ds1path port down due to oper
Correlation information	activate-flow=true
	correlate=true
	is-correlation-allowed=true
	root-cause-timeout=420000
	weight=810

Table 15-161 DS1 Path Port Down Due to Oper (continued)

Event Setting	Registry Parameter
Northbound metadata	alarm-type=1381
	auto-cleared=false
	auto-removed=true
	auto-removed-timeout=5000000
	duplication-counter=1
	functionality-type=SERVICE
	is-ticketable=true
	priority=0
	reduction-counter=1
	send-to-gw=true
	severity=MAJOR
	short-description=DS1 Path down due to Oper

Table 15-162 DS1 Path Port Down Due to Card

Event Setting	Registry Parameter
Type	ds1path port down
Subtype	ds1path port down due to card
Correlation information	activate-flow=false
	correlate=true
	is-correlation-allowed=true
	root-cause-timeout=420000
	weight=815
Northbound metadata	alarm-type=1381
	auto-cleared=false
	auto-removed=true
	auto-removed-timeout=5000000
	duplication-counter=1
	functionality-type=SERVICE
	is-ticketable=true
	priority=0
	reduction-counter=1
	send-to-gw=true
	severity=MAJOR
	short-description=DS1 Path down due to Card

Table 15-163 DS1 Path Port Up

Event Setting	Registry Parameter
Type	ds1path port down
Subtype	ds1path port up
Correlation information	activate-flow=false
	correlate=false
	is-correlation-allowed=false
	root-cause-timeout=420000
	weight=0
Northbound metadata	alarm-type=1381
	auto-cleared=false
	auto-removed=true
	auto-removed-timeout=5000000
	duplication-counter=1
	functionality-type=SERVICE
	is-ticketable=false
	priority=0
	reduction-counter=1
	send-to-gw=true
	severity=CLEARED
	short-description=DS1 Path up

DS3 Path Link Down

Table 15-164 DS3 Path Link Down Due to Admin Down

Event Setting	Registry Parameter
Type	ds3path link down
Subtype	ds3path link admin due to admin down
Correlation information	activate-flow=false
	correlate=false
	is-correlation-allowed=true
	root-cause-timeout=420000
	weight=825

Table 15-164 DS3 Path Link Down Due to Admin Down (continued)

Event Setting	Registry Parameter
Northbound metadata	alarm-type=1356
	auto-cleared=false
	auto-removed=true
	auto-removed-timeout=5000000
	duplication-counter=1
	functionality-type=SERVICE
	is-ticketable=true
	priority=0
	reduction-counter=1
	send-to-gw=true
	severity=CRITICAL
	short-description=DS3 Path Link down due to admin down

Table 15-165 DS3 Path Link Down Due to Oper Down

Event Setting	Registry Parameter
Type	ds3path link down
Subtype	ds3path link down due to oper down
Correlation information	activate-flow=true
	correlate=true
	is-correlation-allowed=true
	root-cause-timeout=420000
	weight=820
Northbound metadata	alarm-type=1356
	auto-cleared=false
	auto-removed=true
	auto-removed-timeout=5000000
	duplication-counter=1
	functionality-type=SERVICE
	is-ticketable=true
	priority=0
	reduction-counter=1
	send-to-gw=true
	severity=CRITICAL
	short-description=DS3 Path Link down due to oper down

Table 15-166 DS3 Path Link Down Due to Card

Event Setting	Registry Parameter
Type	ds3path link down
Subtype	ds3path link down due to card
Correlation information	activate-flow=false
	correlate=true
	is-correlation-allowed=true
	root-cause-timeout=420000
	weight=825
Northbound metadata	alarm-type=1356
	auto-cleared=false
	auto-removed=true
	auto-removed-timeout=5000000
	duplication-counter=1
	functionality-type=SERVICE
	is-ticketable=true
	priority=0
	reduction-counter=1
	send-to-gw=true
	severity=CRITICAL
	short-description=DS3 Path Link down due to Card event

Table 15-167 DS3 Path Link Down on Unreachable

Event Setting	Registry Parameter
Type	ds3path link down
Subtype	ds3path link down on unreachable
Correlation information	activate-flow=true
	correlate=true
	is-correlation-allowed=true
	root-cause-timeout=420000
	weight=820

Table 15-167 DS3 Path Link Down on Unreachable (continued)

Event Setting	Registry Parameter
Northbound metadata	alarm-type=1356
	auto-cleared=false
	auto-removed=true
	auto-removed-timeout=5000000
	duplication-counter=1
	functionality-type=SERVICE
	is-ticketable=true
	priority=0
	reduction-counter=1
	send-to-gw=true
	severity=CRITICAL
	short-description=DS3 Path Link down on unreachable

Table 15-168 DS3 Path Link Up

Event Setting	Registry Parameter
Type	ds3path link down
Subtype	ds3path link up
Correlation information	activate-flow=false
	correlate=false
	is-correlation-allowed=false
	root-cause-timeout=420000
	weight=0
Northbound metadata	alarm-type=1356
	auto-cleared=false
	auto-removed=true
	auto-removed-timeout=5000000
	duplication-counter=1
	functionality-type=SERVICE
	is-ticketable=false
	priority=0
	reduction-counter=1
	send-to-gw=true
	severity=CLEARED
	short-description=DS3 Path Link up

DS3 Path Port Down

Table 15-169 DS3 Path Port Down Due to Admin

Event Setting	Registry Parameter
Type	ds3path port down
Subtype	ds3path port down due to admin
Correlation information	activate-flow=true
	correlate=true
	is-correlation-allowed=true
	root-cause-timeout=420000
	weight=820
Northbound metadata	alarm-type=1357
	auto-cleared=false
	auto-removed=true
	auto-removed-timeout=5000000
	duplication-counter=1
	functionality-type=SERVICE
	is-ticketable=true
	priority=0
	reduction-counter=1
	send-to-gw=true
	severity=MAJOR
	short-description=DS3 path port down due to Admin

Table 15-170 DS3 Path Port Down Due to Oper

Event Setting	Registry Parameter
Type	ds3path port down
Subtype	ds3path port down due to oper
Correlation information	activate-flow=true
	correlate=true
	is-correlation-allowed=true
	root-cause-timeout=420000
	weight=820

Table 15-170 DS3 Path Port Down Due to Oper (continued)

Event Setting	Registry Parameter
Northbound metadata	alarm-type=1357
	auto-cleared=false
	auto-removed=true
	auto-removed-timeout=5000000
	duplication-counter=1
	functionality-type=SERVICE
	is-ticketable=true
	priority=0
	reduction-counter=1
	send-to-gw=true
	severity=MAJOR
	short-description=DS3 Path Down due to Oper

Table 15-171 DS3 Path Port Down Due to Card

Event Setting	Registry Parameter
Type	ds3path port down
Subtype	ds3path port down due to card
Correlation information	activate-flow=false
	correlate=true
	is-correlation-allowed=true
	root-cause-timeout=420000
	weight=825
Northbound metadata	alarm-type=1357
	auto-cleared=false
	auto-removed=true
	auto-removed-timeout=5000000
	duplication-counter=1
	functionality-type=SERVICE
	is-ticketable=true
	priority=0
	reduction-counter=1
	send-to-gw=true
	severity=MAJOR
	short-description=DS3 Path Down due to Card

Table 15-172 DS3 Path Port Up

Event Setting	Registry Parameter
Type	ds3path port down
Subtype	ds3path port up
Correlation information	activate-flow=false
	correlate=false
	is-correlation-allowed=false
	root-cause-timeout=420000
	weight=0
Northbound metadata	alarm-type=1357
	auto-cleared=false
	auto-removed=true
	auto-removed-timeout=5000000
	duplication-counter=1
	functionality-type=SERVICE
	is-ticketable=false
	priority=0
	reduction-counter=1
	send-to-gw=true
	severity=MAJOR
	short-description=DS3 Path up

Dual Stack IP Changed

Table 15-173 Dual Stack IP Removed

Event Setting	Registry Parameter
Type	Dual stack IP Changed
Subtype	Dual stack IP removed
Correlation information	activate-flow=true
	correlate=false
	is-correlation-allowed=false
	root-cause-timeout=420000
	weight=820

Table 15-173 Dual Stack IP Removed (continued)

Event Setting	Registry Parameter
Northbound metadata	alarm-type=1170
	auto-cleared=false
	auto-removed=true
	auto-removed-timeout=5000000
	duplication-counter=1
	functionality-type=SERVICE
	is-ticketable=true
	priority=0
	reduction-counter=1
	send-to-gw=true
	severity=MINOR
	short-description=Dual stack IP removed

Table 15-174 Dual Stack IP Added

Event Setting	Registry Parameter
Type	Dual stack IP Changed
Subtype	Dual stack IP added
Correlation information	activate-flow=false
	correlate=false
	is-correlation-allowed=false
	root-cause-timeout=420000
	weight=0
Northbound metadata	alarm-type=1170
	auto-cleared=false
	auto-removed=true
	auto-removed-timeout=5000000
	duplication-counter=1
	functionality-type=SERVICE
	is-ticketable=false
	priority=0
	reduction-counter=1
	send-to-gw=true
	severity=CLEARED
	short-description=Dual stack IP added

DWDM Controller

Table 15-175 DWDM Controller Down

Event Setting	Registry Parameter
Type	dwdm controller down
Subtype	dwdm controller down
Correlation information	activate-flow=false
	correlate=false
	is-correlation-allowed=false
	root-cause-timeout=420000
	weight=0
Northbound metadata	alarm-type=1888
	auto-cleared=false
	auto-removed=true
	auto-removed-timeout=5000000
	duplication-counter=1
	functionality-type=SERVICE
	is-ticketable=true
	priority=0
	reduction-counter=1
	send-to-gw=true
	severity=MAJOR
	short-description=dwdm controller down

Table 15-176 DWDM Controller Up

Event Setting	Registry Parameter
Type	dwdm controller down
Subtype	dwdm controller up
Correlation information	activate-flow=false
	correlate=false
	is-correlation-allowed=false
	root-cause-timeout=420000
	weight=0

Table 15-176 DWDM Controller Up (continued)

Event Setting	Registry Parameter
Northbound metadata	alarm-type=1888
	auto-cleared=false
	auto-removed=true
	auto-removed-timeout=5000000
	duplication-counter=1
	functionality-type=SERVICE
	is-ticketable=false
	priority=0
	reduction-counter=1
	send-to-gw=true
	severity=CLEARED
	short-description=dwdm controller up

DWDM G709 Status

Table 15-177 DWDM G709 Status Down

Event Setting	Registry Parameter
Type	dwdm g709 status down
Subtype	dwdm g709 status down
Correlation information	activate-flow=false
	correlate=false
	is-correlation-allowed=false
	root-cause-timeout=420000
	weight=0

Table 15-177 DWDM G709 Status Down (continued)

Event Setting	Registry Parameter
Northbound metadata	alarm-type=1889
	auto-cleared=false
	auto-removed=true
	auto-removed-timeout=5000000
	duplication-counter=1
	functionality-type=SERVICE
	is-ticketable=true
	priority=0
	reduction-counter=1
	send-to-gw=true
	severity=MINOR
	short-description=dwdm g709 status down

Table 15-178 DWDM G709 Status Up

Event Setting	Registry Parameter
Type	dwdm g709 status down
Subtype	dwdm g709 status up
Correlation information	activate-flow=false
	correlate=false
	is-correlation-allowed=false
	root-cause-timeout=420000
	weight=0
Northbound metadata	alarm-type=1889
	auto-cleared=false
	auto-removed=true
	auto-removed-timeout=5000000
	duplication-counter=1
	functionality-type=SERVICE
	is-ticketable=false
	priority=0
	reduction-counter=1
	send-to-gw=true
	severity=CLEARED
	short-description=dwdm g709 status up

EFP Down

Table 15-179 EFP Admin Down

Event Setting	Registry Parameter
Type	efp down
Subtype	efp admin down
Correlation information	activate-flow=true
	correlate=true
	is-correlation-allowed=true
	weight=849
Northbound metadata	alarm-type=918
	auto-cleared=false
	auto-removed=true
	functionality-type=SERVICE
	severity=MAJOR
	is-ticketable=true
	send-to-gw=true
	short-description=EFP admin down

Table 15-180 EFP Down Due to Error Disabled

Event Setting	Registry Parameter
Type	efp down
Subtype	efp down due to error disabled
Correlation information	activate-flow=true
	correlate=true
	is-correlation-allowed=true
	weight=849
Northbound metadata	alarm-type=918
	auto-cleared=false
	auto-removed=true
	functionality-type=SERVICE
	severity=MAJOR
	is-ticketable=true
	send-to-gw=true
	short-description=EFP down due to error disabled

Table 15-181 EFP Oper Down

Event Setting	Registry Parameter
Type	efp down
Subtype	efp oper down
Correlation information	activate-flow=true
	correlate=true
	is-correlation-allowed=true
	weight=849
Northbound metadata	alarm-type=918
	auto-cleared=false
	auto-removed=true
	functionality-type=SERVICE
	severity=MAJOR
	is-ticketable=true
	send-to-gw=true
	short-description=EFP oper down

Table 15-182 EFP Up

Event Setting	Registry Parameter
Type	efp down
Subtype	efp up
Correlation information	activate-flow=false
	correlate=false
	is-correlation-allowed=false
	weight=0
Northbound metadata	alarm-type=918
	auto-cleared=false
	auto-removed=true
	functionality-type=SERVICE
	severity=CLEARED
	is-ticketable=false
	send-to-gw=true
	short-description=EFP up

ESMC Process Down

Table 15-183 ESMC Process Down

Event Setting	Registry Parameter
Type	esmc process down
Subtype	esmc process down
Correlation information	activate-flow=false
	correlate=false
	is-correlation-allowed=true
	weight=750
Northbound metadata	alarm-type=690
	auto-cleared=false
	auto-removed=true
	auto-removed-timeout=5000000
	duplication-counter=1
	functionality-type=SERVICE
	is-ticketable=true
	priority=0
	reduction-counter=1
	send-to-gw=true
	severity=MAJOR
	short-description=esmc process down

Table 15-184 ESMC Process Up

Event Setting	Registry Parameter
Type	esmc process up
Subtype	esmc process up
Correlation information	activate-flow=false
	correlate=false
	is-correlation-allowed=false
	weight=0

Table 15-184 ESMC Process Up (continued)

Event Setting	Registry Parameter
Northbound metadata	alarm-type=690
	auto-cleared=false
	auto-removed=true
	auto-removed-timeout=5000000
	duplication-counter=1
	functionality-type=SERVICE
	is-ticketable=false
	priority=0
	reduction-counter=1
	send-to-gw=true
	severity=CLEARED
	short-description=esmc process up

Fan-Tray Down

Table 15-185 Fan-Tray Down

Event Setting	Registry Parameter
Type	fan-tray down
Subtype	fan-tray down
Correlation information	activate-flow=false
	correlate=false
	is-correlation-allowed=true
	weight=0
Northbound metadata	alarm-type=13003
	auto-cleared=false
	auto-removed=true
	auto-removed-timeout=5000000
	duplication-counter=1
	functionality-type=SERVICE
	is-ticketable=true
	priority=0
	reduction-counter=1
	send-to-gw=true
	severity=MAJOR
	short-description=fan-tray down

Table 15-186 Fan-Tray Up

Event Setting	Registry Parameter
Type	fan-tray down
Subtype	fan-tray up
Correlation information	activate-flow=false
	correlate=false
	is-correlation-allowed=false
	weight=0
Northbound metadata	alarm-type=13003
	auto-cleared=false
	auto-removed=true
	auto-removed-timeout=5000000
	duplication-counter=1
	functionality-type=SERVICE
	is-ticketable=false
	priority=0
	reduction-counter=1
	send-to-gw=true
	severity=CLEARED
	short-description=fan-tray up

Fan-Tray Out

Table 15-187 Fan-Tray Out

Event Setting	Registry Parameter
Type	fan-tray out
Subtype	fan-tray out
Correlation information	activate-flow=false
	correlate=false
	is-correlation-allowed=true
	weight=0

Table 15-187 Fan-Tray Out (continued)

Event Setting	Registry Parameter
Northbound metadata	alarm-type=13002
	auto-cleared=false
	auto-removed=true
	auto-removed-timeout=5000000
	duplication-counter=1
	functionality-type=SERVICE
	is-ticketable=true
	priority=0
	reduction-counter=1
	send-to-gw=true
	severity=MAJOR
	short-description=fan-tray out

Table 15-188 Fan-Tray In

Event Setting	Registry Parameter
Type	fan-tray out
Subtype	fan-tray in
Correlation information	activate-flow=false
	correlate=false
	is-correlation-allowed=false
	weight=0
Northbound metadata	alarm-type=13002
	auto-cleared=false
	auto-removed=true
	auto-removed-timeout=5000000
	duplication-counter=1
	functionality-type=SERVICE
	is-ticketable=false
	priority=0
	reduction-counter=1
	send-to-gw=true
	severity=CLEARED
	short-description=fan-tray in

GRE Keepalive

Table 15-189 Keepalive Not Set

Event Setting	Registry Parameter
Type	keepalive set
Subtype	Keepalive not set
Correlation information	activate-flow=false
	correlate=false
	is-correlation-allowed=false
	weight=0
Northbound metadata	alarm-type=915
	auto-cleared=false
	auto-removed=true
	auto-removed-timeout=5000000
	duplication-counter=1
	functionality-type=SERVICE
	is-ticketable=true
	priority=0
	reduction-counter=1
	send-to-gw=true
	severity=MINOR
	short-description=keepalive not configured

Table 15-190 Keepalive Set

Event Setting	Registry Parameter
Type	keepalive set
Subtype	keepalive set
Correlation information	activate-flow=false
	correlate=false
	is-correlation-allowed=false
	weight=0

Table 15-190 Keepalive Set (continued)

Event Setting	Registry Parameter
Northbound metadata	alarm-type=915
	auto-cleared=false
	auto-removed=true
	auto-removed-timeout=5000000
	duplication-counter=1
	functionality-type=SERVICE
	is-ticketable=false
	priority=0
	reduction-counter=1
	send-to-gw=true
	severity=CLEARED
	short-description=keepalive configured

GRE Tunnel Down

Table 15-191 GRE Tunnel Down

Event Setting	Registry Parameter
Type	GRE tunnel down
Subtype	GRE tunnel down
Correlation information	activate-flow=true
	correlate=true
	is-correlation-allowed=true
	weight=830
Northbound metadata	alarm-type=358
	auto-cleared=false
	auto-removed=true
	functionality-type=SERVICE
	severity=MAJOR
	is-ticketable=true
	send-to-gw=true
	short-description=GRE tunnel down

Table 15-192 GRE Tunnel Up

Event Setting	Registry Parameter
Type	GRE tunnel down
Subtype	GRE tunnel up
Correlation information	activate-flow=false
	correlate=false
	is-correlation-allowed=false
	weight=0
Northbound metadata	alarm-type=358
	auto-cleared=false
	auto-removed=true
	functionality-type=SERVICE
	severity=CLEARED
	is-ticketable=false
	send-to-gw=true
	short-description=GRE tunnel up

HSRP Group Status Changed

Table 15-193 Primary HSRP Interface Is Active

Event Setting	Registry Parameter
Type	hsrp group status changed
Subtype	Primary HSRP interface is active
Correlation information	activate-flow=false
	correlate=false
	is-correlation-allowed=false
	weight=0
Northbound metadata	alarm-type=22
	auto-cleared=false
	auto-removed=true
	functionality-type=SERVICE
	severity=CLEARED
	is-ticketable=false
	send-to-gw=true
	short-description=Primary HSRP interface is active

Table 15-194 Primary HSRP Interface Is Not Active

Event Setting	Registry Parameter
Type	hsrp group status changed
Subtype	Primary HSRP interface is not active
Correlation information	activate-flow=true
	correlate=true
	is-correlation-allowed=true
	weight=720
Northbound metadata	alarm-type=22
	auto-cleared=false
	auto-removed=true
	functionality-type=SERVICE
	severity=MAJOR
	is-ticketable=true
	send-to-gw=true
	short-description=Primary HSRP interface is not active

Table 15-195 Secondary HSRP Interface Is Active

Event Setting	Registry Parameter
Type	hsrp group status changed
Subtype	Secondary HSRP interface is active
Correlation information	activate-flow=true
	correlate=true
	is-correlation-allowed=true
	weight=720
Northbound metadata	alarm-type=22
	auto-cleared=false
	auto-removed=true
	functionality-type=SERVICE
	severity=MAJOR
	is-ticketable=true
	send-to-gw=true
	short-description=Secondary HSRP interface is active

Table 15-196 Secondary HSRP Interface Is Not Active

Event Setting	Registry Parameter
Type	hsrp group status changed
Subtype	Secondary HSRP interface is not active
Correlation information	activate-flow=false
	correlate=false
	is-correlation-allowed=false
	weight=0
Northbound metadata	alarm-type=22
	auto-cleared=false
	auto-removed=true
	functionality-type=SERVICE
	severity=CLEARED
	is-ticketable=false
	send-to-gw=true
	short-description=Secondary HSRP interface is not active

Interface Status

Table 15-197 Interface Status Down GRE Tunnel

Event Setting	Registry Parameter
Type	interface status
Subtype	interface status down GRE tunnel
Correlation information	activate-flow=false
	correlate=true
	is-correlation-allowed=true
	weight=825
Northbound metadata	alarm-type=700
	auto-cleared=false
	auto-removed=true
	functionality-type=SERVICE
	severity=MAJOR
	is-ticketable=true
	send-to-gw=true
	short-description=Interface status down

Table 15-197 Interface Status Down GRE Tunnel (continued)

Event Setting	Registry Parameter
Flapping information	clear-interval=240000
	flapping-interval=60000
	flapping-threshold=5
	update-interval=200000
	update-threshold=20

Table 15-198 Interface Status Down Connection

Event Setting	Registry Parameter
Type	interface status
Subtype	interface status down connection
Correlation information	activate-flow=true
	correlate=true
	is-correlation-allowed=true
	weight=500
Northbound metadata	alarm-type=700
	auto-cleared=false
	auto-removed=true
	functionality-type=SERVICE
	severity=MAJOR
	is-ticketable=true
	send-to-gw=true
	short-description=Interface status down
Flapping information	clear-interval=240000
	flapping-interval=60000
	flapping-threshold=5
	update-interval=200000
	update-threshold=20

Table 15-199 Interface Status Down Nonconnection

Event Setting	Registry Parameter
Type	interface status
Subtype	interface status down non connection

Table 15-199 Interface Status Down Nonconnection (continued)

Event Setting	Registry Parameter
Correlation information	activate-flow=true
	correlate=true
	is-correlation-allowed=true
	weight=700
Northbound metadata	alarm-type=700
	auto-cleared=false
	auto-removed=true
	functionality-type=SERVICE
	severity=MAJOR
	is-ticketable=true
	send-to-gw=true
	short-description=Interface status down
Flapping information	clear-interval=240000
	flapping-interval=60000
	flapping-threshold=5
	update-interval=200000
	update-threshold=20

Table 15-200 Interface Status Up

Event Setting	Registry Parameter
Type	interface status
Subtype	interface status up
Correlation information	activate-flow=false
	correlate=false
	is-correlation-allowed=false
	weight=0
Northbound metadata	alarm-type=700
	auto-cleared=false
	auto-removed=true
	functionality-type=SERVICE
	severity=CLEARED
	is-ticketable=false
	send-to-gw=true
	short-description=Interface status up

Table 15-200 Interface Status Up (continued)

Event Setting	Registry Parameter
Flapping information	clear-interval=240000
	flapping-interval=60000
	flapping-threshold=5
	update-interval=200000
	update-threshold=20

Investigation State

Table 15-201 Investigation State

Event Setting	Registry Parameter
Type	investigation state
Subtype	investigation state module unsupported
Correlation information	activate-flow=false
	correlate=false
	is-correlation-allowed=false
	weight=0
Northbound metadata	alarm-type=262
	auto-cleared=false
	auto-removed=true
	functionality-type=SERVICE
	severity=CRITICAL
	is-ticketable=true
	send-to-gw=true
	short-description=Module unsupported

L2TP Peer Not Established

Table 15-202 L2TP Peer Established

Event Setting	Registry Parameter
Type	l2tp peer not established
Subtype	l2tp peer established
Correlation information	activate-flow=false
	correlate=false
	is-correlation-allowed=false
	weight=0

Table 15-202 L2TP Peer Established (continued)

Event Setting	Registry Parameter
Northbound metadata	alarm-type=185
	auto-cleared=false
	auto-removed=true
	functionality-type=SERVICE
	severity=CLEARED
	is-ticketable=false
	send-to-gw=true
	short-description=l2tp peer established
Flapping information	clear-interval=240000
	flapping-interval=60000
	flapping-threshold=5
	update-interval=200000
	update-threshold=20

Table 15-203 L2TP Peer Is Removed

Event Setting	Registry Parameter
Type	l2tp peer not established
Subtype	l2tp peer is removed
Correlation information	activate-flow=true
	correlate=true
	is-correlation-allowed=false
	weight=0
Northbound metadata	alarm-type=185
	auto-cleared=false
	auto-removed=true
	functionality-type=SERVICE
	severity=MAJOR
	is-ticketable=false
	send-to-gw=true
	short-description=l2tp peer is removed
Flapping information	clear-interval=240000
	flapping-interval=60000
	flapping-threshold=5
	update-interval=200000
	update-threshold=20

Table 15-204 L2TP Peer Not Established

Event Setting	Registry Parameter
Type	l2tp peer not established
Subtype	l2tp peer not established
Correlation information	activate-flow=true
	correlate=true
	is-correlation-allowed=false
	weight=0
Northbound metadata	alarm-type=185
	auto-cleared=false
	auto-removed=true
	functionality-type=SERVICE
	severity=MAJOR
	is-ticketable=true
	send-to-gw=true
	short-description=l2tp peer not established
Flapping information	clear-interval=240000
	flapping-interval=60000
	flapping-threshold=5
	update-interval=200000
	update-threshold=20

L2TP Sessions Threshold

Table 15-205 L2TP Sessions Count Exceeds Maximum Threshold

Event Setting	Registry Parameter
Type	l2tp sessions threshold
Subtype	l2tp sessions count exceeds max threshold
Correlation information	activate-flow=false
	correlate=true
	is-correlation-allowed=false
	weight=0

Table 15-205 L2TP Sessions Count Exceeds Maximum Threshold (continued)

Event Setting	Registry Parameter
Northbound metadata	alarm-type=N/A (TCA alarm)
	auto-cleared=false
	auto-removed=true
	functionality-type=SERVICE
	severity=MINOR
	is-ticketable=true
	send-to-gw=true
	short-description=l2tp sessions count exceeds max threshold

Table 15-206 L2TP Sessions Count Has Returned to Normal

Event Setting	Registry Parameter
Type	l2tp sessions threshold
Subtype	l2tp sessions count has returned to normal
Correlation information	activate-flow=false
	correlate=false
	is-correlation-allowed=false
	weight=0
Northbound metadata	alarm-type=N/A (TCA alarm)
	auto-cleared=false
	auto-removed=true
	functionality-type=SERVICE
	severity=CLEARED
	is-ticketable=false
	send-to-gw=true
	short-description=l2tp sessions count has returned to normal

Lag Down

Table 15-207 Lag Admin Down

Event Setting	Registry Parameter
Type	Lag down
Subtype	Lag admin down

Table 15-207 Lag Admin Down (continued)

Event Setting	Registry Parameter
Correlation information	activate-flow=false
	correlate=false
	is-correlation-allowed=false
	weight=0
Northbound metadata	alarm-type=718
	auto-cleared=false
	auto-removed=true
	functionality-type=SERVICE
	severity=MAJOR
	is-ticketable=true
	send-to-gw=true
	short-description=LAG down due to admin down

Table 15-208 Lag Oper Down

Event Setting	Registry Parameter
Type	lag down
Subtype	lag oper down
Correlation information	activate-flow=false
	correlate=false
	is-correlation-allowed=false
	weight=0
Northbound metadata	alarm-type=718
	auto-cleared=false
	auto-removed=true
	functionality-type=SERVICE
	severity=MAJOR
	is-ticketable=true
	send-to-gw=true
	short-description=Lag down due to oper down

Table 15-209 Lag Up

Event Setting	Registry Parameter
Type	lag down
Subtype	lag up

Table 15-209 Lag Up (continued)

Event Setting	Registry Parameter
Correlation information	activate-flow=false
	correlate=false
	is-correlation-allowed=false
	weight=0
Northbound metadata	alarm-type=718
	auto-cleared=false
	auto-removed=true
	functionality-type=SERVICE
	severity=CLEARED
	is-ticketable=false
	send-to-gw=true
	short-description=Lag up

Lag Link Down

Table 15-210 Lag Link Admin Down

Event Setting	Registry Parameter
Type	lag link down
Subtype	lag link admin down
Correlation information	activate-flow=false
	correlate=false
	is-correlation-allowed=false
	weight=0
Northbound metadata	alarm-type=719
	auto-cleared=false
	auto-removed=true
	functionality-type=SERVICE
	severity=MAJOR
	is-ticketable=true
	send-to-gw=true
	short-description=Lag Link down due to admin down

Table 15-211 Lag Link Oper Down

Event Setting	Registry Parameter
Type	lag link down
Subtype	lag link oper down
Correlation information	activate-flow=false
	correlate=false
	is-correlation-allowed=false
	weight=0
Northbound metadata	alarm-type=719
	auto-cleared=false
	auto-removed=true
	functionality-type=SERVICE
	severity=MAJOR
	is-ticketable=true
	send-to-gw=true
	short-description=Lag Link down due to oper down

Table 15-212 Lag Link Down on Unreachable

Event Setting	Registry Parameter
Type	lag link down
Subtype	lag link down on unreachable
Correlation information	activate-flow=false
	correlate=false
	is-correlation-allowed=false
	weight=0
Northbound metadata	alarm-type=719
	auto-cleared=false
	auto-removed=true
	functionality-type=SERVICE
	severity=CRITICAL
	is-ticketable=true
	send-to-gw=true
	short-description=Lag Link down on unreachable

Table 15-213 Lag Link Up

Event Setting	Registry Parameter
Type	lag link down
Subtype	lag link up
Correlation information	activate-flow=false
	correlate=false
	is-correlation-allowed=false
	weight=0
Northbound metadata	alarm-type=719
	auto-cleared=false
	auto-removed=true
	functionality-type=SERVICE
	severity=CLEARED
	is-ticketable=false
	send-to-gw=true
	short-description=Lag link up

Layer 2 Tunnel Down

Table 15-214 Layer 2 Tunnel Down

Event Setting	Registry Parameter
Type	layer 2 tunnel down
Subtype	layer 2 tunnel down
Correlation information	activate-flow=true
	correlate=true
	is-correlation-allowed=false
	weight=0
Northbound metadata	alarm-type=179
	auto-cleared=false
	auto-removed=true
	functionality-type=SERVICE
	severity=MINOR
	is-ticketable=true
	send-to-gw=true
	short-description=Layer 2 tunnel down

Table 15-215 Layer 2 Tunnel Up

Event Setting	Registry Parameter
Type	layer 2 tunnel down
Subtype	layer 2 tunnel up
Correlation information	activate-flow=false
	correlate=false
	is-correlation-allowed=false
	weight=0
Northbound metadata	alarm-type=179
	auto-cleared=false
	auto-removed=true
	functionality-type=SERVICE
	severity=CLEARED
	is-ticketable=false
	send-to-gw=true
	short-description=Layer 2 tunnel up

LDP Neighbor Loss

Table 15-216 LDP Neighbor Down

Event Setting	Registry Parameter
Type	LDP neighbor loss
Subtype	LDP neighbor down
Correlation information	activate-flow=true
	correlate=true
	is-correlation-allowed=true
	weight=670
Northbound metadata	alarm-type=557
	auto-cleared=false
	auto-removed=true
	functionality-type=SERVICE
	severity=MAJOR
	is-ticketable=true
	send-to-gw=true
	short-description=LDP neighbor down

Table 15-217 LDP Neighbor Up

Event Setting	Registry Parameter
Type	LDP neighbor loss
Subtype	LDP neighbor up
Correlation information	activate-flow=false
	correlate=false
	is-correlation-allowed=false
	weight=0
Northbound metadata	alarm-type=557
	auto-cleared=false
	auto-removed=true
	functionality-type=SERVICE
	severity=CLEARED
	is-ticketable=false
	send-to-gw=true
	short-description=LDP neighbor up

Link Down

Table 15-218 Link Down Due to Admin Down

Event Setting	Registry Parameter
Type	link down
Subtype	link down due to admin down
Correlation information	activate-flow=false
	correlate=false
	is-correlation-allowed=true
	weight=850
Northbound metadata	alarm-type=1
	auto-cleared=false
	auto-removed=true
	functionality-type=SERVICE
	severity=MINOR
	is-ticketable=true
	send-to-gw=true
	short-description=Link down due to admin down

Table 15-218 Link Down Due to Admin Down (continued)

Event Setting	Registry Parameter
Flapping information	clear-interval=360000
	flapping-interval=150000
	flapping-threshold=5
	update-interval=200000
	update-threshold=20

Table 15-219 Link Down Due to Card Event

Event Setting	Registry Parameter
Type	link down
Subtype	link down due to card
Correlation information	activate-flow=false
	correlate=true
	is-correlation-allowed=true
	weight=850
Northbound metadata	alarm-type=1
	auto-cleared=false
	auto-removed=true
	functionality-type=SERVICE
	severity=CRITICAL
	is-ticketable=true
	send-to-gw=true
	short-description=Link down due to Card event
Flapping information	clear-interval=360000
	flapping-interval=150000
	flapping-threshold=5
	update-interval=200000
	update-threshold=20

Table 15-220 Link Down Due to Oper Down

Event Setting	Registry Parameter
Type	link down
Subtype	link down due to oper down

Table 15-220 Link Down Due to Oper Down (continued)

Event Setting	Registry Parameter
Correlation information	activate-flow=false
	correlate=true
	is-correlation-allowed=true
	weight=850
Northbound metadata	alarm-type=1
	auto-cleared=false
	auto-removed=true
	functionality-type=SERVICE
	severity=CRITICAL
	is-ticketable=true
	send-to-gw=true
	short-description=Link down due to oper down
Flapping information	clear-interval=360000
	flapping-interval=150000
	flapping-threshold=5
	update-interval=200000
	update-threshold=20

Table 15-221 Link Down on Unreachable

Event Setting	Registry Parameter
Type	link down
Subtype	link down on unreachable
Correlation information	activate-flow=false
	correlate=true
	is-correlation-allowed=true
	weight=850
Northbound metadata	alarm-type=1
	auto-cleared=false
	auto-removed=true
	functionality-type=SERVICE
	severity=CRITICAL
	is-ticketable=true
	send-to-gw=true
	short-description=Link down on unreachable

Table 15-221 Link Down on Unreachable (continued)

Event Setting	Registry Parameter
Flapping information	clear-interval=360000
	flapping-interval=150000
	flapping-threshold=5
	update-interval=200000
	update-threshold=20

Table 15-222 Link Up

Event Setting	Registry Parameter
Type	link down
Subtype	link up
Correlation information	activate-flow=false
	correlate=false
	is-correlation-allowed=false
	weight=0
Northbound metadata	alarm-type=1
	auto-cleared=false
	auto-removed=true
	functionality-type=SERVICE
	severity=CLEARED
	is-ticketable=false
	send-to-gw=true
	short-description=Link up
Flapping information	clear-interval=360000
	flapping-interval=150000
	flapping-threshold=5
	update-interval=200000
	update-threshold=20

Link Utilization

Table 15-223 Link Overutilized

Event Setting	Registry Parameter
Type	link utilization
Subtype	link over Utilized

Table 15-223 Link Overutilized (continued)

Event Setting	Registry Parameter
Correlation information	activate-flow=false
	correlate=true
	is-correlation-allowed=true
	weight=0
Northbound metadata	alarm-type=642
	auto-cleared=false
	auto-removed=true
	functionality-type=SERVICE
	severity=MINOR
	is-ticketable=true
	send-to-gw=true
	short-description=Link over utilized

Table 15-224 Link Utilization Normal

Event Setting	Registry Parameter
Type	link utilization
Subtype	link utilization normal
Correlation information	activate-flow=false
	correlate=false
	is-correlation-allowed=true
	weight=0
Northbound metadata	alarm-type=642
	auto-cleared=false
	auto-removed=true
	functionality-type=SERVICE
	severity=CLEARED
	is-ticketable=false
	send-to-gw=true
	short-description=Link utilization normal

Local Switching Down

Table 15-225 Local Switching Entry Down

Event Setting	Registry Parameter
Type	local switching down
Subtype	local switching down
Correlation information	activate-flow=true
	correlate=true
	is-correlation-allowed=false
	weight=0
Northbound metadata	alarm-type=1299
	auto-cleared=false
	auto-removed=true
	functionality-type=SERVICE
	severity=MAJOR
	is-ticketable=true
	send-to-gw=true
	short-description=Local switching entry down

Table 15-226 Local Switching Entry Up

Event Setting	Registry Parameter
Type	local switching down
Subtype	local switching up
Correlation information	activate-flow=false
	correlate=false
	is-correlation-allowed=false
	weight=0
Northbound metadata	alarm-type=1299
	auto-cleared=false
	auto-removed=true
	functionality-type=SERVICE
	severity=CLEARED
	is-ticketable=false
	send-to-gw=true
	short-description=Local switching entry up

Logical Port Down

Table 15-227 Logical Port Down

Event Setting	Registry Parameter
Type	logical port down
Subtype	logical port down
Correlation information	activate-flow=false
	correlate=true
	is-correlation-allowed=true
	weight=0
Northbound metadata	alarm-type=198
	auto-cleared=false
	auto-removed=true
	functionality-type=SERVICE
	severity=MAJOR
	is-ticketable=true
	send-to-gw=true
	short-description=Logical port down

Table 15-228 Logical Port Up

Event Setting	Registry Parameter
Type	logical port down
Subtype	logical port up
Correlation information	activate-flow=false
	correlate=false
	is-correlation-allowed=false
	weight=0
Northbound metadata	alarm-type=198
	auto-cleared=false
	auto-removed=true
	functionality-type=SERVICE
	severity=CLEARED
	is-ticketable=false
	send-to-gw=true
	short-description=Logical port up

LSP Down

Table 15-229 LSP Down

Event Setting	Registry Parameter
Type	LSP Down
Subtype	LSP Down
Correlation information	activate-flow=true
	correlate=true
	is-correlation-allowed=true
	weight=110
Northbound metadata	alarm-type=189
	auto-cleared=false
	auto-removed=true
	functionality-type=SERVICE
	severity=MAJOR
	is-ticketable=true
	send-to-gw=true
	short-description=LSP down

Table 15-230 LSP Down Due to Label Mismatch

Event Setting	Registry Parameter
Type	LSP Down
Subtype	LSP Down Due to Label Mismatch
Correlation information	activate-flow=false
	correlate=false
	is-correlation-allowed=true
	weight=115
Northbound metadata	alarm-type=189
	auto-cleared=false
	auto-removed=true
	functionality-type=SERVICE
	severity=MAJOR
	is-ticketable=true
	send-to-gw=true
	short-description=LSP down due to label mismatch

Table 15-231 LSP Down Due to Lock Out

Event Setting	Registry Parameter
Type	LSP Down
Subtype	LSP Down Due to Lock Out
Correlation information	activate-flow=true
	correlate=true
	is-correlation-allowed=true
	weight=120
Northbound metadata	alarm-type=189
	auto-cleared=false
	auto-removed=true
	functionality-type=SERVICE
	severity=MINOR
	is-ticketable=true
	send-to-gw=true
	short-description=LSP locked out

Table 15-232 LSP Up

Event Setting	Registry Parameter
Type	LSP Down
Subtype	LSP Up
Correlation information	activate-flow=false
	correlate=false
	is-correlation-allowed=false
	weight=0
Northbound metadata	alarm-type=189
	auto-cleared=false
	auto-removed=true
	functionality-type=SERVICE
	severity=CLEARED
	is-ticketable=false
	send-to-gw=true
	short-description=LSP up

Members Changed

Table 15-233 High Priority Member Down

Event Setting	Registry Parameter
Type	Members Changed
Subtype	high priority member down
Correlation information	activate-flow=false
	correlate=false
	is-correlation-allowed=false
	weight=800
Northbound metadata	alarm-type=682
	auto-cleared=false
	auto-removed=true
	functionality-type=SERVICE
	severity=CRITICAL
	is-ticketable=true
	send-to-gw=true
	short-description=High priority member down

Table 15-234 Medium Priority Member Down

Event Setting	Registry Parameter
Type	Members Changed
Subtype	medium priority member down
Correlation information	activate-flow=false
	correlate=false
	is-correlation-allowed=false
	weight=800
Northbound metadata	alarm-type=682
	auto-cleared=false
	auto-removed=true
	functionality-type=SERVICE
	severity=MAJOR
	is-ticketable=true
	send-to-gw=true
	short-description=Medium priority member down

Table 15-235 Low Priority Member Down

Event Setting	Registry Parameter
Type	members changed
Subtype	low priority member down
Correlation information	activate-flow=false
	correlate=false
	is-correlation-allowed=false
	weight=800
Northbound metadata	alarm-type=682
	auto-cleared=false
	auto-removed=true
	functionality-type=SERVICE
	severity=MINOR
	is-ticketable=true
	send-to-gw=true
	short-description=Low priority member down

Table 15-236 All Members Operationally Up

Event Setting	Registry Parameter
Type	members changed
Subtype	members up
Correlation information	activate-flow=false
	correlate=false
	is-correlation-allowed=false
	weight=0
Northbound metadata	alarm-type=682
	auto-cleared=false
	auto-removed=true
	functionality-type=SERVICE
	severity=CLEARED
	is-ticketable=false
	send-to-gw=true
	short-description=All members operationally up

Memory Utilization

Table 15-237 Memory OK

Event Setting	Registry Parameter
Type	memory utilization
Subtype	memory normal use
Correlation information	activate-flow=false
	correlate=false
	is-correlation-allowed=false
	weight=0
Northbound metadata	alarm-type=18
	auto-cleared=false
	auto-removed=true
	functionality-type=SERVICE
	severity=CLEARED
	is-ticketable=false
	send-to-gw=true
	short-description=Memory utilization less than normal threshold

Table 15-238 Memory Overutilized

Event Setting	Registry Parameter
Type	memory utilization
Subtype	memory over utilized
Correlation information	activate-flow=-
	correlate=-
	is-correlation-allowed=-
	weight=-
Northbound metadata	alarm-type=18
	auto-cleared=false
	auto-removed=true
	functionality-type=SERVICE
	severity=MAJOR
	is-ticketable=true
	send-to-gw=true
	short-description=Memory utilization exceeded upper threshold

MLPPP Bundle

Table 15-239 MLPPP Down Due To Flapping

Event Setting	Registry Parameter
Type	mlppp down
Subtype	flapping
Correlation information	activate-flow=false
	correlate=false
	is-correlation-allowed=true
	weight=1000
Northbound metadata	alarm-type=914
	auto-cleared=false
	auto-removed=true
	auto-removed-timeout=5000000
	duplication-counter=1
	functionality-type=SERVICE
	is-ticketable=true
	priority=0
	reduction-counter=1
	send-to-gw=true
	severity=MAJOR
	short-description=mlppp down flapping

Table 15-240 MLPPP Down Flapping Update

Event Setting	Registry Parameter
Type	mlppp down
Subtype	flapping update
Correlation information	activate-flow=false
	correlate=false
	is-correlation-allowed=true
	weight=1000

Table 15-240 MLPPP Down Flapping Update (continued)

Event Setting	Registry Parameter
Northbound metadata	alarm-type=914
	auto-cleared=false
	auto-removed=true
	auto-removed-timeout=5000000
	duplication-counter=1
	functionality-type=SERVICE
	is-ticketable=true
	priority=0
	reduction-counter=1
	send-to-gw=true
	severity=MAJOR
	short-description=mlppp down flapping update

Table 15-241 MLPPP Down Due To Admin Down

Event Setting	Registry Parameter
Type	mlppp down
Subtype	mlppp admin down
Correlation information	activate-flow=false
	correlate=false
	is-correlation-allowed=true
	weight=1000
Northbound metadata	alarm-type=914
	auto-cleared=false
	auto-removed=true
	auto-removed-timeout=5000000
	duplication-counter=1
	functionality-type=SERVICE
	is-ticketable=true
	priority=0
	reduction-counter=1
	send-to-gw=true
	severity=CRITICAL
	short-description=mlppp administratively down

Table 15-242 MLPPP Down Flapping Proxy

Event Setting	Registry Parameter
Type	mlppp down
Subtype	local flapping proxy
Correlation information	activate-flow=false
	correlate=false
	is-correlation-allowed=true
	weight=1000
Northbound metadata	alarm-type=914
	auto-cleared=false
	auto-removed=true
	auto-removed-timeout=5000000
	duplication-counter=1
	functionality-type=SERVICE
	is-ticketable=false
	priority=0
	reduction-counter=1
	send-to-gw=false
	severity=INFO
	short-description=mlppp down flapping proxy

Table 15-243 MLPPP Down Due To Oper Down

Event Setting	Registry Parameter
Type	mlppp down
Subtype	mlppp oper down
Correlation information	activate-flow=false
	correlate=false
	is-correlation-allowed=true
	weight=1000

Table 15-243 MLPPP Down Due To Oper Down (continued)

Event Setting	Registry Parameter
Northbound metadata	alarm-type=914
	auto-cleared=false
	auto-removed=true
	auto-removed-timeout=5000000
	duplication-counter=1
	functionality-type=SERVICE
	is-ticketable=true
	priority=0
	reduction-counter=1
	send-to-gw=true
	severity=MAJOR
	short-description=mlppp operationally down

Table 15-244 MLPPP Up

Event Setting	Registry Parameter
Type	mlppp down
Subtype	mlppp up
Correlation information	activate-flow=false
	correlate=false
	is-correlation-allowed=true
	weight=1000
Northbound metadata	alarm-type=914
	auto-cleared=false
	auto-removed=true
	auto-removed-timeout=5000000
	duplication-counter=1
	functionality-type=SERVICE
	is-ticketable=false
	priority=0
	reduction-counter=1
	send-to-gw=true
	severity=CLEARED
	short-description=mlppp up

MPLS Black Hole Found

Table 15-245 MPLS Black Hole Cleared

Event Setting	Registry Parameter
Type	MPLS Black hole found
Subtype	MPLS Black hole cleared
Correlation information	activate-flow=false
	correlate=false
	is-correlation-allowed=false
	weight=0
Northbound metadata	alarm-type=128
	auto-cleared=false
	auto-removed=true
	functionality-type=SERVICE
	severity=CLEARED
	is-ticketable=false
	send-to-gw=true
	short-description=MPLS Black hole cleared

Table 15-246 MPLS Black Hole Found

Event Setting	Registry Parameter
Type	MPLS Black hole found
Subtype	MPLS Black hole found
Correlation information	activate-flow=true
	correlate=true
	is-correlation-allowed=true
	weight=650
Northbound metadata	alarm-type=128
	auto-cleared=false
	auto-removed=true
	functionality-type=SERVICE
	severity=WARNING
	is-ticketable=true
	send-to-gw=true
	short-description=MPLS Black hole found

MPLS TP Bandwidth Mismatch

Table 15-247 MPLS TP Bandwidth Mismatch

Event Setting	Registry Parameter
Type	MPLS TP Bandwidth Mismatch
Subtype	MPLS TP Bandwidth Mismatch
Correlation information	activate-flow=—
	correlate=—
	is-correlation-allowed=—
	weight=—
Northbound metadata	alarm-type=972
	auto-cleared=true
	auto-removed=true
	functionality-type=SERVICE
	severity=WARNING
	is-ticketable=true
	send-to-gw=true
	short-description=TPTunnel bandwidth mismatch

MPLS Interface Removed

Table 15-248 MPLS Interface Added

Event Setting	Registry Parameter
Type	MPLS interface removed
Subtype	MPLS interface added
Correlation information	activate-flow=false
	correlate=false
	is-correlation-allowed=false
	weight=0

Table 15-248 MPLS Interface Added (continued)

Event Setting	Registry Parameter
Northbound metadata	alarm-type=972
	auto-cleared=false
	auto-removed=true
	functionality-type=SERVICE
	severity=CLEARED
	is-ticketable=false
	send-to-gw=true
	short-description=MPLS interface added

Table 15-249 MPLS Interface Removed

Event Setting	Registry Parameter
Type	MPLS interface removed
Subtype	MPLS interface removed
Correlation information	activate-flow=true
	correlate=true
	is-correlation-allowed=true
	weight=700
Northbound metadata	alarm-type=972
	auto-cleared=false
	auto-removed=true
	functionality-type=SERVICE
	severity=MAJOR
	is-ticketable=true
	send-to-gw=true
	short-description=MPLS interface removed

MPLS TE FRR State Changed

Table 15-250 MPLS TE FRR State Changed to Active

Event Setting	Registry Parameter
Type	MPLS TE FRR State Changed
Subtype	MPLS TE FRR State Changed to Active

Table 15-250 MPLS TE FRR State Changed to Active (continued)

Event Setting	Registry Parameter
Correlation information	activate-flow=true
	correlate=true
	is-correlation-allowed=true
	root-cause-timeout=420000
	weight=700
Northbound metadata	alarm-type=1322
	auto-cleared=false
	auto-removed=true
	auto-removed-timeout=5000000
	duplication-counter=1
	functionality-type=SERVICE
	is-ticketable=true
	priority=0
	reduction-counter=1
	send-to-gw=true
	severity=MAJOR
	short-description=MPLS TE FRR State Changed to Active

Table 15-251 MPLS TE FRR State Changed to Ready

Event Setting	Registry Parameter
Type	MPLS TE FRR State Changed
Subtype	MPLS TE FRR State Changed to Ready
Correlation information	activate-flow=false
	correlate=false
	is-correlation-allowed=false
	root-cause-timeout=420000
	weight=0

Table 15-251 MPLS TE FRR State Changed to Ready (continued)

Event Setting	Registry Parameter
Northbound metadata	alarm-type=1322
	auto-cleared=false
	auto-removed=true
	auto-removed-timeout=5000000
	duplication-counter=1
	functionality-type=SERVICE
	is-ticketable=false
	priority=0
	reduction-counter=1
	send-to-gw=true
	severity=CLEARED
	short-description=MPLS TE FRR State Changed to Ready

MPLS TE Tunnel Down

Table 15-252 MPLS TE Tunnel Down

Event Setting	Registry Parameter
Type	mpls te tunnel down
Subtype	mpls te tunnel down
Correlation information	activate-flow=true
	correlate=true
	is-correlation-allowed=true
	weight=800
Northbound metadata	alarm-type=555
	auto-cleared=false
	auto-removed=true
	functionality-type=SERVICE
	severity=MAJOR
	is-ticketable=true
	send-to-gw=true
	short-description=MPLS TE tunnel down

Table 15-252 MPLS TE Tunnel Down (continued)

Event Setting	Registry Parameter
Flapping information	clear-interval=240000
	flapping-interval=60000
	flapping-threshold=5
	update-interval=200000
	update-threshold=20

Table 15-253 High Priority MPLS TE Tunnel Down

Event Setting	Registry Parameter
Type	mpls te tunnel down
Subtype	High Priority mpls te tunnel down
Correlation information	activate-flow=true
	correlate=true
	is-correlation-allowed=true
	weight=800
Northbound metadata	alarm-type=555
	auto-cleared=false
	auto-removed=true
	functionality-type=SERVICE
	severity=CRITICAL
	is-ticketable=true
	send-to-gw=true
	short-description=High Priority MPLS-TE tunnel down
Flapping information	clear-interval=240000
	flapping-interval=60000
	flapping-threshold=5
	update-interval=200000
	update-threshold=20

Table 15-254 Medium Priority MPLS TE Tunnel Down

Event Setting	Registry Parameter
Type	mpls te tunnel down
Subtype	Medium Priority mpls te tunnel down

Table 15-254 Medium Priority MPLS TE Tunnel Down (continued)

Event Setting	Registry Parameter
Correlation information	activate-flow=true
	correlate=true
	is-correlation-allowed=true
	weight=800
Northbound metadata	alarm-type=555
	auto-cleared=false
	auto-removed=true
	functionality-type=SERVICE
	severity=MAJOR
	is-ticketable=true
	send-to-gw=true
	short-description=Medium Priority MPLS-TE tunnel down
Flapping information	clear-interval=240000
	flapping-interval=60000
	flapping-threshold=5
	update-interval=200000
	update-threshold=20

Table 15-255 Low Priority MPLS TE Tunnel Down

Event Setting	Registry Parameter
Type	mpls te tunnel down
Subtype	Low Priority mpls te tunnel down
Correlation information	activate-flow=true
	correlate=true
	is-correlation-allowed=true
	weight=800
Northbound metadata	alarm-type=555
	auto-cleared=false
	auto-removed=true
	functionality-type=SERVICE
	severity=MINOR
	is-ticketable=true
	send-to-gw=true
	short-description=Low Priority MPLS-TE tunnel down

Table 15-255 Low Priority MPLS TE Tunnel Down (continued)

Event Setting	Registry Parameter
Flapping information	clear-interval=240000
	flapping-interval=60000
	flapping-threshold=5
	update-interval=200000
	update-threshold=20

Table 15-256 MPLS TE Tunnel Reoptimized

Event Setting	Registry Parameter
Type	mpls te tunnel down
Subtype	mpls te tunnel down reoptimized
Correlation information	activate-flow=true
	correlate=true
	is-correlation-allowed=true
	weight=800
Northbound metadata	alarm-type=555
	auto-cleared=false
	auto-removed=true
	functionality-type=SERVICE
	severity=INFO
	is-ticketable=true
	send-to-gw=true
	short-description=MPLS TE-tunnel reoptimized
Flapping information	clear-interval=240000
	flapping-interval=60000
	flapping-threshold=5
	update-interval=200000
	update-threshold=20

Table 15-257 MPLS TE Tunnel Rerouted

Event Setting	Registry Parameter
Type	mpls te tunnel down
Subtype	mpls te tunnel rerouted

Table 15-257 MPLS TE Tunnel Rerouted (continued)

Event Setting	Registry Parameter
Correlation information	activate-flow=true
	correlate=true
	is-correlation-allowed=true
	weight=800
Northbound metadata	alarm-type=555
	auto-cleared=false
	auto-removed=true
	functionality-type=SERVICE
	severity=INFO
	is-ticketable=true
	send-to-gw=true
	short-description=MPLS-TE tunnel rerouted
Flapping information	clear-interval=240000
	flapping-interval=60000
	flapping-threshold=5
	update-interval=200000
	update-threshold=20

Table 15-258 MPLS TE Tunnel Up

Event Setting	Registry Parameter
Type	mpls te tunnel down
Subtype	mpls te tunnel up
Correlation information	activate-flow=false
	correlate=false
	is-correlation-allowed=false
	weight=0
Northbound metadata	alarm-type=555
	auto-cleared=false
	auto-removed=true
	functionality-type=SERVICE
	severity=CLEARED
	is-ticketable=false
	send-to-gw=true
	short-description=MPLS-TE tunnel up

Table 15-258 MPLS TE Tunnel Up (continued)

Event Setting	Registry Parameter
Flapping information	clear-interval=240000
	flapping-interval=60000
	flapping-threshold=5
	update-interval=200000
	update-threshold=20

Table 15-259 TP Tunnel Down Due to Admin Down

Event Setting	Registry Parameter
Type	TP Tunnel Down
Subtype	TP Tunnel Down Due to Admin Down
Correlation information	activate-flow=false
	correlate=false
	is-correlation-allowed=true
	weight=150
Northbound metadata	alarm-type=180
	auto-cleared=false
	auto-removed=true
	functionality-type=SERVICE
	severity=MINOR
	is-ticketable=true
	send-to-gw=true
	short-description=MPLS-TP tunnel admin down

MPLS TP Tunnel Down

Table 15-260 TP Tunnel Down Due to Oper Down

Event Setting	Registry Parameter
Type	TP Tunnel Down
Subtype	TP Tunnel Down Due to Oper Down
Correlation information	activate-flow=true
	correlate=true
	is-correlation-allowed=true
	weight=100

Table 15-260 TP Tunnel Down Due to Oper Down (continued)

Event Setting	Registry Parameter
Northbound metadata	alarm-type=180
	auto-cleared=false
	auto-removed=true
	functionality-type=SERVICE
	severity=MAJOR
	is-ticketable=true
	send-to-gw=true
	short-description= MPLS-TP tunnel oper down.

Network-Clock Synchronization

Table 15-261 Network-Clock Synchronization Enabled

Event Setting	Registry Parameter
Type	network-clock synchronization
Subtype	network-clock synchronization enabled
Correlation information	activate-flow=false
	correlate=false
	is-correlation-allowed=false
	weight=0
Northbound metadata	alarm-type=685
	auto-cleared=false
	auto-removed=true
	functionality-type=SERVICE
	severity=CLEARED
	is-ticketable=false
	send-to-gw=true
	short-description= network-clock synchronization enabled

Table 15-262 Network-Clock Synchronization Disabled

Event Setting	Registry Parameter
Type	network-clock synchronization
Subtype	network-clock synchronization disabled

Table 15-262 Network-Clock Synchronization Disabled (continued)

Event Setting	Registry Parameter
Correlation information	activate-flow=false
	correlate=false
	is-correlation-allowed=true
	weight=750
Northbound metadata	alarm-type=685
	auto-cleared=false
	auto-removed=true
	functionality-type=SERVICE
	severity=MAJOR
	is-ticketable=true
	send-to-gw=true
	short-description=network-clock synchronization disabled

OSPF Neighbor State Change

Table 15-263 OSPF Neighbor Down

Event Setting	Registry Parameter
Type	ospf neighbor state change
Subtype	ospf neighbor down
Correlation information	activate-flow=true
	correlate=true
	is-correlation-allowed=true
	weight=200
Northbound metadata	alarm-type=1350
	auto-cleared=false
	auto-removed=true
	functionality-type=SERVICE
	severity=MAJOR
	is-ticketable=true
	send-to-gw=true
	short-description=OSPF Neighbor Down

Table 15-264 OSPF Neighbor Up

Event Setting	Registry Parameter
Type	ospf neighbor state change
Subtype	ospf neighbor up
Correlation information	activate-flow=false
	correlate=false
	is-correlation-allowed=false
	weight=0
Northbound metadata	alarm-type=1350
	auto-cleared=false
	auto-removed=true
	functionality-type=SERVICE
	severity=CLEARED
	is-ticketable=false
	send-to-gw=true
	short-description=OSPF Neighbor Up

Port Down

Table 15-265 Port Down Due to Admin

Event Setting	Registry Parameter
Type	port down
Subtype	port down due to admin
Correlation information	activate-flow=false
	correlate=false
	is-correlation-allowed=true
	weight=100000
Northbound metadata	alarm-type=2
	auto-cleared=false
	auto-removed=true
	functionality-type=SERVICE
	severity=MINOR
	is-ticketable=true
	send-to-gw=true
	short-description=Port down due to admin

Table 15-265 Port Down Due to Admin (continued)

Event Setting	Registry Parameter
Flapping information	clear-interval=360000
	flapping-interval=150000
	flapping-threshold=5
	update-interval=200000
	update-threshold=20

Table 15-266 Port Down Due to Oper

Event Setting	Registry Parameter
Type	port down
Subtype	port down due to oper
Correlation information	activate-flow=false
	correlate=false
	is-correlation-allowed=true
	weight=100000
Northbound metadata	alarm-type=2
	auto-cleared=false
	auto-removed=true
	functionality-type=SERVICE
	severity=MAJOR
	is-ticketable=true
	send-to-gw=true
	short-description=Port down due to oper
Flapping information	clear-interval=360000
	flapping-interval=150000
	flapping-threshold=5
	update-interval=200000
	update-threshold=20

Table 15-267 Port Down Due to Card Event

Event Setting	Registry Parameter
Type	port down
Subtype	port down due to card

Table 15-267 Port Down Due to Card Event (continued)

Event Setting	Registry Parameter
Correlation information	activate-flow=false
	correlate=true
	is-correlation-allowed=true
	weight=900
Northbound metadata	alarm-type=2
	auto-cleared=false
	auto-removed=true
	functionality-type=SERVICE
	severity=MAJOR
	is-ticketable=true
	send-to-gw=true
	short-description=Port down due to Card event
Flapping information	clear-interval=360000
	flapping-interval=150000
	flapping-threshold=5
	update-interval=200000
	update-threshold=20

Table 15-268 Port Up

Event Setting	Registry Parameter
Type	port down
Subtype	port up
Correlation information	activate-flow=false
	correlate=false
	is-correlation-allowed=false
	weight=0
Northbound metadata	alarm-type=2
	auto-cleared=false
	auto-removed=true
	functionality-type=SERVICE
	severity=CLEARED
	is-ticketable=false
	send-to-gw=true
	short-description=Port up

Table 15-268 Port Up (continued)

Event Setting	Registry Parameter
Flapping information	clear-interval=360000
	flapping-interval=150000
	flapping-threshold=5
	update-interval=200000
	update-threshold=20

Power Supply Down

Table 15-269 Power Supply Down

Event Setting	Registry Parameter
Type	Power Supply Down
Subtype	Power Supply Down
Correlation information	activate-flow=false
	correlate=false
	is-correlation-allowed=true
	weight=0
Northbound metadata	alarm-type=13001
	auto-cleared=false
	auto-removed=true
	functionality-type=SERVICE
	severity=MAJOR
	is-ticketable=true
	send-to-gw=true
	short-description=Power supply down

Table 15-270 Power Supply Up

Event Setting	Registry Parameter
Type	Power Supply Down
Subtype	Power Supply Up
Correlation information	activate-flow=false
	correlate=false
	is-correlation-allowed=false
	weight=0

Table 15-270 Power Supply Up

Event Setting	Registry Parameter
Northbound metadata	alarm-type=13001
	auto-cleared=false
	auto-removed=true
	functionality-type=SERVICE
	severity=CLEARED
	is-ticketable=false
	send-to-gw=true
	short-description=Power supply up

Power Supply Out

Table 15-271 Power Supply Out

Event Setting	Registry Parameter
Type	Power supply out
Subtype	Power supply out
Correlation information	activate-flow=false
	correlate=false
	is-correlation-allowed=true
	weight=0
Northbound metadata	alarm-type=13000
	auto-cleared=false
	auto-removed=true
	functionality-type=SERVICE
	severity=MAJOR
	is-ticketable=true
	send-to-gw=true
	short-description=Power supply out

Table 15-272 Power Supply In

Event Setting	Registry Parameter
Type	Power supply out
Subtype	Power supply in

Table 15-272 Power Supply In

Event Setting	Registry Parameter
Correlation information	activate-flow=false
	correlate=false
	is-correlation-allowed=false
	weight=0
Northbound metadata	alarm-type=13000
	auto-cleared=false
	auto-removed=true
	functionality-type=SERVICE
	severity=CLEARED
	is-ticketable=false
	send-to-gw=true
	short-description=Power supply in

Pluggable Transceiver Out

Table 15-273 Pluggable Transceiver In

Event Setting	Registry Parameter
Type	pluggable transceiver out
Subtype	pluggable transceiver in
Correlation information	activate-flow=false
	correlate=false
	is-correlation-allowed=false
	weight=0
Northbound metadata	alarm-type=13004
	auto-cleared=false
	auto-removed=true
	functionality-type=SERVICE
	severity=CLEARED
	is-ticketable=false
	send-to-gw=true
	short-description=Pluggable transceiver in

Table 15-274 Pluggable Transceiver Out

Event Setting	Registry Parameter
Type	pluggable transceiver out
Subtype	pluggable transceiver out
Correlation information	activate-flow=false
	correlate=true
	is-correlation-allowed=true
	weight=750
Northbound metadata	alarm-type=13004
	auto-cleared=false
	auto-removed=true
	functionality-type=SERVICE
	severity=MAJOR
	is-ticketable=true
	send-to-gw=true
	short-description=Pluggable transceiver out

REP Port Role Change

Table 15-275 REP Port Role Failed

Event Setting	Registry Parameter
Type	REP Port Role Change
Subtype	REP Port Role Failed
Correlation information	activate-flow=false
	correlate=true
	is-correlation-allowed=true
	weight=101
Northbound metadata	alarm-type=4000000
	auto-cleared=false
	auto-removed=true
	functionality-type=SERVICE
	severity=MAJOR
	is-ticketable=true
	send-to-gw=true
	short-description=REP Port Role Failed

Table 15-276 REP Port Role Ok

Event Setting	Registry Parameter
Type	REP Port Role Change
Subtype	REP Port Role Ok
Correlation information	activate-flow=false
	correlate=false
	is-correlation-allowed=false
	weight=0
Northbound metadata	alarm-type=4000000
	auto-cleared=false
	auto-removed=true
	functionality-type=SERVICE
	severity=CLEARED
	is-ticketable=false
	send-to-gw=true
	short-description=REP Port Role Ok

Rx Dormant

Table 15-277 Rx Dormant

Event Setting	Registry Parameter
Type	rx dormant
Subtype	rx dormant
Correlation information	activate-flow=false
	correlate=false
	is-correlation-allowed=false
	weight=0
Northbound metadata	alarm-type=378
	auto-cleared=false
	auto-removed=true
	functionality-type=SERVICE
	severity=MINOR
	is-ticketable=true
	send-to-gw=true
	short-description=rx dormant

Table 15-278 Rx Dormant Normal

Event Setting	Registry Parameter
Type	rx dormant
Subtype	rx dormant normal
Correlation information	activate-flow=false
	correlate=false
	is-correlation-allowed=false
	weight=0
Northbound metadata	alarm-type=378
	auto-cleared=false
	auto-removed=true
	functionality-type=SERVICE
	severity=CLEARED
	is-ticketable=false
	send-to-gw=true
	short-description=rx dormant normal

Rx Utilization

Table 15-279 Rx Overutilized

Event Setting	Registry Parameter
Type	rx utilization
Subtype	rx over Utilized
Correlation information	activate-flow=false
	correlate=true
	is-correlation-allowed=false
	weight=0
Northbound metadata	alarm-type=8
	auto-cleared=false
	auto-removed=true
	functionality-type=SERVICE
	severity=MINOR
	is-ticketable=true
	send-to-gw=true
	short-description=Rx utilization exceeded upper threshold

Table 15-280 Rx Utilization Normal

Event Setting	Registry Parameter
Type	rx utilization
Subtype	rx utilization normal
Correlation information	activate-flow=false
	correlate=false
	is-correlation-allowed=false
	weight=0
Northbound metadata	alarm-type=8
	auto-cleared=false
	auto-removed=true
	functionality-type=SERVICE
	severity=CLEARED
	is-ticketable=false
	send-to-gw=true
	short-description=Rx utilization is below lower threshold

Shelf Out

Table 15-281 Shelf In

Event Setting	Registry Parameter
Type	shelf out
Subtype	shelf in
Correlation information	activate-flow=false
	correlate=false
	is-correlation-allowed=false
	weight=0
Northbound metadata	alarm-type=33
	auto-cleared=false
	auto-removed=true
	functionality-type=SERVICE
	severity=CLEARED
	is-ticketable=false
	send-to-gw=true
	short-description=Shelf in

Table 15-282 Shelf Out

Event Setting	Registry Parameter
Type	shelf out
Subtype	shelf out
Correlation information	activate-flow=false
	correlate=false
	is-correlation-allowed=true
	weight=110000
Northbound metadata	alarm-type=33
	auto-cleared=false
	auto-removed=true
	functionality-type=SERVICE
	severity=MAJOR
	is-ticketable=true
	send-to-gw=true
	short-description=Shelf out

SONET Path Link Down

Table 15-283 SONET Path Link Down Due to Admin Down

Event Setting	Registry Parameter
Type	sonetpath link down
Subtype	sonetpath link down due to admin down
Correlation information	activate-flow=false
	correlate=false
	is-correlation-allowed=true
	weight=845
Northbound metadata	alarm-type=1345
	auto-cleared=false
	auto-removed=true
	functionality-type=SERVICE
	severity=CRITICAL
	is-ticketable=true
	send-to-gw=true
	short-description=SONET Path link down due to admin down

Table 15-283 SONET Path Link Down Due to Admin Down (continued)

Event Setting	Registry Parameter
Flapping information	clear-interval=360000
	flapping-interval=150000
	flapping-threshold=5
	update-interval=200000
	update-threshold=20

Table 15-284 SONET Path Link Down Due to Oper Down

Event Setting	Registry Parameter
Type	sonetpath link down
Subtype	sonetpath link down due to oper down
Correlation information	activate-flow=true
	correlate=true
	is-correlation-allowed=true
	weight=840
Northbound metadata	alarm-type=1345
	auto-cleared=false
	auto-removed=true
	functionality-type=SERVICE
	severity=CRITICAL
	is-ticketable=true
	send-to-gw=true
	short-description=SONET Path link down due to oper down
Flapping information	clear-interval=360000
	flapping-interval=150000
	flapping-threshold=5
	update-interval=200000
	update-threshold=20

Table 15-285 SONET Path Link Down Due to Card

Event Setting	Registry Parameter
Type	sonetpath link down
Subtype	sonetpath link down due to card

Table 15-285 SONET Path Link Down Due to Card (continued)

Event Setting	Registry Parameter
Correlation information	activate-flow=false
	correlate=true
	is-correlation-allowed=true
	weight=845
Northbound metadata	alarm-type=1345
	auto-cleared=false
	auto-removed=true
	functionality-type=SERVICE
	severity=CRITICAL
	is-ticketable=true
	send-to-gw=true
	short-description=SONET Path link down due to Card event
Flapping information	clear-interval=360000
	flapping-interval=150000
	flapping-threshold=5
	update-interval=200000
	update-threshold=20

Table 15-286 SONET Path Link Down on Unreachable

Event Setting	Registry Parameter
Type	sonetpath link down
Subtype	sonetpath link down due on unreachable
Correlation information	activate-flow=true
	correlate=true
	is-correlation-allowed=true
	weight=840
Northbound metadata	alarm-type=1345
	auto-cleared=false
	auto-removed=true
	functionality-type=SERVICE
	severity=CRITICAL
	is-ticketable=true
	send-to-gw=true
	short-description=SONET Path Link down on unreachable

Table 15-286 SONET Path Link Down on Unreachable (continued)

Event Setting	Registry Parameter
Flapping information	clear-interval=360000
	flapping-interval=150000
	flapping-threshold=5
	update-interval=200000
	update-threshold=20

Table 15-287 SONET Path Link Up

Event Setting	Registry Parameter
Type	sonetpath link down
Subtype	sonetpath link up
Correlation information	activate-flow=false
	correlate=false
	is-correlation-allowed=false
	weight=0
Northbound metadata	alarm-type=1345
	auto-cleared=false
	auto-removed=true
	functionality-type=SERVICE
	severity=CLEARED
	is-ticketable=false
	send-to-gw=true
	short-description=SONET Path Link up
Flapping information	clear-interval=360000
	flapping-interval=150000
	flapping-threshold=5
	update-interval=200000
	update-threshold=20

SONET Path Port Down

Table 15-288 SONET Path Port Down Due to Admin Down

Event Setting	Registry Parameter
Type	sonetpath port down
Subtype	sonetpath port down due to admin

Table 15-288 SONET Path Port Down Due to Admin Down (continued)

Event Setting	Registry Parameter
Correlation information	activate-flow=true
	correlate=true
	is-correlation-allowed=true
	weight=840
Northbound metadata	alarm-type=1333
	auto-cleared=false
	auto-removed=true
	functionality-type=SERVICE
	severity=MAJOR
	is-ticketable=true
	send-to-gw=true
	short-description=SONET Path down due to Admin
Flapping information	clear-interval=360000
	flapping-interval=150000
	flapping-threshold=5
	update-interval=200000
	update-threshold=20

Table 15-289 SONET Path Port Down Due to Oper Down

Event Setting	Registry Parameter
Type	sonetpath port down
Subtype	sonetpath port down due to oper
Correlation information	activate-flow=true
	correlate=true
	is-correlation-allowed=true
	weight=840
Northbound metadata	alarm-type=1333
	auto-cleared=false
	auto-removed=true
	functionality-type=SERVICE
	severity=MAJOR
	is-ticketable=true
	send-to-gw=true
	short-description=SONET Path down due to Oper

Table 15-289 SONET Path Port Down Due to Oper Down (continued)

Event Setting	Registry Parameter
Flapping information	clear-interval=360000
	flapping-interval=150000
	flapping-threshold=5
	update-interval=200000
	update-threshold=20

Table 15-290 SONET Path Port Down Due to Card

Event Setting	Registry Parameter
Type	sonetpath port down
Subtype	sonetpath port down due to card
Correlation information	activate-flow=false
	correlate=true
	is-correlation-allowed=true
	weight=845
Northbound metadata	alarm-type=1333
	auto-cleared=false
	auto-removed=true
	functionality-type=SERVICE
	severity=MAJOR
	is-ticketable=true
	send-to-gw=true
	short-description=SONET Path down due to Card
Flapping information	clear-interval=360000
	flapping-interval=150000
	flapping-threshold=5
	update-interval=200000
	update-threshold=20

Table 15-291 SONET Path Port Up

Event Setting	Registry Parameter
Type	sonetpath port down
Subtype	sonetpath port up

Table 15-291 SONET Path Port Up (continued)

Event Setting	Registry Parameter
Correlation information	activate-flow=false
	correlate=false
	is-correlation-allowed=true
	weight=845
Northbound metadata	alarm-type=1333
	auto-cleared=false
	auto-removed=true
	functionality-type=SERVICE
	severity=CLEARED
	is-ticketable=false
	send-to-gw=true
	short-description=SONET Path up
Flapping information	clear-interval=360000
	flapping-interval=150000
	flapping-threshold=5
	update-interval=200000
	update-threshold=20

Subinterface Down

Table 15-292 Subinterface Down

Event Setting	Registry Parameter
Type	sub-interface down
Subtype	sub-interface oper down
Correlation information	activate-flow=true
	correlate=true
	is-correlation-allowed=true
	weight=849

Table 15-292 Subinterface Down (continued)

Event Setting	Registry Parameter
Northbound metadata	alarm-type=917
	auto-cleared=false
	auto-removed=true
	functionality-type=SERVICE
	severity=MAJOR
	is-ticketable=true
	send-to-gw=true
	short-description=VLAN SubInterface oper down

Table 15-293 Subinterface Admin Down

Event Setting	Registry Parameter
Type	sub-interface down
Subtype	sub-interface admin down
Correlation information	activate-flow=true
	correlate=true
	is-correlation-allowed=true
	weight=849
Northbound metadata	alarm-type=917
	auto-cleared=false
	auto-removed=true
	functionality-type=SERVICE
	severity=MAJOR
	is-ticketable=true
	send-to-gw=true
	short-description=VLAN Sub Interface admin down

Table 15-294 Subinterface Up

Event Setting	Registry Parameter
Type	sub-interface down
Subtype	sub-interface up
Correlation information	activate-flow=false
	correlate=false
	is-correlation-allowed=false
	weight=0

Table 15-294 Subinterface Up (continued)

Event Setting	Registry Parameter
Northbound metadata	alarm-type=917
	auto-cleared=false
	auto-removed=true
	functionality-type=SERVICE
	severity=CLEARED
	is-ticketable=false
	send-to-gw=true
	short-description=VLAN Sub Interface up

Tx Dormant

Table 15-295 Tx Dormant

Event Setting	Registry Parameter
Type	tx dormant
Subtype	tx dormant
Correlation information	activate-flow=false
	correlate=false
	is-correlation-allowed=false
	weight=0
Northbound metadata	alarm-type=377
	auto-cleared=false
	auto-removed=true
	functionality-type=SERVICE
	severity=MINOR
	is-ticketable=true
	send-to-gw=true
	short-description=tx dormant

Table 15-296 Tx Dormant Normal

Event Setting	Registry Parameter
Type	tx dormant
Subtype	tx dormant normal

Table 15-296 Tx Dormant Normal (continued)

Event Setting	Registry Parameter
Correlation information	activate-flow=false
	correlate=false
	is-correlation-allowed=false
	weight=0
Northbound metadata	alarm-type=377
	auto-cleared=false
	auto-removed=true
	functionality-type=SERVICE
	severity=CLEARED
	is-ticketable=false
	send-to-gw=true
	short-description=tx dormant normal

Tx Utilization

Table 15-297 Tx Overutilized

Event Setting	Registry Parameter
Type	tx utilization
Subtype	tx over Utilized
Correlation information	activate-flow=false
	correlate=true
	is-correlation-allowed=false
	weight=0
Northbound metadata	alarm-type=7
	auto-cleared=false
	auto-removed=true
	functionality-type=SERVICE
	severity=MINOR
	is-ticketable=true
	send-to-gw=true
	short-description=Tx utilization exceeded upper threshold

Table 15-298 Tx Utilization Normal

Event Setting	Registry Parameter
Type	tx utilization
Subtype	tx utilization normal
Correlation information	activate-flow=false
	correlate=false
	is-correlation-allowed=false
	weight=0
Northbound metadata	alarm-type=7
	auto-cleared=false
	auto-removed=true
	functionality-type=SERVICE
	severity=CLEARED
	is-ticketable=false
	send-to-gw=true
	short-description=Tx utilization is below lower threshold

VSI Down

Table 15-299 VSI Down

Event Setting	Registry Parameter
Type	vsi down
Subtype	vsi oper down
Correlation information	activate-flow=true
	correlate=true
	is-correlation-allowed=true
	weight=845
Northbound metadata	alarm-type=916
	auto-cleared=false
	auto-removed=true
	functionality-type=SERVICE
	severity=MAJOR
	is-ticketable=true
	send-to-gw=true
	short-description=VSI oper down

Table 15-300 VSI Admin Down

Event Setting	Registry Parameter
Type	vsi down
Subtype	vsi admin down
Correlation information	activate-flow=false
	correlate=false
	is-correlation-allowed=true
	weight=101
Northbound metadata	alarm-type=916
	auto-cleared=false
	auto-removed=true
	functionality-type=SERVICE
	severity=MAJOR
	is-ticketable=true
	send-to-gw=true
	short-description=VSI admin down

Table 15-301 VSI Up

Event Setting	Registry Parameter
Type	vsi down
Subtype	vsi up
Correlation information	activate-flow=false
	correlate=false
	is-correlation-allowed=false
	weight=0
Northbound metadata	alarm-type=916
	auto-cleared=false
	auto-removed=true
	functionality-type=SERVICE
	severity=CLEARED
	is-ticketable=false
	send-to-gw=true
	short-description=VSI up

Alarm Source OIDs

These topics describe the possible source object identifiers (OIDs) of alarms generated by Prime Network. A description of each source OID and OID structure is given, with examples of OIDs and service alarms that use those OIDs as their source.

Note The source OID must be unique in the alarm type context. For example, it is not possible to generate multiple different alarms with the same type from the same component using the component OID as the source. An additional differentiator should be added to the base component OID. See LSE OID (ILseOid), for an example.

The following source OIDs are described:

- BFD Connectivity Down OID
- BFD Neighbor Loss OID
- BGP Neighbor Entry OID (IBgpNeighborEntryOid)
- Carrier Grade NAT OID (ICgnServiceOid)
- Chassis Oid (ChassisId)
- DS0 Bundle OID (IDS0BundleOid)
- DS1 Path OID (IDS1PathOid)
- DS3 Path OID (IDS3PathOid)
- DWDM Controller OID (IDWDMOid)
- EFP OID (IEFPOID)
- Fan Tray OID
- IMA Service (IIMAGroupOid)
- IP Interface OID (IPInterfaceOid)
- L2TP Peer OID (IL2tpPeerOid)
- Lag Down OID
- Lag Link Down OID
- Local Switching Entry Down OID
- Logical Port OID (ILogicalPortOid)
- LSE OID (ILseOid)
- Managed Element OID (IManagedElementOid)
- Members Changed OID (IDataLinkAggregationOid)
- MLPPP OID (IMLPPPOid)
- Module OID (IModuleOid)
- MPBGP OID (IMpBgpOid)
- MPLS TE Tunnel OID (IMplsTETunnelOid)
- TP Tunnel Endpoint OID (TP Tunnel EndPoint OID)
- ISyncEOID
- OSPF Neighbor State Change OID

- Power Supply OID
- Physical Layer OID (IPhysicalLayerOid)
- Shelf OID (IShelfOid)
- SONET Path Port Down OID
- SONET Path Link Down OID
- Topological Link OID (ITopologicalLinkOid)
- VLAN Tagged Interface OID (IVlanTaggedInterfaceOID)
- VSI OID (IVSIOID)

BFD Connectivity Down OID

The BFD Connectivity Down OID supports the BFD Connectivity Down Alarm.

Example

```
{[TopologicalLink(AEndPoint={[ManagedElement(Key=p1)][LogicalRoot][Context(ContextName=Def
ault
context)][BfdService]})(LinkType=14)(TunnelID=-1)(ZEndPoint={[ManagedElement(Key=c3-npe1-7
6)][LogicalRoot][Context(ContextName=Default
context)][BfdService][ServiceEvent(DiffObject=2.0.0.29 <-> 2.0.0.30)]})]}
```

BFD Neighbor Loss OID

The BFD Neighbor Loss OID supports the BFD Neighbor Loss Alarm.

Example

```
ManagedElement(Key=p1)][LogicalRoot][Context(ContextName=Default context)][BfdService]})
```

BGP Neighbor Entry OID (IBgpNeighborEntryOid)

The BGP Neighbor Entry OID is the source OID for any alarms related to BGP neighbors.

The BGP Neighbor Entry source OID supports the BGP Neighbor Loss alarm.

The structure of the BGP Neighbor Entry OID is:

{[ManagedElement(Key=*deviceName*)][LogicalRoot][FWComponentContainer(Type=7)][MpBgp][BgpNeighborEntry(PeerIdentifier=*peerIP*)(VrfName=*vrfName*)]}

The VrfName identifier in the BGP entry part exists if the entry is under VRF.

Example

```
{[ManagedElement(Key=PE3-NY-7300)][LogicalRoot][FWComponentContainer(Type=7)][MpBgp][BgpNe
ighbourEntry(PeerIdentifier=10.0.7.4)(VrfName=Red)]}
```

Carrier Grade NAT OID (ICgnServiceOid)

The Carrier Grade NAT OID is the source OID for Carrier Grade NAT alarms.

The structure of the Carrier Grade NAT OID is:

{[ManagedElement(Key=deviceIP)][LogicalRoot][FWComponentContainer(Type=10)][CgnService(CgnName=CgnInstanceName)]}

Example

```
{[ManagedElement(Key=169.254.192.135)][LogicalRoot][FWComponentContainer(Type=10)]
[CgnService(CgnName=demo)]}
```

Chassis Oid (ChassisId)

The Chassis OID is the source OID for any alarms related to a chassis in a network element.

The structure of the Chassis OID is:

{[ManagedElement(Key=VNE_NAME)][PhysicalRoot][Chassis(ChassisId=”0”)]}

Example

```
{[ManagedElement(Key=UCS)][PhysicalRoot][Chassis(ChassisId="sys/switch-A")]}
```

DS0 Bundle OID (IDS0BundleOid)

The DS0 Bundle OID is the source OID for any alarms related to DS0 Bundle.

The alarm supported by Prime Network with DS0 Bundle OID source OID is:

- DS0 Bundle Down

The structure of the DS0 Bundle OID is:

{[ManagedElement(Key=mlppp-*mlppp number*)][PhysicalRoot][Chassis][Slot(SlotNum=*slot number*)][Module][Slot(SlotNum=*shot number*)][Module][Port(PortNumber=*port number*)][PhysicalLayer][Lop(Id=*identifier*)][DS0Bundle(BundleLocation=Bundle:*location*)(Id=*identifier*)]}

Example

```
{[ManagedElement(Key=mlppp-2)][PhysicalRoot][Chassis][Slot(SlotNum=4)][Module][Slot(SlotNu
m=3)][Module][Port(PortNumber=T3
4/3/0)][PhysicalLayer][Lop(Id=14)][DS0Bundle(BundleLocation=Bundle:
Serial4/3/0/14:0)(Id=0)]}
```

DS1 Path OID (IDS1PathOid)

The DS1 Path OID is the source OID for any alarms related to DS1 port and link down.

Alarms supported by DS1 Path OID include:

- DS1 Path Port Down
- DS1 Path Link Down

The structure of the DS1 Path OID is:

{[ManagedElement(Key=*element key*)][PhysicalRoot][Chassis][Slot(SlotNum=*slotnumber*)][Module \][Slot(SlotNum=*slotnumber*)][Module][Port(PortNumber=*portnumber*][PhysicalLayer][Sonet_SdhHop(Id=*hop identifier*)][Lop(Id=*LOP ID*)]}

Example

```
{[ManagedElement(Key=ana-dev-7609-1)][PhysicalRoot][Chassis][Slot(SlotNum=8)][Module \
][Slot(SlotNum=1)][Module][Port(PortNumber=SONET                                    \
8/1/0)][PhysicalLayer][Sonet_SdhHop(Id=3)][Lop(Id=3/5/3)]}
```

DS3 Path OID (IDS3PathOid)

The DS3 Path OID is the source OID for any alarms related to DS3 port down.

Alarms supported by DS3 Path OID include:

- DS3 Path Port Down
- DS3 Path Link Down

The structure of the DS3 Path OID is:

{[ManagedElement(Key=*element key*)][PhysicalRoot][Chassis][Slot(SlotNum=*slotnumber*)][Module \][Slot(SlotNum=*slotnumber*)][Module][Port(PortNumber=*portnumber*][PhysicalLayer][Sonet_SdhHop(Id=*hop identifier*)][Lop(Id=*LOP ID*)]}

Example

```
{[ManagedElement(Key=ana-dev-7609-1)][PhysicalRoot][Chassis][Slot(SlotNum=8)][Module \
][Slot(SlotNum=1)][Module][Port(PortNumber=SONET                                    \
8/1/0)][PhysicalLayer][Sonet_SdhHop(Id=3)][Lop(Id=3/5/3)]}
```

DWDM Controller OID (IDWDMOid)

The DWDM Controller OID is the IMO class of the DWDM controller. Alarms supported with the DWDM Controller OID include:

- DWDM Controller Down
- DWDM G709 Status Down

The structure of the DWDM Controller OID is:

{[ManagedElement(Key=*devicename*)][PhysicalRoot][Chassis][Shelf(ShelfNum=*shelfnumber*)][Slot(SlotNum=*slotnumber*)][Module][Port(PortNumber=*portnumber*)][PhysicalLayer]}

Example

```
{[ManagedElement(Key=CRS1-simu-41)][PhysicalRoot][Chassis][Shelf(ShelfNum=0)][Slot(SlotNum
=5)][Module][Port(PortNumber=POS0/5/0/0)][PhysicalLayer]}
```

EFP OID (IEFPOID)

The structure of the EFP OID is:

{[ManagedElement(Key=*deviceName*)][LogicalRoot][FWComponentContainer(Type=7)][MpBgp][BgpNeighbourEntry(PeerIdentifier=*peerIP*)(VrfName=*vrfName*)]}

Example

```
{[ManagedElement(Key=PE3-NY-7300)][LogicalRoot][FWComponentContainer(Type=7)][MpBgp][BgpNe
ighbourEntry(PeerIdentifier=10.0.7.4)(VrfName=Red)]}
```

Fan Tray OID

The Fan Tray OID supports the Fan Tray service alarm. The structure of the Fan Tray OID is:

{[ManagedElement(Key=ASR1K)][PhysicalRoot][Chassis][Slot(SlotNum=Fan)][Module][Slot(SlotN
um= Slot Fan 0)][FanTray]}

IMA Service (IIMAGroupOid)

The IMA Service OID supports the ATM IMA Service alarm. The structure of the IMA Service OID is:

IIMAGroupOid:
{[ManagedElement(Key=*ManagedElementkey*)][LogicalRoot][PhysicalLayerAggregationContainer(Ty
pe=*type*)][IMAGroup(Id=*IMAGroupID*)]}

Example

```
{[ManagedElement(Key=vne-146)][LogicalRoot][PhysicalLayerAggregationContainer(Type=1)][IMA
Group(Id=ATM8/1/ima10)]}
```

IP Interface OID (IPInterfaceOid)

The IP Interface OID is the source OID for any alarms related to the IP interface.

Alarms supported by Prime Network with IP Interface source OID are:

- Interface Status
- HSRP Group Status Changed
- Dual Stack IP Changed

The structure of the IP Interface OID can be one of the following:

- IP interface under the global routing (RoutingEntity):

  {[ManagedElement(Key=*deviceName*)][LogicalRoot][FWComponentContainer(Type=1)][Routing
  Entity][IpInterface(IpInterfaceName=*ifName*)]}

- IP interface under a VRF:

  {[ManagedElement(Key=*deviceName*)][LogicalRoot][FWComponentContainer(Type=*3*)][Vrf(Vrf
  Name=*vrfName*)][IpInterface(IpInterfaceName=*ifName*)]}

Examples

IP Interface OID under the RoutingEntity:

```
{[ManagedElement(Key=PE2-TX-GSR)][LogicalRoot][FWComponentContainer(Type=1)][RoutingEntity
][IpInterface(IpInterfaceName=POS0/0)]}
```

IP Interface OID under a VRF:

```
{[ManagedElement(Key=PE-South)][LogicalRoot][FWComponentContainer(Type=3)][Vrf(VrfName=vrf
A)][IpInterface(IpInterfaceName=Serial2/0.400)]}
```

Lag Down OID

The Lag Down OID is the source OID for Lag Down Alarm.

Example

```
{[ManagedElement(Key=169.254.77.108)][LogicalRoot][Context(ContextName=Default
context)][DataLinkAggregationContainer(Type=1)][DataLinkAggregation(Index=11)]} .
```

Lag Link Down OID

The Lag Link Down OID is the source OID for the Lag Link alarm. The OID is a topological link with A and Z side endpoints similiar to Lag Down OID.

L2TP Peer OID (IL2tpPeerOid)

Layer 2 Tunneling Protocol (L2TP) modeling in Prime Network is available only for Redback SMS devices. L2TP Peer is a component that is used to model the administrative aspect of L2TP tunnels. It is basically an entity responsible for creating L2TP tunnels based on its configuration.

The L2TP Peer OID is the source OID for any alarms related to L2TP Peer components.

Alarms supported by Prime Network with L2TP Peer source OID are:

- L2TP Peer Not Established
- L2TP Session Threshold

The structure of the L2TP Peer OID is:

{[ManagedElement(Key=*deviceName*)][LogicalRoot][Context(ContextName=*contextName*)][FWComponentContainer(Type=6)][L2tpPeer(PeerName=*peerName*)]}

Example

```
{[ManagedElement(Key=redback)][LogicalRoot][Context(ContextName=l2tpCtx)][FWComponentConta
iner(Type=6)][L2TPPeer(PeerName=peer5)]}
```

Local Switching Entry Down OID

Local Switching Entry Down OID is the source OID for Local Switching Entry Down alarm.

Example

```
Oid: {[ManagedElement(Key=169.254.77.108)][LogicalRoot][Context(ContextName=Default
context)][FWComponentContainer(Type=8)][LocalSwitchingEntity]}
```

with DiffObject as the LocalSwitchingEntryKey

Logical Port OID (ILogicalPortOid)

A logical port represents a logical ATM/FrameRelay interface which is configured on top of a physical port. One physical port might have multiple logical ports. In ATM, logical ports are differentiated by VP muxing, that is, each logical port is configured with a range of VPIs. This type of configuration exists in Lucent GX/CBX, which are supported by Prime Network.

The Logical Port OID is the source OID for any alarms related to logical ports.

The alarm supported by Prime Network with the Logical Port source OID is:

- Logical Port Down

The structure of the Logical Port OID can be one of the following:

- Logical port on a module's physical port:

  {[ManagedElement(Key=*deviceName*)][PhysicalRoot][Chassis][Slot(SlotNum=*slotNum*)][Module][Port(PortNumber=*portNum*)][PhysicalLayer][VpMux][LogicalPort(LogicalPortNumber=*logicalPortNum*)]}

- Logical port on a submodule's physical port:

  {[ManagedElement(Key=*deviceName*)][PhysicalRoot][Chassis][Slot(SlotNum=*slotNum*)][Module][Slot(SlotNum=*subSlotNum*)][Module][Port(PortNumber=*portNum*)][PhysicalLayer][VpMux][LogicalPort(LogicalPortNumber=*logicalPortNum*)]}

- Logical port of a subport:

  {[ManagedElement(Key=*deviceName*)][PhysicalRoot][Chassis][Slot(SlotNum=*slotNum*)][Module][Port(PortNumber=*portNum*)][PhysicalLayer][SubPort(SubPortNumber=*subPortNumber*)][VpMux][LogicalPort(LogicalPortNumber=*logicalPortNum*)]}

LSP Endpoint OID (LSP EndPoint OID)

The LSP Endpoint OID is used as the source OID for any alarms related to LSP entries.

The alarms supported by Prime Network with the LSP Endpoint OID is:

- LSP Down
- LSP down due to label mismatch
- LSP down due to lock out
- LSP up

The structure of the LSP EndPoint OID is:

{[ManagedElement(Key=device IP)][LogicalRoot][Context(ContextName=Default context)][FWComponentContainer(Type=14)][MPLSTPGlobal][LSPEPEntry(Identifier)]}

Example

```
{[ManagedElement(Key=172.23.222.233)][LogicalRoot][Context(ContextName=Default
context)][FWComponentContainer(Type=14)][MPLSTPGlobal][LSPEPEntry(InternalId=111::10.1.99.
1::1019::111::10.3.99.1::1019::1)]}
```

LSE Entry OID (IMplsEntryOid)

The LSE Entry OID is used as the source OID for any alarms related to LSE entries.

The alarm supported by Prime Network with the LSE Entry source OID is:

- Broken LSP Discovered

The structure of the LSE Entry OID is:

{[ManagedElement(Key=*deviceName*)][LogicalRoot][FWComponentContainer(Type=4)][Lse][LSEEntries(InLabel=*inLabel*)][MplsEntry(OutInterface=*outIfOid*)]}

The OutInterface is the IP interface OID of the outgoing interface.

Example

```
{[ManagedElement(Key=PE1-NY-GSR)][LogicalRoot][FWComponentContainer(Type=4)][Lse][LSEEntries(InLabel=74)][MplsEntry(OutInterface={[ManagedElement(Key=PE1-NY-GSR)][LogicalRoot][FWComponentContainer(Type=1)][RoutingEntity][IpInterface(IpInterfaceName=POS0/0)]})]}
```

Note The structure of the OutInterface is a separate OID.

LSE OID (ILseOid)

The Label Switching Entity (LSE) OID is used as the source for various alarms related to MPLS.

Alarms supported by Prime Network with LSE OID are:

- MPLS Black Hole Found
- MPLS Interface Removed
- LDP Neighbor Loss

The structure of the LSE OID is:

{[ManagedElement(Key=*deviceName*)][LogicalRoot][FWComponentContainer(Type=4)][Lse]}

Alarm Differentiators

Multiple alarms of the same type cannot have the same source. When this occurs, then the LSE OID is used as a base OID and is augmented with a differentiator. A specific alarm differentiator is used for each type of alarm.

The following examples show how specific alarm differentiators are used in the different types of alarms:

Example 1

MPLS Black Hole Found—[ServiceEvent(DiffObject=*ifName nextHop*)]

Source OIDs of MPLS Black Hole Found:

```
{[ManagedElement(Key=RR1-IOU)][LogicalRoot][FWComponentContainer(Type=4)][Lse][ServiceEvent(DiffObject=Ethernet0/0 192.168.1.210)]}

{[ManagedElement(Key=RR1-IOU)][LogicalRoot][FWComponentContainer(Type=4)][Lse][ServiceEvent(DiffObject=Ethernet0/0 192.168.1.310)]}
```

Example 2

MPLS Interface Removed—[ServiceEvent(DiffObject=*mplsIfDescr*)]

Source OIDs of MPLS Interface Removed:

```
{[ManagedElement(Key=PE4-NY-7200)][LogicalRoot][FWComponentContainer(Type=4)][Lse][Service
Event(DiffObject=MPLS on interface FastEthernet0/1)]}

{[ManagedElement(Key=PE4-NY-7200)][LogicalRoot][FWComponentContainer(Type=4)][Lse][Service
Event(DiffObject=MPLS on interface FastEthernet0/2)]}
```

Example 3

LDP Neighbor Loss—[ServiceEvent(DiffObject=*peerLdpId*)]

Source OIDs of LDP Neighbor Loss:

```
{[ManagedElement(Key=CORE2-NY-GSR)][LogicalRoot][FWComponentContainer(Type=4)][Lse][Servic
eEvent(DiffObject=172.255.0.1:0)]}

{[ManagedElement(Key=CORE2-NY-GSR)][LogicalRoot][FWComponentContainer(Type=4)][Lse][Servic
eEvent(DiffObject=172.255.0.1:5)]}
```

Managed Element OID (IManagedElementOid)

Managed Element represents the root component of the VNE. Any alarm related to the top-level component of the VNE will have the Managed Element OID as the source.

Alarms which have Managed Element OID as their source are:

- Device Unreachable
- Device Unsupported
- CPU Overutilized
- Module Unsupported (Investigation State)
- Adaptive Polling
- Cloud Problem (for cloud VNEs)

The structure of the Managed Element OID is:

{[ManagedElement(Key=*deviceName*)]}

Example

```
{[ManagedElement(Key=PE4-NY-7200)]}
```

Members Changed OID (IDataLinkAggregationOid)

The Members Changed OID is used as a source OID for service aggregation alarms.

The structure of the Members Changes OID is:

{[ManagedElement(Key=*deviceName*)][LogicalRoot][Context(ContextName=*contextName*)][DataLinkAggregationContainer(*Type=1*)][DataLinkAggregation(Index=*snmpIndex*)]}

Example

```
{[ManagedElement(Key=vne-146)][LogicalRoot][Context(ContextName=Default
context)][DataLinkAggregationContainer(Type=1)][DataLinkAggregation(Index=50)]}
```

MLPPP OID (IMLPPPOid)

The MLPPP OID is the source OID for any alarms related to MLPPP. The structure of the MLPPP OID is:

{[ManagedElement(Key=mlppp-*key*)][LogicalRoot][Context(ContextName=Default context)] [EncapsulationAggregationContainer(Type=*type*)][EncapsulationAggregation(Group=*group*)]}

Example

```
{[ManagedElement(Key=mlppp-2)][LogicalRoot][Context(ContextName=Default
context)][EncapsulationAggregationContainer(Type=1)][EncapsulationAggregation(Group=200)]}
```

Module OID (IModuleOid)

The Module OID is the source OID for any alarms related to a card or module.

Alarms which have Module OID as their source are:

- Card Out
- Card Down

Possible structures of the Module OIDs are:

- Module under chassis:

  {[ManagedElement(Key=*deviceName*)][PhysicalRoot][Chassis][Shelf(ShelfNum=*shelfNum*)][Slot (SlotNum=*slotNum*)][Module]}

- Module under other module (submodule):

  {[ManagedElement(Key=*deviceName*)][PhysicalRoot][Chassis][Shelf(ShelfNum=*shelfNum*)][Slot (SlotNum=*slotNum*)][Module][Slot(SlotNum=*subSlotNum*)][Module]}

Shelf is an optional part of the OID.

Example

```
{[ManagedElement(Key=CRS-1)][PhysicalRoot][Chassis][Shelf(ShelfNum=0)][Slot(SlotNum=4
-Back)][Module][Slot(SlotNum=10)][Module]}
```

MPBGP OID (IMpBgpOid)

The MPBGP OID will be the source OID for any alarms related to BGP service.

The alarm supported by Prime Network with MPBGP source OID is:

- BGP Process Down

The structure of the MPBGP OID is:

{[ManagedElement(Key=*deviceName*)][LogicalRoot][FWComponentContainer(Type=7)][MpBgp]}

Example

```
{[ManagedElement(Key=Juniper M5)][LogicalRoot][FWComponentContainer(Type=7)][MpBgp]}
```

MPLS TE Tunnel OID (IMplsTETunnelOid)

The MPLS TE Tunnel OID is the source OID for any alarms related to MPLS TE tunnels.

The alarm supported by Prime Network with MPLS TE Tunnel source OID is:

- MPLS TE Tunnel Down

The structure of the MPLS TE Tunnel OID is:

{[ManagedElement(Key=*deviceName*)][LogicalRoot][FWComponentContainer(Type=1)][RoutingEntity][IpInterface(IpInterfaceName=*ifName*)][MplsTETunnel]}

Example

```
{[ManagedElement(Key=CRS1-PE)][LogicalRoot][FWComponentContainer(Type=1)][RoutingEntity][IpInterface(IpInterfaceName=tunnel-te0)][MplsTETunnel]}
```

Note The structure of the OID is different when the IP interface is under a VRF (see IP Interface OID (IPInterfaceOid), page 15-200).

TP Tunnel Endpoint OID (TP Tunnel EndPoint OID)

The TP Tunnel Endpoint OID is the source OID for any alarms related to MPLS TP tunnels:

The alarm supported by Prime Network with MPLS TP Tunnel source OID is:

- TP Tunnel Down Due to Admin Down
- TP Tunnel Down to Oper Down

The structure of the TP Tunnel End Point OID is:

{[ManagedElement(Key=device-IP)][LogicalRoot][Context(ContextName=Default context)][FWComponentContainer(Type=Value)][MPLSTPGlobal][MPLSTPTunnelEP(TunnelId=Value]}

Example

```
{[ManagedElement(Key=172.23.222.233)][LogicalRoot][Context(ContextName=Default context)][FWComponentContainer(Type=14)][MPLSTPGlobal][MPLSTPTunnelEP(TunnelId=1014)]}
```

ISyncEOID

The ISyncEOID is the source OID for any alarms related to network synchronization.

The alarms supported by Prime Network with ISyncEOID is:

- Network-Clock Synchronization Disabled
- Network-Clock Synchronization Enabled
- Esmc Process Up
- Esmc Process Down

The structure of the ISyncEOID is:

{[ManagedElement(Key=Device IP)][LogicalRoot][Context(ContextName=Default context)][ClockService][SyncE]}

Example

```
{[ManagedElement(Key=172.25.106.53)][LogicalRoot][Context(ContextName=Default
context)][ClockService][SyncE]}
```

OSPF Neighbor State Change OID

The OSPF Neighbor State Change OID is the source OID for the OSPF Neighbor Up and the OSPF Neighbor Down alarms. The OID of the Members Changed alarm is the OID of the affected Neighbor.

Example

```
{[ManagedElement(Key=172.25.87.145)][LogicalRoot][FWComponentContainer(Type=11)][OspfProce
ss(OspfVersion=v2)(ProcessId=1)][OspfNeighbor(AreaId=0)(IfName=TenGigabitEthernet2/4)(Ospf
NeighborId=10.10.20.3)]}
```

Port OID

The Port OID is the source OID for Pluggable transceiver alarms.

The structure of the Port OID is:

{[ManagedElement(Key=c4-npe1-76)][PhysicalRoot][Chassis][Slot(SlotNum=4)][Module][Slot(SlotNum=0)][Module][Port(PortNumber=GigabitEthernet4/0/6)]}

Power Supply OID

The Power Supply OID is the source OID for Power supply alarms.

The structure of the Power Supply OID is:

{[ManagedElement(Key=ASR1K)][PhysicalRoot][Chassis][Slot(SlotNum=Power)][Module][Slot(SlotNum=0)][PowerSupply]}

Physical Layer OID (IPhysicalLayerOid)

The Physical Layer OID is the source OID for any alarm related to the physical layer of a port.

Alarms which have Physical Layer OID as their source are:

- Port Down
- Tx/Rx Utilization (no adjacent)
- Tx/Rx Dormant
- Dropped/Discarded Packets
- All IP Interfaces Down

The structure of the Physical Layer OID is:

{[ManagedElement(Key=*deviceName*)][PhysicalRoot][Chassis][Shelf(ShelfNum=*shelfNum*)][Slot(SlotNum=*slotNum*)][Module][Slot(SlotNum=*subSlotNum*)][Module][Port(PortNumber=*portNum*)][PhysicalLayer]}

Optional parts of the OID are:

- Shelf
- Second-level slot
- Module representing submodule

PortNum can also be the port name (see the following examples).

Examples

Source of port down where the port is on a submodule:

```
{[ManagedElement(Key=CRS-1)][PhysicalRoot][Chassis][Shelf(ShelfNum=0)][Slot(SlotNum=4
-Back)][Module][Slot(SlotNum=4)][Module][Port(PortNumber=GigabitEthernet0/4/4/1)][Physical
Layer]}
```

Shelf OID (IShelfOid)

The Shelf OID is the source OID for any alarms related to shelf.

The alarm which has Shelf OID as its source is:

- Shelf Out

The structure of the Shelf OID is:

{[ManagedElement(Key=*deviceName*)][PhysicalRoot][Chassis][Shelf(ShelfNum=*shelfNum*)]}

Example

```
{[ManagedElement(Key=CRS-1)][PhysicalRoot][Chassis][Shelf(ShelfNum=0)]}
```

SONET Path Port Down OID

The Sonet Path Port Down OID is the source OID for SONET Path Port Down alarm.

Example

```
{[ManagedElement(Key=172.25.87.146)][PhysicalRoot][Chassis][Slot(SlotNum=8)][Module][Slot(
SlotNum=1)][Module][Port(PortNumber=SONET 8/1/0)][PhysicalLayer][Sonet_SdhHop(Id=2)]}
```

SONET Path Link Down OID

The SONET Path Link Down OID is the source OID for the SONET Path Link alarm. The OID is a topological link with A and Z side endpoints similiar to SONET Path port Down OID.

Topological Link OID (ITopologicalLinkOid)

The Topological Link OID is the source OID for any Link Down alarm. It has the following structure:

{[TopologicalLink(AEndPoint=*AEndOid*)(TunnelID=*tunnelId*)(ZEndPoint=*ZEndOid*)]}

- AEndOid, ZEndOid—The OIDs of the link endpoint components.
- TunnelID—Where multiple links can exist between two components, the TunnelID value is used to distinguish between the links.

Supported Alarms with Topological Link OID Source

The alarms supported in Prime Network which have Topological Link OID source are:

- Link Down—Link down between physical ports, the endpoint OIDs of the physical layer. In this case, the TunnelId is not used and is set to -1. See Link Down Endpoint OID Structure, page 15-209.

Note There are various alarm subtypes of link down (for example, Link Down to Admin Down, and Link Down on Unreachable). They all have the same source OID.

- Link Utilization—The source OID is the same as for link down.
- Tx/Rx Utilization—The source OID is the same as for link down where the physical layer component is adjacent.
- GRE Tunnel Down—The endpoint OIDs are the GRE tunnel endpoints. In this case, the TunnelID is not used and is set to -1. See GRE Tunnel Endpoint OID Structure, page 15-210.
- Layer 2 Tunnel Down—The endpoint OIDs are the Layer 2 MPLS tunnel endpoints. In this case, the TunnelID is not used, nor is it initialized. See Layer 2 MPLS Tunnel Endpoint OID Structure, page 15-210.
- BGP Link Down—The endpoint OIDs are the MpBGP. In this case, the TunnelID is not used, nor is it initialized. See BGP Link Down Endpoint OID Structure, page 15-210.
- DS1 Path Link Down—See DS1 Path Link Down, page 15-29.
- DS3 Path Link Down—See DS3 Path Link Down, page 15-30.
- MLPPP Down Due to Admin Down—See MLPPP Bundle, page 15-49.
- MLPPP Down Due to Oper Down—See MLPPP Bundle, page 15-49.

Link Down Endpoint OID Structure

The structure of the Link Down Endpoint OID is:

{[ManagedElement(Key=*deviceName*)][PhysicalRoot][Chassis][Shelf(ShelfNum=*shelfNum*)][Slot(SlotNum=*slotNum*)][Module][Slot(SlotNum=*subSlotNum*)][Module][Port(PortNumber=*portNum*)][PhysicalLayer]}

Optional parts of the Link Down Endpoint OID are:

- Shelf
- Second-level slot
- Module representing a submodule

PortNum can also be the port name (see the following examples).

Examples

Source of link down where the physical ports are on a module:

```
{[TopologicalLink(AEndPoint={[ManagedElement(Key=PE3-NY-7300)][PhysicalRoot][Chassis][Slot
(SlotNum=1)][Module][Port(PortNumber=FastEthernet1/1)][PhysicalLayer]})(TunnelID=-1)(ZEndP
oint={[ManagedElement(Key=PE1-NY-GSR)][PhysicalRoot][Chassis][Slot(SlotNum=1)][Module][Slo
t(SlotNum=1)][Module][Port(PortNumber=GigabitEthernet1/1/2)][PhysicalLayer]})]}
```

Source of link down where the physical port of AendPoint is on a submodule:

```
{[TopologicalLink(AEndPoint={[ManagedElement(Key=PE1-NY-GSR)][PhysicalRoot][Chassis][Slot(
SlotNum=1)][Module][Slot(SlotNum=1)][Module][Port(PortNumber=GigabitEthernet1/1/1)][Physic
alLayer]})(TunnelID=-1)(ZEndPoint={[ManagedElement(Key=NPE1-NY-7600)][PhysicalRoot][Chassi
s][Slot(SlotNum=4)][Module][Port(PortNumber=FastEthernet4/48)][PhysicalLayer]})]}
```

See also, DS3 Path OID (IDS3PathOid), page 15-199, DS3 Path OID (IDS3PathOid), page 15-199, MLPPP OID (IMLPPPOid), page 15-205.

GRE Tunnel Endpoint OID Structure

The structure of the GRE Tunnel Endpoint OID is:

{[ManagedElement(Key=*deviceName*)][LogicalRoot][Context(ContextName=*contextName*)][TunnelContainer(TunnelType=*4*)][TunnelGre(TunnelName=*tunnelName*)]}

Examples

Source of GRE Tunnel Down alarm:

```
{[TopologicalLink(AEndPoint={[ManagedElement(Key=PE-East-IOU-158)][LogicalRoot][Context(Co
ntextName=Default
context)][TunnelContainer(TunnelType=4)][TunnelGre(TunnelName=Tunnel1)]})(TunnelID=-1)(ZEn
dPoint={[ManagedElement(Key=PE-South-IOU-158)][LogicalRoot][Context(ContextName=Default
context)][TunnelContainer(TunnelType=4)][TunnelGre(TunnelName=Tunnel1)]})]}
```

Layer 2 Tunnel Down—The endpoint OIDs are the Layer 2 MPLS tunnel endpoints. In this case, the TunnelID is not used and is not initialized.

Layer 2 MPLS Tunnel Endpoint OID Structure

The structure of the Layer 2 MPLS Tunnel Endpoint OID is:

{[ManagedElement(Key=*deviceName*)][LogicalRoot][Context(ContextName=*contextName*)][TunnelContainer(TunnelType=*1*)][PTPLayer2MplsTunnel(PeerRouterIp=*peerRouterIP*)(TunnelId=*tunnelId*)]}

Example

Source of Layer 2 Tunnel Down:

```
{[TopologicalLink(AEndPoint={[ManagedElement(Key=NPE1-NY-7600)][LogicalRoot][Context(Conte
xtName=Default
context)][TunnelContainer(TunnelType=1)][PTPLayer2MplsTunnel(PeerRouterIp=172.255.1.5)(Tun
nelId=100)]})(TunnelID=)(ZEndPoint={[ManagedElement(Key=PE4-NY-7200)][LogicalRoot][Context
(ContextName=Default
context)][TunnelContainer(TunnelType=1)][PTPLayer2MplsTunnel(PeerRouterIp=172.255.1.3)(Tun
nelId=100)]})]}
```

BGP Link Down Endpoint OID Structure

The structure of the MpBGP Link Down Endpoint OID is:

{[ManagedElement(Key=*deviceName*)][LogicalRoot][FWComponentContainer(Type=7)][TunnelId=*tunnelId*)]}

Example

Source of BGP Link Down:

```
{[TopologicalLink(AEndPoint={[ManagedElement(Key=PE-East-IOU-159)][LogicalRoot][FWComponen
tContainer(Type=7)][MpBgp]})(TunnelID=-1)(ZEndPoint={[ManagedElement(Key=RR2-IOU-159)][Log
icalRoot][FWComponentContainer(Type=7)][MpBgp]})]}
```

VLAN Tagged Interface OID (IVlanTaggedInterfaceOID)

The VLAN Tagged Interface OID is used as the source OID for alarms related to QinQ or stacked VLANs, such as Subinterface Down.

A subinterface is a logical division of traffic on an interface, such as multiple subnets across one physical interface. A subinterface name is represented as an extension to an interface name using dot notation, such as Interface Gigabit Ethernet 0/1/2/3.10. In this example, the main interface name is Gigabit Ethernet 0/1/2/3 and the subinterface is 10.

The structure of the VLAN Tagged Interface OID is:

{[ManagedElement(Key=*deviceName*)][PhysicalRoot][Chassis][Slot(SlotNum=*slotNum*)][Module][Slot(SlotNum=*subSlotNum*)][Module][Port(PortNumber=*portNum*)][PhysicalLayer][DataLinkLayer][VlanEncapMux][VLANTaggedInterface(InterfaceName=*subInterfaceName*)]}

Example

```
{[ManagedElement(Key=10.56.101.133)][PhysicalRoot][Chassis][Slot(SlotNum=4)][Module][Slot(
SlotNum=0)][Module][Port(PortNumber=GigabitEthernet4/0/2)][PhysicalLayer][DataLinkLayer][V
lanEncapMux][VLANTaggedInterface(InterfaceName=Gi4/0/2.1)]}
```

VSI OID (IVSIOID)

The VSI OID is used as a source for VSI IMOs and VSI alarms including VSI Admin Down, VSI Down, and VSI Up.

The VSI OID is structured so that the VPLS name and VPN ID are identifiers for the VSI entity concatenated to the logical context OID.

Example

```
[ManagedElement(Key=7606S-PE1)][LogicalRoot][Context(ContextName=Default
context)][FWComponentContainer(Type=10)] [VSI(VplsInstanceName=eli_VFI)(VpnId=101)]}
```



CHAPTER 16

Traps

This section describes the Prime Network traps. Traps appear in the Cisco Prime Network Events V1 Trap, V2 Trap, and V3 Trap tabs. (For information about Prime Network Events, see the *Cisco Prime Network 3.9 User Guide.)* Trap information is presented in two forms:

- Trap Tables—A section devoted to the supported traps for for both versions V1 and V2 (for example, Cisco IOS V1 Traps and Cisco IOS V2/V3 Traps). Each of these sections contains a table listing the name of each Prime Network-supported trap in that MIB, along with its OID, varbinds, and a short description. The trap's Short Description is what you see in a ticket's Trap tabs in Prime Network Events 3.9. In the trap tables in this Reference guide, each trap's Short Description is also a link to the trap's corresponding parameters.
- Registry Parameter Tables—A section devoted to the event types, event subtypes and Prime Network registry parameters for the traps supported in each MIB. There is one parameter table for every trap table (for example, Cisco IOS V1 Trap Registry Parameters). Each trap event can have multiple event subtypes, or states. The parameter tables indicate when each trap state is generated, and how Prime Network processes them (such as their severity, and whether they are ticketable, can be correlated, are autocleared, and so on).

Please note that SNMP V2 and V3 trap information is identical; the only difference is the transport and encryption options for each version. Prime Network natively supports SNMP informs and SNMP V3 AuthNoPriv and AuthPriv options.

Cisco Prime Network 3.9 users can enable an additional IP address in the device for traps and syslogs other than the device management IP address. This new feature is called Multisource Events. When Cisco Prime Network 3.9 receives a trap or syslog from that device (from the new IP) it will still recognize the device.

This chapter includes the following sections:

- Cisco ASR 9000 V1 Traps, page 16-3
- Cisco ASR 9000 V2/V3 Traps, page 16-4
- Cisco IOS V1 Traps, page 16-6
- Cisco IOS V2/V3 Traps, page 16-61
- Cisco IOX V1 Traps, page 16-89
- Cisco IOX V2/V3 Traps, page 16-103
- Cisco MIB2 V1 Traps, page 16-119
- Cisco MIB2 V2/V3 Traps, page 16-129
- Cisco ACE V1 Traps, page 16-138
- Cisco ACE V2/V3 Traps, page 16-140

- Cisco Nexus V1 Traps, page 16-141
- Cisco Nexus V2/V3 Traps, page 16-154
- Cisco CPT V2 Traps, page 16-160
- Cisco ASR 5000 Series V2 Traps, page 16-161
- Cisco Unified Computing System V2 Traps, page 16-186
- Cisco ASR 1000 V2 Traps, page 16-197
- Cisco ASR 9000 V1 Trap Registry Parameters, page 16-197
- Cisco ASR 9000 V2/V3 Registry Parameters, page 16-198
- Cisco IOS V1 Trap Registry Parameters, page 16-199
- Cisco IOS V2/V3 Trap Registry Parameters, page 16-223
- Cisco IOX V1 Trap Registry Parameters, page 16-244
- Cisco IOX V2/V3 Trap Registry Parameters, page 16-253
- Cisco MIB2 V1 Trap Registry Parameters, page 16-263
- Cisco MIB2 V2/V3 Trap Registry Parameters, page 16-270
- Cisco ACE V1 Trap Registry Parameters, page 16-278
- Cisco ACE V2/V3 Trap Registry Parameters, page 16-279
- Cisco Nexus V1 Trap Registry Parameters, page 16-280
- Cisco Nexus V2/V3 Trap Registry Parameters, page 16-284
- Cisco CPT V2 Trap Registry Parameters, page 16-288
- Cisco ASR 5000 Series V2 Trap Registry Parameters, page 16-289
- Cisco Unified Computing System V2 Trap Registry Parameters, page 16-311
- Cisco ASR 1000 V2 Trap Registry Parameters, page 16-322

Note Cisco IOS devices, Cisco XR 12000 Series and the Cisco CRS Carrier Routing System must be configured to send traps in SNMP V2. Cisco CRS series includes Cisco CRS-1 and Cisco CRS-3 Carrier Routing Systems.

Cisco ASR 9000 V1 Traps

Table 16-1 lists the Cisco ASR 9000 SNMP V1 traps supported in Prime Network. For associated event types, event subtypes, and Prime Network registry parameters, use the link under Short Description or see Table 16-17.

Table 16-1 Cisco ASR 9000 V1 Traps

Trap Name	Generic Type	Specific Type	Enterprise OID	Subtype Varbind OID	Subtype Varbind Value	Description	Short Description
dot1agCfmFaultAlarm	6	1	1.0.8802.1.1.3,1.3.111.2.802.1.1.8.1.7.1.1.13	1.3.111.2.802.1.1.8.1.7.1.1.13	!=1	A MEP has lost contact with one or more MEPs. A notification (fault alarm) is sent to the management entity with the OID of the MEP that has detected the fault. Whenever a MEP loses contact with one or more other MEPs, it may or may not generate a Fault Alarm to warn the system administrator of the problem, as controlled by the MEP Fault Notification Generator State Machine and associated Managed Objects. Only the highest-priority defect, as shown in Table 20-1, is reported in the Fault Alarm. 802.1ag clause 12.14.7.7.	dot1ag CFM Fault Alarm
dot1agCfmFaultAlarm	6	1	1.0.8802.1.1.3,1.3.111.2.802.1.1.8.1.7.1.1.13	1.3.111.2.802.1.1.8.1.7.1.1.13	1	A MEP has lost contact with one or more MEPs. A notification (fault alarm) is sent to the management entity with the OID of the MEP that has detected the fault. Whenever a MEP loses contact with one or more other MEPs, it may or may not generate a Fault Alarm to warn the system administrator of the problem, as controlled by the MEP Fault Notification Generator State Machine and associated Managed Objects. Only the highest-priority defect, as shown in Table 20-1, is reported in the Fault Alarm. 802.1ag clause 12.14.7.7.	dot1ag CFM Fault Alarm

Cisco ASR 9000 V2/V3 Traps

Table 16-2 lists the Cisco ASR 9000 SNMP V2/V3 traps supported in Prime Network. For associated event types, event subtypes, and Prime Network registry parameters, use the link in the Short Description column or see Table 16-18.

Table 16-2 Cisco ASR 9000 V2 Traps

Trap Name	Trap OID	Subtype Varbind OID	Subtype Varbind Value	Description	Short Description
ciscoNtpSrvStatusChange	.1.3.6.1.4.1.9.9.168.0.1	1.3.6.1.4.1.9.9.168.1.1.11	=1	Sent whenever the value of cntpSysSrvStatus changes.	NTP Server Status Changes to Unknown
ciscoNtpSrvStatusChange	.1.3.6.1.4.1.9.9.168.0.1	1.3.6.1.4.1.9.9.168.1.1.11	=2	Sent whenever the value of cntpSysSrvStatus changes.	NTP Server Status Changes to notRunning
ciscoNtpSrvStatusChange	.1.3.6.1.4.1.9.9.168.0.1	1.3.6.1.4.1.9.9.168.1.1.11	=3	Sent whenever the value of cntpSysSrvStatus changes.	NTP Server Status Changes to notSynchronized
ciscoNtpSrvStatusChange	1.3.6.1.4.1.9.9.168.0.1	1.3.6.1.4.1.9.9.168.1.1.11	=4	Sent whenever the value of cntpSysSrvStatus changes.	NTP Server Status Changes to syncToLocal
ciscoNtpSrvStatusChange	1.3.6.1.4.1.9.9.168.0.1	1.3.6.1.4.1.9.9.168.1.1.11	=5	Sent whenever the value of cntpSysSrvStatus changes.	NTP Server Status Changes to syncToRefclock
ciscoNtpSrvStatusChange	1.3.6.1.4.1.9.9.168.0.1	1.3.6.1.4.1.9.9.168.1.1.11	=6	Sent whenever the value of cntpSysSrvStatus changes.	NTP Server Status Changes to syncToRemoteServer
topologyChange	1.3.6.1.2.1.17.0.2	N/A	N/A	Sent by a bridge when any of its configured ports transitions from the Learning state to the Forwarding state, or from the Forwarding state to the Blocking state. The trap is not sent if a newRoot trap is sent for the same transition. Implementation of this trap is optional.	Spanning Tree Topology Changed
warmStart	1.3.6.1.6.3.1.1.5.2	N/A	N/A	A warmStart trap signifies that the SNMP entity,supporting a notification originator application,is reinitializing itself such that its configuration is unaltered.	Warm start trap

Table 16-2 Cisco ASR 9000 V2 Traps (continued)

Trap Name	Trap OID	Subtype Varbind OID	Subtype Varbind Value	Description	Short Description
dot1agCfmFaultAlarm	1.0.8802.1.1.3.0.11.3.111.2.802.1.1.8.0.1	1.3.111.2.802.1.1.8.1.7.1.1.13	!=1	A MEP has lost contact with one or more MEPs. A notification (fault alarm) is sent to the management entity with the OID of the MEP that has detected the fault.Whenever a MEP loses contact with one or more other MEPs, it may or may not generate a Fault Alarm to warn the system administrator of the problem, as controlled by the MEP Fault Notification Generator State Machine and associated Managed Objects. Only the highest-priority defect, as shown in Table 20-1, is reported in the Fault Alarm. 802.1ag clause 12.14.7.7.	dot1ag CFM Fault Alarm
dot1agCfmFaultAlarm	1.0.8802.1.1.3.0.11.3.111.2.802.1.1.8.0.1	1.3.111.2.802.1.1.8.1.7.1.1.13	1	A MEP has lost contact with one or more MEPs. A notification (fault alarm) is sent to the management entity with the OID of the MEP that has detected the fault. Whenever a MEP loses contact with one or more other MEPs, it may or may not generate a Fault Alarm to warn the system administrator of the problem, as controlled by the MEP Fault Notification Generator State Machine and associated Managed Objects. Only the highest-priority defect, as shown in Table 20-1, is reported in the Fault Alarm. 802.1ag clause 12.14.7.7.	dot1ag CFM Fault Alarm

Cisco IOS V1 Traps

Table 16-3 lists the Cisco IOS SNMP V1 traps supported in Prime Network. For associated event types, event subtypes, and Prime Network registry parameters, use the link under Short Description or see Table 16-19.

Table 16-3 Cisco IOS V1 Traps

Trap Name	Generic Type	Specific Type	Enterprise OID	Subtype Varbind OID	Subtype Varbind Value	Description	Short Description
ciscoEnvMonTemperatureNotification	6	3	1.3.6.1.4.1.9.9.13.3.0	1.3.6.1.4.1.9.9.13.1.3.1.6	3	Cisco Environment Monitoring Temperature Notification.	Critical Temprature
ciscoEnvMonTemperatureNotification	6	3	1.3.6.1.4.1.9.9.13.3.0	1.3.6.1.4.1.9.9.13.1.3.1.6	1	Cisco Environment Monitoring Temperature Notification.	Normal Temprature
ciscoEnvMonTemperatureNotification	6	3	1.3.6.1.4.1.9.9.13.3.0	1.3.6.1.4.1.9.9.13.1.3.1.6	6	Cisco Environment Monitoring Temperature Notification.	Not Functioning
ciscoEnvMonTemperatureNotification	6	3	1.3.6.1.4.1.9.9.13.3.0	1.3.6.1.4.1.9.9.13.1.3.1.6	5	Cisco Environment Monitoring Temperature Notification.	Not Present
ciscoEnvMonTemperatureNotification	6	3	1.3.6.1.4.1.9.9.13.3.0	1.3.6.1.4.1.9.9.13.1.3.1.6	4	Cisco Environment Monitoring Temperature Notification.	Critical Temprature - Device Shutdown
ciscoEnvMonTemperatureNotification	6	3	1.3.6.1.4.1.9.9.13.3.0	1.3.6.1.4.1.9.9.13.1.3.1.6	2	Cisco Environment Monitoring Temperature Notification.	Temprature Rising
ciscoEnvMonSupplyStatusChangeNotif	6	9	1.3.6.1.4.1.9.9.13.3.0	1.3.6.1.4.1.9.9.13.1.5.1.3	3	Cisco EnvMon Supply State Notification Trap.	Power Supply - Critical
ciscoEnvMonSupplyStatusChangeNotif	6	9	1.3.6.1.4.1.9.9.13.3.0	1.3.6.1.4.1.9.9.13.1.5.1.3	1	Cisco EnvMon Supply State Notification Trap.	Power Supply - Normal
ciscoEnvMonSupplyStatusChangeNotif	6	9	1.3.6.1.4.1.9.9.13.3.0	1.3.6.1.4.1.9.9.13.1.5.1.3	6	Cisco EnvMon Supply State Notification Trap.	Power Supply - Not Functioning
ciscoEnvMonSupplyStatusChangeNotif	6	9	1.3.6.1.4.1.9.9.13.3.0	1.3.6.1.4.1.9.9.13.1.5.1.3	5	Cisco EnvMon Supply State Notification Trap.	Power Supply - Not Present

Table 16-3 Cisco IOS V1 Traps (continued)

Trap Name	Generic Type	Specific Type	Enterprise OID	Subtype Varbind OID	Subtype Varbind Value	Description	Short Description
ciscoEnvMonSuppStatusChangeNotif	6	9	1.3.6.1.4.1.9.9.13.3.0	1.3.6.1.4.1.9.9.13.1.5.1.3	4	Cisco EnvMon Supply State Notification Trap.	Power Supply - Shutdown
ciscoEnvMonSuppStatusChangeNotif	6	9	1.3.6.1.4.1.9.9.13.3.0	1.3.6.1.4.1.9.9.13.1.5.1.3	2	Cisco EnvMon Supply State Notification Trap.	Power Supply - Warning
ciscoEnvMonFanNotification	6	4	1.3.6.1.4.1.9.9.13.3.0	1.3.6.1.4.1.9.9.13.1.4.1.3	!= 1	Cisco private fan down trap.	Fan down trap
ciscoEnvMonFanNotification	6	4	1.3.6.1.4.1.9.9.13.3.0	1.3.6.1.4.1.9.9.13.1.4.1.3	1	Cisco private fan down trap.	Fan up trap
rttMonTimeoutNotification	6	2	1.3.6.1.4.1.9.9.42.2.0	N/A	N/A	Indicates the occurrence of a timeout for an RTT operation.	RTT Operation Timeout
rttMonThresholdNotification	6	3	1.3.6.1.4.1.9.9.42.2.0	N/A	N/A	Indicates the occurrence of a threshold violation for an RTT operation	RTT Operation Threshold Violation
topologyChange	6	2	1.3.6.1.2.1.17	N/A	N/A	Sent by a bridge when any of its configured ports transitions from the Learning state to the Forwarding state, or from the Forwarding state to the Blocking state.	dot1qBridge trap

Table 16-3 Cisco IOS V1 Traps (continued)

Trap Name	Generic Type	Specific Type	Enterprise OID	Subtype Varbind OID	Subtype Varbind Value	Description	Short Description
cEtherCfmCcMepUp	6	1	1.3.6.1.4.1.9.9.461	N/A	N/A	Sent when: • A remote MEP first comes up (i.e., when we receive a CC message from that MEP for the first time) • The device receives a CC message from a MEP for which it has an expired CCDB entry • A CC message is received for a remote MEP for which the device already has a CCDB entry and the port state in the received CC message is different from the cached previous state	Mep up trap
cEtherCfmCcMepDown	6	2	1.3.6.1.4.1.9.9.461	N/A	N/A	Sent when a remote MEP goes down, namely, the entry in CCDB corresponding to this MEP times out or the device receives a CC message with zero hold-time.	Mep down trap
coldStart	6	0	1.3.6.1.2.1.11.0	N/A	N/A	Indicates that the sending protocol entity is reinitializing itself such that the configuration of the agent or the protocol entity implementation may be altered.	Cold start trap

Table 16-3 Cisco IOS V1 Traps (continued)

Trap Name	Generic Type	Specific Type	Enterprise OID	Subtype Varbind OID	Subtype Varbind Value	Description	Short Description
MIB2 V1 link down	2	0	1.3.6.1.6.3.1.1.5	N/A	N/A	Indicates that the sending protocol entity recognizes a failure in one of the communication links represented in the agent's configuration. The Trap-PDU of type linkDown contains as the first element of its variable bindings, the name and value of the ifIndex instance for the affected interface.	SNMP Link down
MIB2 V1 link up	3	0	1.3.6.1.6.3.1.1.5	N/A	N/A	Indicates that the sending protocol entity recognizes that one of the communication links represented in the agent's configuration has come up. The Trap-PDU of type linkUp contains as the first element of its variable-bindings the name and value of the ifIndex instance for the affected interface.	SNMP Link up
imaFailureAlarm	6	1	1.3.6.1.4.1.353.5.7.1.2	1.3.6.1.4.1.353.5.7.1.1.6	10,12,15	ima-Group-FailureAlarm v1	IMA Group Remote Failure
imaFailureAlarm	6	1	1.3.6.1.4.1.353.5.7.1.2	1.3.6.1.4.1.353.5.7.1.1.6	14	ima-Group-FailureAlarm v1	IMA Group Remote insufficient links trap
imaFailureAlarm	6	1	1.3.6.1.4.1.353.5.7.1.2	1.3.6.1.4.1.353.5.7.1.1.5	1	ima-Group-Clearing Alarm v1	IMA Group Up Trap
imaFailureAlarm	6	1	1.3.6.1.4.1.353.5.7.1.2	1.3.6.1.4.1.353.5.7.1.1.6	11,16	ima-Group-FailureAlarm v1	IMA Group local Failure

Table 16-3 Cisco IOS V1 Traps (continued)

Trap Name	Generic Type	Specific Type	Enterprise OID	Subtype Varbind OID	Subtype Varbind Value	Description	Short Description
imaFailureAlarm	6	1	1.3.6.1.4.1.353 .5.7.1.2	1.3.6.1.4.1.353 .5.7.1.1.6	13	ima-Group-FailureAlarm v1	IMA Group local insufficient links trap
imaFailureAlarm	6	1	1.3.6.1.4.1.353 .5.7.1.2	1.3.6.1.4.1.353 .5.7.1.1.6	2	ima Link ima-Link-FailureAlarm v1	Ima Link Loss of delay Frame Trap
imaFailureAlarm	6	1	1.3.6.1.4.1.353 .5.7.1.2	1.3.6.1.4.1.353 .5.7.1.1.6	1	ima Link ima-Link-FailureAlarm v1	Ima Link Loss of ima Frame Trap
imaFailureAlarm	6	1	1.3.6.1.4.1.353 .5.7.1.2	1.3.6.1.4.1.353 .5.7.1.1.6	5,7,9	ima Link ima-Link-FailureAlarm v1	Ima Link Rcv Failure Trap
imaFailureAlarm	6	1	1.3.6.1.4.1.353 .5.7.1.2	1.3.6.1.4.1.353 .5.7.1.1.6	3	ima Link ima-Link-FailureAlarm v1	Ima Link Remote Failure Trap
imaFailureAlarm	6	1	1.3.6.1.4.1.353 .5.7.1.2	1.3.6.1.4.1.353 .5.7.1.1.5	1	ima-Link-ClearingAlarm v1	Ima Link Up Trap
imaFailureAlarm	6	1	1.3.6.1.4.1.353 .5.7.1.2	1.3.6.1.4.1.353 .5.7.1.1.6	4,6,8	ima Link ima-Link-FailureAlarm v1	Ima Link Xmt Failure Trap
Cisco-UMT-state-change-v1	6	2	.1.3.6.1.4.1.9.9 .483	N/A	N/A	The state of the connection between the UMTS interfaces.	Cisco UMT state Change trap
Cisco-GSM-state-change-trap-v1	6	1	.1.3.6.1.4.1.9.9 .483	N/A	N/A	The state of the connection between the GSM interfaces	Cisco GSM state Change trap
Cisco-IPRAN-Backhaul-received-util-v1	6	3	.1.3.6.1.4.1.9.9 .483	1.3.6.1.4.1.9.9. 483.1.2.2.1.1.1 .3	1	When Rcvd. util changes to any of the status : acceptable, warning, overloaded.	IPRAN Backhaul Received Util Acceptable Trap
Cisco-IPRAN-Backhaul-received-util-v1	6	3	.1.3.6.1.4.1.9.9 .483	1.3.6.1.4.1.9.9. 483.1.2.2.1.1.1 .3	2	When Rcvd. util changes from or to any of the following : acceptable, warning, overloaded.	IPRAN Backhaul Received Util Warning Trap
Cisco-IPRAN-Backhaul-received-util-v1	6	3	.1.3.6.1.4.1.9.9 .483	1.3.6.1.4.1.9.9. 483.1.2.2.1.1.1 .3	3	When Rcvd. util changes from or to any of the following : acceptable, warning, overloaded.	IPRAN Backhaul Received Util Overloaded Trap

Table 16-3 Cisco IOS V1 Traps (continued)

Trap Name	Generic Type	Specific Type	Enterprise OID	Subtype Varbind OID	Subtype Varbind Value	Description	Short Description
Cisco-IPRAN-Backhaul-sent-util-v1	6	4	.1.3.6.1.4.1.9.9.483	1.3.6.1.4.1.9.9.483.1.2.2.1.1.1.4	1	When sent util changes from or to any of the following : acceptable, warning, overloaded.	IPRAN Backhaul Sent Util Acceptable Trap
Cisco-IPRAN-Backhaul-sent-util-v1	6	4	.1.3.6.1.4.1.9.9.483	1.3.6.1.4.1.9.9.483.1.2.2.1.1.1.4	2	When sent util changes from or to any of the following : acceptable, warning, overloaded.	IPRAN Backhaul Sent Util Overloaded Trap
Cisco-IPRAN-Backhaul-sent-util-v1	6	4	.1.3.6.1.4.1.9.9.483	1.3.6.1.4.1.9.9.483.1.2.2.1.1.1.4	3	When sent util changes from or to any of the following : acceptable, warning, overloaded.	IPRAN Backhaul Sent Util Warning Trap
rttMonConnectionChangeNotification	6	1	1.3.6.1.4.1.9.9.42.2	1.3.6.1.4.1.9.9.42.1.2.9.1.5	1	IPSLA echo ConnLoss Trap v2	Connection Loss detected by ipsla icmp echo trap
rttMonConnectionChangeNotification	6	1	1.3.6.1.4.1.9.9.42.2	1.3.6.1.4.1.9.9.42.1.2.9.1.5	2	IPSLA echo ConnLoss Trap v2	Connection re-establish detected by ipsla icmp echo trap
rttMonTimeoutNotification	6	2	1.3.6.1.4.1.9.9.42.2	1.3.6.1.4.1.9.9.42.1.2.9.1.6	1	IPSLA IP or LSP echo Timeout trap v2	Timeout detected by ipsla icmp echo trap
rttMonTimeoutNotification	6	2	1.3.6.1.4.1.9.9.42.2	1.3.6.1.4.1.9.9.42.1.2.9.1.6	2	IPSLA IP or LSP echo Timeout trap v2	Connection re-establish detected by ipsla icmp echo trap
rttMonThresholdNotification	6	3	1.3.6.1.4.1.9.9.42.2	1.3.6.1.4.1.9.9.42.1.2.9.1.7	1	IPSLA Threshold Notification trap v2	Threshold crossing under trap
rttMonThresholdNotification	6	3	1.3.6.1.4.1.9.9.42.2	1.3.6.1.4.1.9.9.42.1.2.9.1.7	2	IPSLA Threshold Notification trap v2	Threshold crossing over trap
rttMonVerifyErrorNotification	6	4	1.3.6.1.4.1.9.9.42.2	1.3.6.1.4.1.9.9.42.1.2.9.1.11	1	IPSLA Threshold Notification deprecated trap v2	Data corruption in rtt operation trap

Table 16-3 Cisco IOS V1 Traps (continued)

Trap Name	Generic Type	Specific Type	Enterprise OID	Subtype Varbind OID	Subtype Varbind Value	Description	Short Description
rttMonVerifyError Notification	6	4	1.3.6.1.4.1.9.9.42.2	1.3.6.1.4.1.9.9.42.1.2.9.1.11	2	IPSLA Threshold Notification deprecated trap v2	Data corruption cleared in rtt operation trap
rttMonNotification	6	5	1.3.6.1.4.1.9.9.42.2	1.3.6.1.4.1.9.9.42.1.2.19.1.2, 1.3.6.1.4.1.9.9.42.1.2.2.1.33, 1.3.6.1.4.1.9.9.42.1.2.19.1.10	8, null, 1	RTT MON notification	Connection Loss detected by ipsla icmp echo trap
rttMonNotification	6	5	1.3.6.1.4.1.9.9.42.2	1.3.6.1.4.1.9.9.42.1.2.19.1.2, 1.3.6.1.4.1.9.9.42.1.2.2.1.33, 1.3.6.1.4.1.9.9.42.1.2.19.1.10	8, not null, 1	RTT MON notification	Connection Loss detected by ipsla LSP icmp echo trap
rttMonNotification	6	5	1.3.6.1.4.1.9.9.42.2	1.3.6.1.4.1.9.9.42.1.2.19.1.2, 1.3.6.1.4.1.9.9.42.1.2.2.1.33, 1.3.6.1.4.1.9.9.42.1.2.19.1.10	8, null, 2	RTT MON notification	Connection re-establish detected by ipsla icmp echo trap
rttMonNotification	6	5	1.3.6.1.4.1.9.9.42.2	1.3.6.1.4.1.9.9.42.1.2.19.1.2, 1.3.6.1.4.1.9.9.42.1.2.2.1.33, 1.3.6.1.4.1.9.9.42.1.2.19.1.10	8, not null, 2	RTT MON notification	Connection re-establish detected by ipsla LSP icmp echo trap
rttMonNotification	6	5	1.3.6.1.4.1.9.9.42.2	1.3.6.1.4.1.9.9.42.1.2.19.1.2, 1.3.6.1.4.1.9.9.42.1.2.2.1.33, 1.3.6.1.4.1.9.9.42.1.2.19.1.10	7, null, 1	RTT MON notification	Timeout detected by ipsla icmp echo trap
rttMonNotification	6	5	1.3.6.1.4.1.9.9.42.2	1.3.6.1.4.1.9.9.42.1.2.19.1.2, 1.3.6.1.4.1.9.9.42.1.2.2.1.33, 1.3.6.1.4.1.9.9.42.1.2.19.1.10	7, not null, 1	RTT MON notification	Timeout detected by ipsla LSP icmp echo trap

Table 16-3 Cisco IOS V1 Traps (continued)

Trap Name	Generic Type	Specific Type	Enterprise OID	Subtype Varbind OID	Subtype Varbind Value	Description	Short Description
rttMonNotification	6	5	1.3.6.1.4.1.9.9.42.2	1.3.6.1.4.1.9.9.42.1.2.19.1.2, 1.3.6.1.4.1.9.9.42.1.2.2.1.33, 1.3.6.1.4.1.9.9.42.1.2.19.1.10	7, null, 2	RTT MON notification	Connection re-establish detected by ipsla icmp echo trap
rttMonNotification	6	5	1.3.6.1.4.1.9.9.42.2	1.3.6.1.4.1.9.9.42.1.2.19.1.2, 1.3.6.1.4.1.9.9.42.1.2.2.1.33, 1.3.6.1.4.1.9.9.42.1.2.19.1.10	7, not null, 2	RTT MON notification	Connection re-establish detected by ipsla LSP icmp echo trap
rttMonNotification	6	5	1.3.6.1.4.1.9.9.42.2	1.3.6.1.4.1.9.9.42.1.2.19.1.2, 1.3.6.1.4.1.9.9.42.1.2.19.1.10	1, 1	RTT MON notification	RTT threshold crossing over trap
rttMonNotification	6	5	1.3.6.1.4.1.9.9.42.2	1.3.6.1.4.1.9.9.42.1.2.19.1.2, 1.3.6.1.4.1.9.9.42.1.2.19.1.10	1, 2	RTT MON notification	RTT threshold crossing under trap
rttMonLpdDiscoveryNotification	6	6	1.3.6.1.4.1.9.9.42.2	1.3.6.1.4.1.9.9.42.1.3.7.1.13	1	IPSLA LPD Discovery trap v2	IPSLA LSP path discovery failure trap
rttMonLpdDiscoveryNotification	6	6	1.3.6.1.4.1.9.9.42.2	1.3.6.1.4.1.9.9.42.1.3.7.1.13	2	IPSLA LPD Discovery trap v2	IPSLA LSP path rediscovery trap
rttMonLpdGrpStatusNotification	6	7	1.3.6.1.4.1.9.9.42.2	1.3.6.1.4.1.9.9.42.1.3.7.1.16	3,4	IPSLA LDP Group Status trap v2	IPSLA LDP group status failure trap
rttMonLpdGrpStatusNotification	6	7	1.3.6.1.4.1.9.9.42.2	1.3.6.1.4.1.9.9.42.1.3.7.1.16	2	IPSLA LDP Group Status trap v2	IPSLA LDP group status restoration trap
cmplsFrrProtected	6	1	1.3.6.1.4.1.9.10.98	N/A	N/A	TE FRR trigger notification v1	FRR Protected Trap
cmplsFrrUnProtected	6	2	1.3.6.1.4.1.9.10.98	N/A	N/A	TE FRR trigger notification v1	FRR Unprotected Trap

Table 16-3 Cisco IOS V1 Traps (continued)

Trap Name	Generic Type	Specific Type	Enterprise OID	Subtype Varbind OID	Subtype Varbind Value	Description	Short Description
cpwVcUp	6	2	1.3.6.1.4.1.9.10.106.2	N/A	N/A	This notification is generated when the cpwVcOperStatus object for one or more contiguous entries in cpwVcTable are about to enter the up(1) state from some other state.	Pseudo wire tunnel up
cpwVcDown	6	1	1.3.6.1.4.1.9.10.106.2	N/A	N/A	This notification is generated when the cpwVcOperStatus object for one or more contiguous entries in cpwVcTable are about to enter the up(1) state from some other state.	Pseudo wire tunnel down

Table 16-3 Cisco IOS V1 Traps (continued)

Trap Name	Generic Type	Specific Type	Enterprise OID	Subtype Varbind OID	Subtype Varbind Value	Description	Short Description
vtpConfigRevNumberError	6	1	1.3.6.1.4.1.9.9.46.2	N/A	N/A	A configuration revision number error notification signifies that a device has incremented its vtpConfigRevNumberErrors counter. Generation of this notification is suppressed if the vtpNotificationsEnabled has the value 'false'. The device must throttle the generation of consecutive vtpConfigRevNumberError notifications so that there is at least a five-second gap between notification of this type. When notification are throttled, they are dropped, not queued for sending at a future time. (Note that 'generating' a notification means sending to all configured recipients.	vtp configuration revision number error trap

Table 16-3 Cisco IOS V1 Traps (continued)

Trap Name	Generic Type	Specific Type	Enterprise OID	Subtype Varbind OID	Subtype Varbind Value	Description	Short Description
vtpConfigDigestError	6	2	1.3.6.1.4.1.9.9.46.2	N/A	N/A	A configuration digest error notification signifies that a device has incremented its vtpConfigDigestErrors counter. Generation of this notification is suppressed if the vtpNotificationsEnabled has the value 'false'. The device must throttle the generation of consecutive vtpConfigDigestError notifications so that there is at least a five-second gap between notification of this type. When notification are throttled, they are dropped, not queued for sending at a future time. (Note that 'generating' a notification means sending to all configured recipients).	vtp configuration digest error trap

Table 16-3 Cisco IOS V1 Traps (continued)

Trap Name	Generic Type	Specific Type	Enterprise OID	Subtype Varbind OID	Subtype Varbind Value	Description	Short Description
vtpVersionOneDeviceDetected	6	6	1.3.6.1.4.1.9.9.46.2	N/A	N/A	A VTP version one device detected notification is generated by a device when: A. A management domain has been put into version 2 mode (as accessed by managementDomain VersionInUse). B. 15 minutes has passed since (A) occurred. C. A version 1 PDU is detected on a trunk on the device that is in that management domain which has a lower revision number than the current configuration.	vtp VersionOne Device Detected trap
vtpLocalModeChanged	6	8	1.3.6.1.4.1.9.9.46.2	N/A	N/A	A vtpLocalModeChanged notification is generated by a device when the value of the object managementDomain LocalMode is changed.	vtp Local Mode Changed trap
vtpVersionInUseChanged	6	9	1.3.6.1.4.1.9.9.46.2	N/A	N/A	A vtpVersionInUseChanged notification is generated by a device when the value of the object managementDomain VersionInUse is changed.	vtp VersionInUse Changed trap

Table 16-3 Cisco IOS V1 Traps (continued)

Trap Name	Generic Type	Specific Type	Enterprise OID	Subtype Varbind OID	Subtype Varbind Value	Description	Short Description
vlanTrunkPortDynamicStatusChange	6	7	1.3.6.1.4.1.9.9.46.2	1.3.6.1.4.1.9.9.46.1.6.1.1.14	1	A vlanTrunkPortDynamicStatusChange notification is generated by a device when the value of vlanTrunkPortDynamicStatus object has been changed.	Vlan trunk port dynamic status changed to trunking
vlanTrunkPortDynamicStatusChange	6	7	1.3.6.1.4.1.9.9.46.2	1.3.6.1.4.1.9.9.46.1.6.1.1.14	2	A vlanTrunkPortDynamicStatusChange notification is generated by a device when the value of vlanTrunkPortDynamicStatus object has been changed.	Vlan trunk port dynamic status changed to not trunking
crepLinkStatus	6	1	.1.3.6.1.4.1.9.9.601	1.3.6.1.4.1.9.9.601.1.2.1.1.3	5	Cisco REP link status change trap	REP port state fully operational Trap
crepLinkStatus	6	1	.1.3.6.1.4.1.9.9.601	1.3.6.1.4.1.9.9.601.1.2.1.1.3	!=5	Cisco REP link status change trap	REP port state not operational Trap
crepPortRoleChange	6	3	.1.3.6.1.4.1.9.9.601	1.3.6.1.4.1.9.9.601.1.2.1.1.4	1	Cisco REP port role change trap	REP port role failed Trap
crepPortRoleChange	6	3	.1.3.6.1.4.1.9.9.601	1.3.6.1.4.1.9.9.601.1.2.1.1.4	!=1	Cisco REP port role change trap	REP port role clear Trap
ciscoSonetVTStatusChange	6	4	1.3.6.1.4.1.9.9.126	1.3.6.1.2.1.10.39.3.1.1.1.2	!=1	VT Status is down	Cisco Sonet vt status changed to error
ciscoSonetVTStatusChange	6	4	1.3.6.1.4.1.9.9.126	1.3.6.1.2.1.10.39.3.1.1.1.2	1	VT Status is down	Cisco Sonet vt status changed to clear
cEtherCfmCcMepUp	6	1	.1.3.6.1.4.1.9.9.461.0.0.1	N/A	N/A	mep up	CFM cc mep up trap
cEtherCfmCcMepDown	6	2	.1.3.6.1.4.1.9.9.461.0.0.2	.1.3.6.1.4.1.9.9.461.1.1.2.1.16	5	timeout	CFM cc mep down due to timeout trap
cEtherCfmCcMepDown	6	2	.1.3.6.1.4.1.9.9.461.0.0.2	.1.3.6.1.4.1.9.9.461.1.1.2.1.16	4	lastgasp	CFM cc mep down due to last gasp trap

Table 16-3 Cisco IOS V1 Traps (continued)

Trap Name	Generic Type	Specific Type	Enterprise OID	Subtype Varbind OID	Subtype Varbind Value	Description	Short Description
cEtherCfmCcCrossconnect	6	3	.1.3.6.1.4.1.9.9.461.0.0.3	N/A	N/A	cross-connected service error trap	CFM cc cross-connected service error trap
cEtherCfmCcMepDown	6	2	.1.3.6.1.4.1.9.9.461.0.0.2	.1.3.6.1.4.1.9.9.461.1.1.2.1.16	8	cross-connected service error trap clear	CFM cc cross-connected service error trap clear
cEtherCfmCcLoop	6	4	.1.3.6.1.4.1.9.9.461.0.0.4	N/A	N/A	loop trap	CFM cc loop trap
cEtherCfmCcMepDown	6	2	.1.3.6.1.4.1.9.9.461.0.0.2	.1.3.6.1.4.1.9.9.461.1.1.2.1.16	7	loop trap clear	CFM cc loop trap clear
cEtherCfmCcConfigError	6	5	.1.3.6.1.4.1.9.9.461.0.0.5	N/A	N/A	config error trap	CFM cc config error trap
cEtherCfmCcMepDown	6	2	.1.3.6.1.4.1.9.9.461.0.0.2	.1.3.6.1.4.1.9.9.461.1.1.2.1.16	6	config error trap clear	CFM cc config error trap clear
cEtherCfmXCheckMissing	6	6	.1.3.6.1.4.1.9.9.461.0.0.6	N/A	N/A	mep missing trap	CFM crossconnect mep missing trap
cEtherCfmXCheckUnknown	6	7	.1.3.6.1.4.1.9.9.461.0.0.7	N/A	N/A	mep unknown trap	CFM crossconnect mep unknown trap
cEtherCfmCcMepDown	6	2	.1.3.6.1.4.1.9.9.461.0.0.2	.1.3.6.1.4.1.9.9.461.1.1.2.1.16	9	mep unknown trap clear	CFM crossconnect mep unknown trap clear
cEtherCfmXCheckServiceUp	6	8	.1.3.6.1.4.1.9.9.461.0.0.8	N/A	N/A	ICfmServiceOid	CFM crossconnect mep service up trap
vrrpTrapAuthFailure	6	2	1.3.6.1.2.1.68	N/A	N/A	vrrp trap auth failure trap	Vrrp trap auth failure trap
vrrpTrapNewMaster	6	1	1.3.6.1.2.1.68	N/A	N/A	vrrp trap new master trap	Vrrp trap new master trap
cdot3OamNonThresholdEvent	6	2	1.3.6.1.4.1.9.10.136	1.3.6.1.4.1.9.10.136.1.6.1.4	256	Local or remote non-threshold crossing event is detected.	OAM Non-threshold crossing link fault trap

Table 16-3 Cisco IOS V1 Traps (continued)

Trap Name	Generic Type	Specific Type	Enterprise OID	Subtype Varbind OID	Subtype Varbind Value	Description	Short Description
cdot3OamNonThresholdEvent	6	2	1.3.6.1.4.1.9.10.136	1.3.6.1.4.1.9.10.136.1.6.1.4	257	Local or remote non-threshold crossing event is detected.	OAM Non-threshold crossing dying gasp trap
cdot3OamNonThresholdEvent	6	2	1.3.6.1.4.1.9.10.136	1.3.6.1.4.1.9.10.136.1.6.1.4	258	Local or remote non-threshold crossing event is detected.	OAM Non-threshold crossing critical Link trap
cdot3OamThresholdEvent	6	1	1.3.6.1.4.1.9.10.136	1.3.6.1.4.1.9.10.136.1.6.1.4	1	Local or remote threshold crossing event is detected.	OAM threshold errored Symbol trap
cdot3OamThresholdEvent	6	1	1.3.6.1.4.1.9.10.136	1.3.6.1.4.1.9.10.136.1.6.1.4	2	Local or remote threshold crossing event is detected.	OAM threshold errored Frame Period trap
cdot3OamThresholdEvent	6	1	1.3.6.1.4.1.9.10.136	1.3.6.1.4.1.9.10.136.1.6.1.4	3	Local or remote threshold crossing event is detected.	OAM threshold errored Frame trap
cdot3OamThresholdEvent	6	1	1.3.6.1.4.1.9.10.136	1.3.6.1.4.1.9.10.136.1.6.1.4	4	Local or remote threshold crossing event is detected.	OAM threshold errored Frame Seconds trap
cbfDefineFileCompletion	6	1	1.3.6.1.4.1.9.9.81.2	N/A	N/A	A cbfDefineFileCompletion notification is sent on the following conditions : - completion of a file consumption operation in case of ephemeral files. - completion of file creation operation in case of volatile or permanent files. - any error during file creation.	CBF File operation state indicator

Table 16-3 Cisco IOS V1 Traps (continued)

Trap Name	Generic Type	Specific Type	Enterprise OID	Subtype Varbind OID	Subtype Varbind Value	Description	Short Description
cbgpBackwardTransition	6	2	1.3.6.1.4.1.9.9.187	1.3.6.1.4.1.9.9.187.0.2	!= (1or 6)	The cbgpBackwardTransition Event is generated when the BGP FSM moves from a higher numbered state to a lower numbered state. The bgpPeerRemoteAddr value is attached to the notification object ID.	Cisco BGP backward transition trap
cbgpFsmStateChange	6	1	1.3.6.1.4.1.9.9.187	1.3.6.1.4.1.9.9.187.0.2	= 1	The BGP cbgpFsmStateChange notification is generated for every BGP FSM state change.	Cisco BGP down trap
cbgpFsmStateChange	6	1	1.3.6.1.4.1.9.9.187	1.3.6.1.4.1.9.9.187.0.2	= 6	The BGP cbgpFsmStateChange notification is generated for every BGP FSM state change.	Cisco BGP established trap
cbgpPrefixThresholdExceeded	6	3	1.3.6.1.4.1.9.9.187	N/A	N/A	The cbgpPrfefixMaxThresholdExceeded notification is generated when prefix count exceeds the configured warning threshold on a session for an address family	Cisco BGP prefix threshold exceeded

Table 16-3 Cisco IOS V1 Traps (continued)

Trap Name	Generic Type	Specific Type	Enterprise OID	Subtype Varbind OID	Subtype Varbind Value	Description	Short Description
cbgpPrefixThresholdClear	6	4	1.3.6.1.4.1.9.9.187	N/A	N/A	The cbgpPrefixThresholdClear notification is generated when prefix count drops below the configured clear threshold on a session for an address family once cbgpPrefixThresholdExceeded is generated. This won't be generated if the peer session goes down after the generation of bgpPrefixThresholdExceeded. The bgpPeerRemoteAddr, bgpPeerAddrFamilyAfi and cbgpPeerAddrFamilySafi values are attached to the notification object ID.	Cisco BGP prefix threshold clear
ciscoConfigManEvent	6	1	1.3.6.1.4.1.9.9.43.2	N/A	N/A	Notification of a configuration management event as recorded in ccmHistoryEventTable.	Cisco Configuration management event notification
cefcFanTrayStatusChange	6	6	1.3.6.1.4.1.9.9.117.2	1.3.6.1.4.1.9.9.117.1.4.1.1.1	!=2	This notification is generated when the value of cefcFanTrayOperStatus changes.	cefc fan-tray oper status down
cefcFanTrayStatusChange	6	6	1.3.6.1.4.1.9.9.117.2	1.3.6.1.4.1.9.9.117.1.4.1.1.1	=2	This notification is generated when the value of cefcFanTrayOperStatus changes.	cefc fan-tray oper status up

Table 16-3 Cisco IOS V1 Traps (continued)

Trap Name	Generic Type	Specific Type	Enterprise OID	Subtype Varbind OID	Subtype Varbind Value	Description	Short Description
cefcFRUInserted	6	3	1.3.6.1.4.1.9.9.117.2	N/A	N/A	The cecfFRUInserted notification indicates that a FRU was inserted. The varbind for this notification indicates the entPhysicalIndex of the inserted FRU, and the entPhysicalIndex of the FRU's container.	cefc FRU inserted
cefcFRURemoved	6	4	1.3.6.1.4.1.9.9.117.2	N/A	N/A	The cefcFRURemoved notification indicates that a FRU was removed. The varbind for this notification indicates the entPhysicalIndex of the removed FRU, and the entPhysicalIndex of the FRU's container.	cefc FRU removed
cefcModuleStatus Change	6	1	1.3.6.1.4.1.9.9.117.2	1.3.6.1.4.1.9.9.117.1.2.1.1.2	!=2	This notification is generated when the value of cefcModuleOperStatus changes. It can be utilized by an NMS to update the status of the module it is managing.	cefc module oper status down
cefcModuleStatus Change	6	1	1.3.6.1.4.1.9.9.117.2	1.3.6.1.4.1.9.9.117.1.2.1.1.2	=2	This notification is generated when the value of cefcModuleOperStatus changes. It can be utilized by an NMS to update the status of the module it is managing.	cefc module oper status up

Table 16-3 Cisco IOS V1 Traps (continued)

Trap Name	Generic Type	Specific Type	Enterprise OID	Subtype Varbind OID	Subtype Varbind Value	Description	Short Description
cefcPowerStatusChange	6	2	1.3.6.1.4.1.9.9.117.2	1.3.6.1.4.1.9.9.117.1.1.2.1.2	!=2	The cefcFRUPowerStatusChange notification indicates that the power status of a FRU has changed. The varbind for this notification indicates the entPhysicalIndex of the FRU, and the new operational-status of the FRU.	cefc power status down
cefcPowerStatusChange	6	2	1.3.6.1.4.1.9.9.117.2	1.3.6.1.4.1.9.9.117.1.1.2.1.2	=2	The cefcFRUPowerStatusChange notification indicates that the power status of a FRU has changed. The varbind for this notification indicates the entPhysicalIndex of the FRU, and the new operational-status of the FRU.	cefc power status up
entSensorThresholdNotification	6	1	1.3.6.1.4.1.9.9.91.2.0.1	N/A	N/A	The sensor value crossed the threshold listed in entSensorThreshold Table. This notification is generated once each time the sensor value crosses the threshold	sensor value crossed threshold in entSensorThresholdTable
ciscoFlashCopyCompletionTrap	6	1	1.3.6.1.4.1.9.9.10.1.3	1.3.6.1.4.1.9.9.10.1.2.1.1.8	!= (0 or 1 or 2)	A ciscoFlashCopyCompletionTrap is sent at the completion of a flash copy operation if such a trap was requested when the operation was initiated.	Cisco flash copy failed

Table 16-3 Cisco IOS V1 Traps (continued)

Trap Name	Generic Type	Specific Type	Enterprise OID	Subtype Varbind OID	Subtype Varbind Value	Description	Short Description
ciscoFlashCopyCompletionTrap	6	1	1.3.6.1.4.1.9.9.10.1.3	1.3.6.1.4.1.9.9.10.1.2.1.1.8	=2	A ciscoFlashCopyCompletionTrap is sent at the completion of a flash copy operation if such a trap was requested when the operation was initiated.	Cisco flash copy completion
ciscoFlashCopyCompletionTrap	6	1	1.3.6.1.4.1.9.9.10.1.3	1.3.6.1.4.1.9.9.10.1.2.1.1.8	=(0 or 1)	A ciscoFlashCopyCompletionTrap is sent at the completion of a flash copy operation if such a trap was requested when the operation was initiated.	Cisco flash copy in progress
ciscoFlashDeviceChangeTrap	6	4	1.3.6.1.4.1.9.9.10.1.3	N/A	N/A	A ciscoFlashDeviceChangeTrap is sent whenever a removable Flash device is inserted or removed.	Cisco Flash device changed
ciscoFlashDeviceInsertedNotif	6	5	1.3.6.1.4.1.9.9.10.1.3	N/A	N/A	A ciscoFlashDeviceInsertedNotif notification is sent whenever a removable Flash device is inserted.	Cisco Flash device inserted
ciscoFlashDeviceRemovedNotif	6	6	1.3.6.1.4.1.9.9.10.1.3	N/A	N/A	A ciscoFlashDeviceRemovedNotif notification is sent whenever a removable Flash device is removed.	Cisco Flash device removed

Table 16-3 Cisco IOS V1 Traps (continued)

Trap Name	Generic Type	Specific Type	Enterprise OID	Subtype Varbind OID	Subtype Varbind Value	Description	Short Description
ciscoFlashDeviceInsertedNotifRev1	6	7	1.3.6.1.4.1.9.9.10.1.3	N/A	N/A	A ciscoFlashDeviceInsertedNotifRev1 notification is sent whenever a removable Flash device is inserted. The ciscoFlashDeviceInsertedNotifRev1 depcrecates ciscoFlashDeviceInsertedNotif since it uses ciscoFlashDeviceName as a varbind which is deprecated.	Cisco Flash device inserted
ciscoFlashDeviceRemovedNotifRev1	6	8	1.3.6.1.4.1.9.9.10.1.3	N/A	N/A	A ciscoFlashDeviceRemovedNotifRev1 notification is sent whenever a removable Flash device is removed. The ciscoFlashDeviceRemovedNotifRev1 depcrecates ciscoFlashDeviceRemovedNotif since it uses ciscoFlashDeviceName as a varbind which is deprecated.	Cisco Flash device removed

Table 16-3 Cisco IOS V1 Traps (continued)

Trap Name	Generic Type	Specific Type	Enterprise OID	Subtype Varbind OID	Subtype Varbind Value	Description	Short Description
ciscoFlashMiscOpCompletionTrap	6	3	1.3.6.1.4.1.9.9.10.1.3	1.3.6.1.4.1.9.9.10.1.2.3.1.4	!= (1 or 2)	A ciscoFlashMiscOpCompletionTrap is sent at the completion of a miscellaneous flash operation (enumerated in ciscoFlashMiscOpCommand) if such a trap was requested when the operation was initiated.	Cisco Flash miscellaneous operation failed
ciscoFlashMiscOpCompletionTrap	6	3	1.3.6.1.4.1.9.9.10.1.3	1.3.6.1.4.1.9.9.10.1.2.3.1.4	=2	A ciscoFlashMiscOpCompletionTrap is sent at the completion of a miscellaneous flash operation (enumerated in ciscoFlashMiscOpCommand) if such a trap was requested when the operation was initiated.	Cisco Flash miscellaneous operation completed
ciscoFlashMiscOpCompletionTrap	6	3	1.3.6.1.4.1.9.9.10.1.3	1.3.6.1.4.1.9.9.10.1.2.3.1.4	=1	A ciscoFlashMiscOpCompletionTrap is sent at the completion of a miscellaneous flash operation (enumerated in ciscoFlashMiscOpCommand) if such a trap was requested when the operation was initiated.	Cisco Flash miscellaneous operation in progress
chassisAlarmOff	6	6	1.3.6.1.4.1.9.5	N/A	N/A	chassis alarm trap	chassis alarm off
chassisAlarmOn	6	5	1.3.6.1.4.1.9.5	N/A	N/A	chassis alarm trap	chassis alarm on

Table 16-3 Cisco IOS V1 Traps (continued)

Trap Name	Generic Type	Specific Type	Enterprise OID	Subtype Varbind OID	Subtype Varbind Value	Description	Short Description
cPimNbrLoss	6	2	1.3.6.1.4.1.9.10.119	N/A	N/A	A cPimNbrLoss trap signifies the loss of an adjacency with a neighbor. This trap should be generated when the neighbor timer expires, and the router has no other neighbors on the same interface with a lower IP address than itself.	Cisco PIM neighbor lost
ciscoPingCompletion	6	1	1.3.6.1.4.1.9.9.16.2	N/A	N/A	A ciscoPingCompleted trap is sent at the completion of a sequence of pings if such a trap was requested when the sequence was initiated.	Cisco ping completion
ciscoSonetSectionStatusChange	6	1	1.3.6.1.4.1.9.9.126	1.3.6.1.2.1.10.39.1.2.1.1.1	!=1	This notification is generated whenever the value of sonetSectionCurrentStatus changes to value more than 1.	Cisco Sonet section status changed to error
ciscoSonetSectionStatusChange	6	1	1.3.6.1.4.1.9.9.126	1.3.6.1.2.1.10.39.1.2.1.1.1	=1	This notification is generated whenever the value of sonetSectionCurrentStatus changes to value 1.	Cisco Sonet section status changed to clear
ciscoSonetLineStatusChange	6	2	1.3.6.1.4.1.9.9.126	1.3.6.1.2.1.10.39.1.3.1.1.1	!=1	This notification is generated whenever the value of sonetLineCurrentStatus changes to value more than 1.	Cisco Sonet line status changed to error
ciscoSonetLineStatusChange	6	2	1.3.6.1.4.1.9.9.126	1.3.6.1.2.1.10.39.1.3.1.1.1	=1	This notification is generated whenever the value of sonetLineCurrentStatus changes to value 1.	Cisco Sonet line status changed to clear

Table 16-3 Cisco IOS V1 Traps (continued)

Trap Name	Generic Type	Specific Type	Enterprise OID	Subtype Varbind OID	Subtype Varbind Value	Description	Short Description
ciscoSonetPathStatusChange	6	3	1.3.6.1.4.1.9.9.126	1.3.6.1.2.1.10.39.2.1.1.1.2	!=1	This notification is generated whenever the value of sonetPathCurrentStatus changes to value more than 1.	Cisco Sonet path status changed to error
ciscoSonetPathStatusChange	6	3	1.3.6.1.4.1.9.9.126	1.3.6.1.2.1.10.39.2.1.1.1.2	=1	This notification is generated whenever the value of sonetPathCurrentStatus changes to value 1.	Cisco Sonet path status changed to clear
mplsLdpFailedInitSessionThresholdExceeded	6	1	1.3.6.1.4.1.9.10.65.2	N/A	N/A	This notification is generated when the value of the 'mplsLdpEntityPVLimitMismatchTrapEable' object is 'enabled(1)' and the value of the object, 'mplsLdpEntityFailedInitSessionThreshold' has been exceeded.	MPLS LDP init session threshold exceeded Trap
mplsLdpSessionDown	6	4	1.3.6.1.4.1.9.10.65.2	N/A	N/A	Generation of this trap occurs when the 'mplsLdpSessionUpDownTrapEnable' object is 'enabled(1)' and the value of mplsLdpSessionState changes from 'operational(5)' to any other state.	MPLS LDP session down Trap
mplsLdpSessionUp	6	3	1.3.6.1.4.1.9.10.65.2	N/A	N/A	Generation of this trap occurs when the 'mplsLdpSessionUpDownTrapEnable' object is 'enabled(1)' and the value of mplsLdpSessionState changes from any state accept 'nonexistent(1)' to 'operational.	MPLS LDP session up Trap

Table 16-3 Cisco IOS V1 Traps (continued)

Trap Name	Generic Type	Specific Type	Enterprise OID	Subtype Varbind OID	Subtype Varbind Value	Description	Short Description
mplsTunnelUp	6	1	1.3.6.1.3.95.3	N/A	N/A	This notification is generated when a mplsTunnelOperStatus object for one of the configured tunnels is about to leave the down state and transition into some other state (but not into the notPresent state). This other state is indicated by the included value of mplsTunnelOperStatus.	MPLS-TE tunnel up trap
mplsTunnelDown	6	2	1.3.6.1.3.95.3	N/A	N/A	This notification is generated when a mplsTunnelOperStatus object for one of the configured tunnels is about to enter the down state from some other state (but not from the notPresent state). This other state is indicated by the included value of mplsTunnelOperStatus.	MPLS-TE tunnel down trap
mplsTunnelRerouted	6	3	1.3.6.1.3.95.3	N/A	N/A	This notification is generated when a tunnel is rerouted or re-optimized. If the Actual Path is used, then this object MAY contain the new path for this tunnel some time after this trap is issued by the agent.	MPLS-TE tunnel rerouted trap

Table 16-3 Cisco IOS V1 Traps (continued)

Trap Name	Generic Type	Specific Type	Enterprise OID	Subtype Varbind OID	Subtype Varbind Value	Description	Short Description
ciscoIpMRouteMissingHeartBeats	6	1	1.3.6.1.4.1.9.10.2.3.1	N/A	N/A	A notification is sent if a multicast router with this feature enabled failed to receive configured number of heartbeat packets from heartbeat sources within a configured time interval	Failed receive multicast router heartbeat
ciscoRFProgressionNotif	6	2	1.3.6.1.4.1.9.9.176.2.	1.3.6.1.4.1.9.9.176.1.1.4	2	VSL link goes down or one of the chassis reloads	Cisco VSS Shelf 1 is Disabled
ciscoRFProgressionNotif	6	2	1.3.6.1.4.1.9.9.176.2	1.3.6.1.4.1.9.9.176.1.1.4	5	VSL link goes down or one of the chassis reloads	Cisco VSS Shelf 1 is Standby Cold
ciscoRFProgressionNotif	6	2	1.3.6.1.4.1.9.9.176.2.	1.3.6.1.4.1.9.9.176.1.1.4	9	VSL link goes down or one of the chassis reloads	Cisco VSS Shelf 1 is Standby Hot
ciscoRFProgressionNotif	6	2	1.3.6.1.4.1.9.9.176.2	1.3.6.1.4.1.9.9.176.1.1.4	2	VSL link goes down or one of the chassis reloads	Cisco VSS Shelf 2 is Disabled
ciscoRFProgressionNotif	6	2	1.3.6.1.4.1.9.9.176.2	1.3.6.1.4.1.9.9.176.1.1.4	5	VSL link goes down or one of the chassis reloads	Cisco VSS Shelf 2 is Standby Cold
ciscoRFProgressionNotif	6	2	1.3.6.1.4.1.9.9.176.2	1.3.6.1.4.1.9.9.176.1.1.4	9	VSL link goes down or one of the chassis reloads	Cisco VSS Shelf 2 is Standby Hot
cvsVSLConnectionChangeNotif	6	1	1.3.6.1.4.1.9.9.388	N/A	N/A	when VSL connection is down	VSL Connection Changed: Down
cvsVSLConnectionChangeNotif	6	1	1.3.6.1.4.1.9.9.388	N/A	N/A	when VSL connection is up	VSL Connection Change: Up
topologyChange	6	2	1.3.6.1.2.1.17	N/A	N/A	This Notification is sent by a bridge when any of its configured ports transitions from the Learning state to the Forwarding state, or from the Forwarding state to the Blocking state.	dot1qBridge trap

Table 16-3 Cisco IOS V1 Traps (continued)

Trap Name	Generic Type	Specific Type	Enterprise OID	Subtype Varbind OID	Subtype Varbind Value	Description	Short Description
cEtherCfmCcMepUp	6	1	1.3.6.1.4.1.9.9.461.0	N/A	N/A	This notification is generated in the following cases: when a remote MEP first comes up, that is when we receive CC message from that MEP for the first time. - when the device receives a CC message from a MEP for which t has an expired CCDB entry. when a CC message is received for a remote MEP for which the device already has a CCDB entry and the port-state in the received CC message is different from the cached previous state.	Mep up trap
cEtherCfmCcMepDown	6	2	1.3.6.1.4.1.9.9.461.0	N/A	N/A	This notification is generated when a remote MEP goes down; i.e. the entry in CCDB corresponding to this MEP times out or the device receives a CC message with zero hold-time.	Mep down trap
coldStart	6	0	1.3.6.1.2.1.11	N/A	N/A	This trap signifies that the sending protocol entity is reinitializing itself such that the agent s configuration or the protocol entity implementation may be altered.	Cold start trap

Table 16-3 Cisco IOS V1 Traps (continued)

Trap Name	Generic Type	Specific Type	Enterprise OID	Subtype Varbind OID	Subtype Varbind Value	Description	Short Description
cHsrpStateChange	6	1	1.3.6.1.4.1.9.9.106.2	1.3.6.1.4.1.9.9.106.1.2.1.1.15	= 5	A cHsrpStateChange notification is sent when a cHsrpGrpStandbyState transitions to either active or standby state, or leaves active or standby state. There will be only one notification issued when the state change is from standby to active and vice versa.	Cisco hsrp state standby
cHsrpStateChange	6	1	1.3.6.1.4.1.9.9.106.2	1.3.6.1.4.1.9.9.106.1.2.1.1.15	= 5	A cHsrpStateChange notification is sent when a cHsrpGrpStandbyState transitions to either active or standby state, or leaves active or standby state. There will be only one notification issued when the state change is from standby to active and vice versa.	Cisco hsrp state non active
cHsrpStateChange	6	1	1.3.6.1.4.1.9.9.106.2	1.3.6.1.4.1.9.9.106.1.2.1.1.15	= 6	A cHsrpStateChange notification is sent when a cHsrpGrpStandbyState transitions to either active or standby state, or leaves active or standby state. There will be only one notification issued when the state change is from standby to active and vice versa.	Cisco hsrp state active

Table 16-3 Cisco IOS V1 Traps (continued)

Trap Name	Generic Type	Specific Type	Enterprise OID	Subtype Varbind OID	Subtype Varbind Value	Description	Short Description
ciscoEnvMonFanNotification	6	4	1.3.6.1.4.1.9.9.13.3	1.3.6.1.4.1.9.9.13.1.4.1.3	= 3	A ciscoEnvMonFanNotification is sent if any one of the fans in the fan array (where existent) fails. Since such a notification is usually generated before the shutdown state is reached, it can convey more data and has a better chance of being sent than does the ciscoEnvMonShutdownNotification.	Cisco Environment Monitoring Fan Notification - Critical
ciscoEnvMonFanNotification	6	4	1.3.6.1.4.1.9.9.13.3	1.3.6.1.4.1.9.9.13.1.4.1.3	= 1	A ciscoEnvMonFanNotification is sent if any one of the fans in the fan array (where existent) fails. Since such a notification is usually generated before the shutdown state is reached, it can convey more data and has a better chance of being sent than does the ciscoEnvMonShutdownNotification.	Cisco Environment Monitoring Fan Notification - Normal

Table 16-3 Cisco IOS V1 Traps (continued)

Trap Name	Generic Type	Specific Type	Enterprise OID	Subtype Varbind OID	Subtype Varbind Value	Description	Short Description
ciscoEnvMonFanNotification	6	4	1.3.6.1.4.1.9.9.13.3	1.3.6.1.4.1.9.9.13.1.4.1.3	= 6	A ciscoEnvMonFanNotification is sent if any one of the fans in the fan array (where existent) fails. Since such a notification is usually generated before the shutdown state is reached, it can convey more data and has a better chance of being sent than does the ciscoEnvMonShutdownNotification.	Cisco Environment Monitoring Fan Notification - Not Functioning
ciscoEnvMonFanNotification	6	4	1.3.6.1.4.1.9.9.13.3	1.3.6.1.4.1.9.9.13.1.4.1.3	= 5	A ciscoEnvMonFanNotification is sent if any one of the fans in the fan array (where existent) fails. Since such a notification is usually generated before the shutdown state is reached, it can convey more data and has a better chance of being sent than does the ciscoEnvMonShutdownNotification.	Cisco Environment Monitoring Fan Notification - Not Present

Table 16-3 Cisco IOS V1 Traps (continued)

Trap Name	Generic Type	Specific Type	Enterprise OID	Subtype Varbind OID	Subtype Varbind Value	Description	Short Description
ciscoEnvMonFanNotification	6	4	1.3.6.1.4.1.9.9.13.3	1.3.6.1.4.1.9.9.13.1.4.1.3	= 4	A ciscoEnvMonFanNotification is sent if any one of the fans in the fan array (where existent) fails. Since such a notification is usually generated before the shutdown state is reached, it can convey more data and has a better chance of being sent than does the ciscoEnvMonShutdownNotification.	Cisco Environment Monitoring Fan Notification - Shutdown
ciscoEnvMonFanNotification	6	4	1.3.6.1.4.1.9.9.13.3	1.3.6.1.4.1.9.9.13.1.4.1.3	= 2	A ciscoEnvMonFanNotification is sent if any one of the fans in the fan array (where existent) fails. Since such a notification is usually generated before the shutdown state is reached, it can convey more data and has a better chance of being sent than does the ciscoEnvMonShutdownNotification.	Cisco Environment Monitoring Fan Notification - Warning

Table 16-3 Cisco IOS V1 Traps (continued)

Trap Name	Generic Type	Specific Type	Enterprise OID	Subtype Varbind OID	Subtype Varbind Value	Description	Short Description
ciscoEnvMonRedundantSupplyNotification	6	5	1.3.6.1.4.1.9.9.13.3	1.3.6.1.4.1.9.9.13.1.5.1.3	= 3	A ciscoEnvMonRedundantSupplyNotification is sent if the redundant power supply (where exists) fails. Since such a notification is usually generated before the shutdown state is reached, it can convey more data and has a better chance of being sent than does the ciscoEnvMonShutdownNotification.	Redundant Supply State - Critical
ciscoEnvMonRedundantSupplyNotification	6	5	1.3.6.1.4.1.9.9.13.3	1.3.6.1.4.1.9.9.13.1.5.1.3	= 1	A ciscoEnvMonRedundantSupplyNotification is sent if the redundant power supply (where exists) fails. Since such a notification is usually generated before the shutdown state is reached, it can convey more data and has a better chance of being sent than does the ciscoEnvMonShutdownNotification.	Redundant Supply State - Normal

Table 16-3 Cisco IOS V1 Traps (continued)

Trap Name	Generic Type	Specific Type	Enterprise OID	Subtype Varbind OID	Subtype Varbind Value	Description	Short Description
ciscoEnvMonRedundantSupplyNotification	6	5	1.3.6.1.4.1.9.9.13.3	1.3.6.1.4.1.9.9.13.1.5.1.3	= 6	A ciscoEnvMonRedundantSupplyNotification is sent if the redundant power supply (where exists) fails. Since such a notification is usually generated before the shutdown state is reached, it can convey more data and has a better chance of being sent than does the ciscoEnvMonShutdownNotification.	Redundant Supply State - Not Functioning
ciscoEnvMonRedundantSupplyNotification	6	5	1.3.6.1.4.1.9.9.13.3	1.3.6.1.4.1.9.9.13.1.5.1.3	= 5	A ciscoEnvMonRedundantSupplyNotification is sent if the redundant power supply (where exists) fails. Since such a notification is usually generated before the shutdown state is reached, it can convey more data and has a better chance of being sent than does the ciscoEnvMonShutdownNotification.	Redundant Supply State - Not Present

Table 16-3 Cisco IOS V1 Traps (continued)

Trap Name	Generic Type	Specific Type	Enterprise OID	Subtype Varbind OID	Subtype Varbind Value	Description	Short Description
ciscoEnvMonRedundantSupplyNotification	6	5	1.3.6.1.4.1.9.9.13.3	1.3.6.1.4.1.9.9.13.1.5.1.3	= 4	A ciscoEnvMonRedundantSupplyNotification is sent if the redundant power supply (where exists) fails. Since such a notification is usually generated before the shutdown state is reached, it can convey more data and has a better chance of being sent than does the ciscoEnvMonShutdownNotification.	Redundant Supply State - Shutdown
ciscoEnvMonRedundantSupplyNotification	6	5	1.3.6.1.4.1.9.9.13.3	1.3.6.1.4.1.9.9.13.1.5.1.3	= 2	A ciscoEnvMonRedundantSupplyNotification is sent if the redundant power supply (where exists) fails. Since such a notification is usually generated before the shutdown state is reached, it can convey more data and has a better chance of being sent than does the ciscoEnvMonShutdownNotification.	Redundant Supply State - Warning

Table 16-3 Cisco IOS V1 Traps (continued)

Trap Name	Generic Type	Specific Type	Enterprise OID	Subtype Varbind OID	Subtype Varbind Value	Description	Short Description
newRoot	6	1	1.3.6.1.2.1.17	N/A	N/A	The newRoot trap indicates that the sending agent has become the new root of the Spanning Tree; the trap is sent by a bridge soon after its election as the new root, e.g., upon expiration of the Topology Change Timer,immediately subsequent to its election.Implementation of this trap is optional.	new root trap
stpxInconsistency Update	6	1	1.3.6.1.4.1.9.9.82.2	1.3.6.1.4.1.9.9.82.1.3.1.1.3	=1	A stpxPortInconsistencyUpdate notification is sent by a bridge when an instance of stpxInconsistentState is created or destroyed. That is, when an inconsistency is discovered in the VLAN's Spanning Tree for a particular port, or when such an inconsistency disappears. Note that the trap is not sent if the port transitions between different types of inconsistency.The stpxInconsistentState value indicates the type of inconsistency which now exists/no longer exists for the relevant VLAN on the relevant port.	stpx port inconsistency discovered

Table 16-3 Cisco IOS V1 Traps (continued)

Trap Name	Generic Type	Specific Type	Enterprise OID	Subtype Varbind OID	Subtype Varbind Value	Description	Short Description
stpxInconsistency Update	6	1	1.3.6.1.4.1.9.9.82.2	1.3.6.1.4.1.9.9.82.1.3.1.1.4	=2	A stpxPortInconsistencyUpdate notification is sent by a bridge when an instance of stpxInconsistentState is created or destroyed. That is, when an inconsistency is discovered in the VLAN's Spanning Tree for a particular port, or when such an inconsistency disappears. Note that the trap is not sent if the port transitions betweendifferent types of inconsistency.The stpxInconsistentState value indicates the type of inconsistency which now exists/no longer exists for the relevant VLAN on the relevant port.	stpx port inconsistency resolved

Table 16-3 Cisco IOS V1 Traps (continued)

Trap Name	Generic Type	Specific Type	Enterprise OID	Subtype Varbind OID	Subtype Varbind Value	Description	Short Description
stpxLoopInconsistencyUpdate	6	3	1.3.6.1.4.1.9.9.82.2	1.3.6.1.4.1.9.9.82.1.8.2.1.3	= 1	A stpxLoopInconsistencyUpdate notification is sent by a bridge when an instance of stpxLoopInconsistencyState is created or destroyed. That is, when an loop-inconsistency is discovered in the VLAN's or instance's Spanning Tree for a particular port, or when such a loop-inconsistency disappears. For creation, the value of stpxLoopInconsistencyState in the notification is true(1); for deletion, the value is false(2).The object value of stpxSpanningTreeType indicates which Spanning Tree protocol is running when an instanceof stpxLoopInconsistencyState is created or destroyed.	stpx loop inconsistency discovered

Table 16-3 Cisco IOS V1 Traps (continued)

Trap Name	Generic Type	Specific Type	Enterprise OID	Subtype Varbind OID	Subtype Varbind Value	Description	Short Description
stpxLoopInconsistencyUpdate	6	3	1.3.6.1.4.1.9.9.82.2	1.3.6.1.4.1.9.9.82.1.8.2.1.3	= 2	A stpxLoopInconsistencyUpdate notification is sent by a bridge when an instance of stpxLoopInconsistencyStateis created or destroyed. That is, when an loop-inconsistency is discovered in the VLAN's or instance's Spanning Tree for a particular port, or when such a loop-inconsistency disappears. For creation, the value of stpxLoopInconsistencyState in the notification is true(1); for deletion, the value is false(2). The object value of stpxSpanningTreeType indicateswhich Spanning Tree protocol is running when an instance of stpxLoopInconsistencyState is created or destroyed.	stpx loop inconsistency resolved

Table 16-3 Cisco IOS V1 Traps (continued)

Trap Name	Generic Type	Specific Type	Enterprise OID	Subtype Varbind OID	Subtype Varbind Value	Description	Short Description
stpxRootInconsistencyUpdate	6	2	1.3.6.1.4.1.9.9.82.2	1.3.6.1.4.1.9.9.82.1.5.2.1.3	= 1	A stpxRootInconsistencyUpdate notification is sent by bridge when an instance of stpxRootInconsistencyStateis created or destroyed. That is, when an root-inconsistency is discovered in the VLAN's or instance's Spanning Tree for a particular port, or when such an root-inconsistency disappears. For creation, the value of stpxRootInconsistencyState in the notification is true(1); for deletion, the value is false(2). The object value of stpxSpanningTreeType indicates which Spanning Tree protocol is running when an instance of stpxRootInconsistencyState is created or destroyed.	stpx root inconsistency discovered

Table 16-3 Cisco IOS V1 Traps (continued)

Trap Name	Generic Type	Specific Type	Enterprise OID	Subtype Varbind OID	Subtype Varbind Value	Description	Short Description
stpxRootInconsistencyUpdate	6	2	1.3.6.1.4.1.9.9.82.2	1.3.6.1.4.1.9.9.82.1.5.2.1.3	= 2	A stpxRootInconsistencyUpdate notification is sent by a bridge when an instance of stpxRootInconsistencyState is created or destroyed. That is, when an root-inconsistency is discovered in the VLAN's or instance's Spanning Tree for a particular port, or when such an root-inconsistency disappears. For creation, the value of stpxRootInconsistencyState in the notification is true(1); for deletion, the value is false(2).The object value of stpxSpanningTreeType indicates which Spanning Tree protocol is running when an instance of stpxRootInconsistencyState is created or destroyed.	stpx root inconsistency resolved

Table 16-3 Cisco IOS V1 Traps (continued)

Trap Name	Generic Type	Specific Type	Enterprise OID	Subtype Varbind OID	Subtype Varbind Value	Description	Short Description
vtpConfigRevNumberError	6	1	1.3.6.1.4.1.9.9.46.2	N/A	N/A	A configuration revision number error notification signifies that a device has incremented its vtpConfigRevNumberErrors counter. Generation of this notification is suppressed if the vtpNotificationsEnabled has the value 'false'. The device must throttle the generation of consecutive vtpConfigRevNumberError notifications so that there is at least a five-second gap between notification of this type. When notification are throttled, they are dropped, not queued for sending at a future time. (Note that 'generating' a notification means sending to all configured recipients.)	vtp configuration revision number error trap

Table 16-3 Cisco IOS V1 Traps (continued)

Trap Name	Generic Type	Specific Type	Enterprise OID	Subtype Varbind OID	Subtype Varbind Value	Description	Short Description
vtpConfigDigestError	6	2	1.3.6.1.4.1.9.9.46.2	N/A	N/A	A configuration digest error notification signifies that a device has incremented its vtpConfigDigestErrors counter. Generation of this notification is suppressed if the vtpNotificationsEnabled has the value 'false'.The device must throttle the generation of consecutive vtpConfigDigestError notifications so that there is at least a five-second gap between notification of this type. When notification are throttled, they are dropped, not queued for sending at a future time. (Note that 'generating' a notification means sending to all configured recipients).	vtp configuration digest error trap

Table 16-3 Cisco IOS V1 Traps (continued)

Trap Name	Generic Type	Specific Type	Enterprise OID	Subtype Varbind OID	Subtype Varbind Value	Description	Short Description
ciscoEnvMonShutdownNotification	6	1	1.3.6.1.4.1.9.9.13.3	N/A	N/A	A ciscoEnvMonShutdownNotification is sent if the environmental monitor detects a test point reaching a critical state and is about to initiate a shutdown. This notification contains no objects so that it may be encoded and sent in the shortest amount of time possible. Even so, management applications should not rely on receiving such a notification as it may not be sent before the shutdown completes.	cisco EnvMon Shutdown Notification Trap
caemTemperatureNotification	6	1	1.3.6.1.4.1.9.9.61.2	N/A	N/A	A caemTemperatureNotification is sent if the over temperature condition is detected in the managed system. This is a replacement for the ciscoEnvMonTemperatureNotification trap because the information 'ciscoEnvMonTemperatureStatusValue' required by the trap is not available in the managed system.	caem Temperature Notification Trap

Table 16-3 Cisco IOS V1 Traps (continued)

Trap Name	Generic Type	Specific Type	Enterprise OID	Subtype Varbind OID	Subtype Varbind Value	Description	Short Description
caemVoltageNotification	6	2	1.3.6.1.4.1.9.9.61.2	N/A	N/A	A caemVoltageNotification is sent if the over voltage condition is detected and ciscoEnvMonVoltageState is not set to 'notPresent' in the managed system. This is a replacement for the ciscoEnvMonVoltageNotification trap because the information 'ciscoEnvMonVoltageStatusValue' required by the trap is not available in the managed system.	caem Voltage Notification Trap

Table 16-3 Cisco IOS V1 Traps (continued)

Trap Name	Generic Type	Specific Type	Enterprise OID	Subtype Varbind OID	Subtype Varbind Value	Description	Short Description
cmnMacChangedNotification	6	1	1.3.6.1.4.1.9.9.215.2	N/A	N/A	This notification is generated when there is enough MAC address information to fully occupy a maximum size SNMP trapmessage. This notification is also generated when there is at least one MAC address changed or removed and the amount of time elapsed from the previous notification is greater than the maximum wait time denoted by cmnNotificationInterval object. If there are more MAC addresses information than can fit into one cmmHistTrapContent object, then multiple notifications will be generated.	cmn Mac Changed Notification Trap
cmnMacMoveNotification	6	2	1.3.6.1.4.1.9.9.215.2	N/A	N/A	cmnMacMoveNotification is generated when a MAC address is moved between two interfaces.	cmn Mac Move Notification Trap

Table 16-3 Cisco IOS V1 Traps (continued)

Trap Name	Generic Type	Specific Type	Enterprise OID	Subtype Varbind OID	Subtype Varbind Value	Description	Short Description
vtpVersionOneDeviceDetected	6	6	1.3.6.1.4.1.9.9.46.2	N/A	N/A	A VTP version one device detected notification is generated by a device when: a) a management domain has been put into version 2 mode (as accessed by managementDomain VersionInUse). b) 15 minutes has passed since a). c) a version 1 PDU is detected on a trunk on the device that is in that management domain which has a lower revision number than the current configuration.	vtp VersionOne Device Detected trap
vtpLocalModeChanged	6	8	1.3.6.1.4.1.9.9.46.2	N/A	N/A	A vtpLocalModeChanged notification is generated by a device when the value of the object managementDomain LocalMode is changed.	vtp Local Mode Changed trap
vtpVersionInUseChanged	6	9	1.3.6.1.4.1.9.9.46.2	N/A	N/A	A vtpVersionInUseChanged notification is generated by a device when the value of the objectmanagementDomainVersionInUse is changed.	vtp VersionInUse Changed trap

Table 16-3 Cisco IOS V1 Traps (continued)

Trap Name	Generic Type	Specific Type	Enterprise OID	Subtype Varbind OID	Subtype Varbind Value	Description	Short Description
vlanTrunkPortDynamicStatusChange	6	7	1.3.6.1.4.1.9.9.46.2	1.3.6.1.4.1.9.9.46.1.6.1.1.14	= 1	A vlanTrunkPortDynamicStatusChange notification is generated by a device when the value of vlanTrunkPortDynamicStatus object has been changed.	Vlan trunk port dynamic status changed to trunking
vlanTrunkPortDynamicStatusChange	6	7	1.3.6.1.4.1.9.9.46.2	1.3.6.1.4.1.9.9.46.1.6.1.1.14	2	A vlanTrunkPortDynamicStatusChange notification is generated by a device when the value of vlanTrunkPortDynamicStatus object has been changed.	Vlan trunk port dynamic status changed to not trunking
cpsSecureMacAddrViolation	6	1	1.3.6.1.4.1.9.9.315.0	N/A	N/A	The address violation notification is generated when port security address violation is detected on a secure non-trunk, access interface (that carries a single vlan) and the cpsIfViolationAction is set to 'dropNotify'.	cps Secure MacAddr Violation Trap
cpsIfVlanSecureMacAddrViolation	6	3	1.3.6.1.4.1.9.9.315.0	N/A	N/A	The address violation notification is generated when port security address violation is detected on a multi-vlan interface and the cpsIfViolationAction is set to 'dropNotify'.	cps IfVlan Secure MacAddr Violation Trap

Table 16-3 Cisco IOS V1 Traps (continued)

Trap Name	Generic Type	Specific Type	Enterprise OID	Subtype Varbind OID	Subtype Varbind Value	Description	Short Description
clcVlanMacLimitNotif	6	1	1.3.6.1.4.1.9.9.313	N/A	N/A	Notification is sent when the number of MAC addresses (the value of clcFdbVlanMacUsage) has crossed the configured limit of MAC addresses (clcVlanMaxMacLimit) either rising above or falling below it.	cisco L2 Control VlanMacLimit Notif Trap
clcVlanMacLimitHighNotif	6	2	1.3.6.1.4.1.9.9.313	N/A	N/A	Notification is sent when the number of MAC addresses (the value of clcFdbVlanMacUsage) has crossed the configured higher threshold limit of MAC addresses (clcVlanMacLimitHigh) either rising above or falling below it.	cisco L2 Control VlanMacLimit High Notif Trap
clcIfMacLimitLowNotif	6	3	1.3.6.1.4.1.9.9.313	N/A	N/A	Notification is sent when the number of MAC addresses (the value of clcFdbIfMacUsage) has crossed the configured lower threshold limit of MAC addresses (clcIfMacLimitLow) either rising above or falling below it.	cisco L2 Control IfMacLimit Low Notif Trap

Table 16-3 Cisco IOS V1 Traps (continued)

Trap Name	Generic Type	Specific Type	Enterprise OID	Subtype Varbind OID	Subtype Varbind Value	Description	Short Description
clcIfMacLimitHigh Notif	6	4	1.3.6.1.4.1.9.9.313	N/A	N/A	Notification is sent when the number of MAC addresses (the value of clcFdbIfMacUsage) has crossed the configured higher threshold limit of MAC addresses (clcIfMacLimitHigh) either rising above or falling below it.	cisco L2 Control IfMacLimit High Notif Trap
clcIfVlanMacLimit LowNotif	6	5	1.3.6.1.4.1.9.9.313	N/A	N/A	Notification is sent when the number of MAC addresses (the value of clcFdbIfVlanMacUsage) has crossed the configured lower threshold limit of MAC addresses (clcIfVlanMacLimit Low) either rising above or falling below it.	cisco L2 Control IfVlanMacLimit Low Notif Trap
clcIfVlanMacLimit HighNotif	6	6	1.3.6.1.4.1.9.9.313	N/A	N/A	Notification is sent when the number of MAC addresses (the value of clcFdbIfVlanMacUsage) has crossed the configured higher threshold limit of MAC addresses (clcIfVlanMacLimit High) either rising above or falling below it.	cisco L2 Control IfVlanMacLimit High Notif Trap

Table 16-3 Cisco IOS V1 Traps (continued)

Trap Name	Generic Type	Specific Type	Enterprise OID	Subtype Varbind OID	Subtype Varbind Value	Description	Short Description
csbSourceAlertEvent	6	1	1.3.6.1.4.1.9.9.658	1.3.6.1.4.1.9.9.658.1.2	= 1	This notification is generated when after SIP/H.248 call establishment with one party, the media packets are received from some unexpected source/party (or some wrong/unexpected IP address). This is to alert that some unwanted data packets are received by the system from an undesirable IP/port.	Cisco SBC source alert off trap
csbSourceAlertEvent	6	1	1.3.6.1.4.1.9.9.658	1.3.6.1.4.1.9.9.658.1.2	!= (1 or 7)	This notification is generated when after SIP/H.248 call establishment with one party, the media packets are received from some unexpected source/party (or some wrong/unexpected IPaddress). This is to alert that some unwanted data packets are received by the system from an undesirable IP/port.	Cisco SBC source alert on trap

Table 16-3 Cisco IOS V1 Traps (continued)

Trap Name	Generic Type	Specific Type	Enterprise OID	Subtype Varbind OID	Subtype Varbind Value	Description	Short Description
csbSourceAlertEvent	6	1	1.3.6.1.4.1.9.9.658	1.3.6.1.4.1.9.9.658.1.2	= 7	This notification is generated when after SIP/H.248 call establishment with one party, the media packets are received from some unexpected source/party (or some wrong/unexpected IP address). This is to alert that some unwanted data packets are received by the system from an undesirable IP/port.	Cisco SBC source alert informational trap

Table 16-3 Cisco IOS V1 Traps (continued)

Trap Name	Generic Type	Specific Type	Enterprise OID	Subtype Varbind OID	Subtype Varbind Value	Description	Short Description
csbDynamicBlackListEvent	6	2	1.3.6.1.4.1.9.9.658	1.3.6.1.4.1.9.9.658.1.2	= 1	This notification is generated when a source is added to or removed from the blacklist table. Dynamic blacklists put in place automatically (subject to a set of configurable constraints) by the SBC when it detects an attempt to disrupt traffic flowing through it. Dynamic blacklisting does not require management interference. Blacklist table is restricted only to SBC service. This table is not made available to NM. For more Information on Dynamic Blacklisting refer to the following link: http://lbj.cisco.com/push_targets1/ucdit/cc/td/doc/product/ioxsoft/iox34/cgcr34/sbc_c34/sbc34dos.htm or Search cisco.com using keywords 'DoS Prevention and Dynamic Blacklisting'.	Cisco SBC dynamic blacklist trap
csbAdjacencyStatus	6	3	1.3.6.1.4.1.9.9.658	1.3.6.1.4.1.9.9.658.1.2	= 1	This notification is generated when an Adjacency is attached to (or detached from) the SBC.	Cisco SBC adjacency state up trap

Table 16-3 Cisco IOS V1 Traps (continued)

Trap Name	Generic Type	Specific Type	Enterprise OID	Subtype Varbind OID	Subtype Varbind Value	Description	Short Description
csbAdjacencyStatus	6	3	1.3.6.1.4.1.9.9.658	1.3.6.1.4.1.9.9.658.1.2	!= (1 or 7)	This notification is generated when an Adjacency is attached to (or detached from) the SBC.	Cisco SBC adjacency state down trap
csbAdjacencyStatus	6	3	1.3.6.1.4.1.9.9.658	1.3.6.1.4.1.9.9.658.1.2	= 7	This notification is generated when an Adjacency is attached to (or detached from) the SBC.	Cisco SBC adjacency state informational trap
csbServiceStateEvent	6	4	1.3.6.1.4.1.9.9.658	1.3.6.1.4.1.9.9.658.1.28	= 1	This notification is generated when there is a change in the state of a service card. The changes in the service state are: -Active -Standby	Cisco SBC service state up trap
csbServiceStateEvent	6	4	1.3.6.1.4.1.9.9.658	1.3.6.1.4.1.9.9.658.1.28	= 3	This notification is generated when there is a change in the state of a service card. The changes in the service state are: -Active -Standby	Cisco SBC service state down trap
csbServiceStateEvent	6	4	1.3.6.1.4.1.9.9.658	1.3.6.1.4.1.9.9.658.1.28	= 2	This notification is generated when there is a change in the state of a service card. The changes in the service state are: -Active -Standby	Cisco SBC service state informational trap
csbSystemCongestionAlarmEvent	6	5	1.3.6.1.4.1.9.9.658	1.3.6.1.4.1.9.9.658.1.2	= 1	This notification is generated when CPU/Memory congestion in SBC is raised or cleared.	Cisco SBC system congestion cleared trap

Table 16-3 Cisco IOS V1 Traps (continued)

Trap Name	Generic Type	Specific Type	Enterprise OID	Subtype Varbind OID	Subtype Varbind Value	Description	Short Description
csbSystemCongestionAlarmEvent	6	5	1.3.6.1.4.1.9.9.658	1.3.6.1.4.1.9.9.658.1.2	!= (1 or 7)	This notification is generated when CPU/Memory congestion in SBC is raised or cleared.	Cisco SBC system congestion raised trap
csbSystemCongestionAlarmEvent	6	5	1.3.6.1.4.1.9.9.658	1.3.6.1.4.1.9.9.658.1.2	= 7	This notification is generated when CPU/Memory congestion in SBC is raised or cleared.	Cisco SBC system congestion informational trap
csbSLAViolationRev1	6	10	1.3.6.1.4.1.9.9.658	1.3.6.1.4.1.9.9.658.1.2	= 1	This notification is generated when there is a violation of Service Level Agreement as described in the policy tables. The typical service level agreements include maximum number of calls allowed, max call rate, max bandwidth etc. This notification replaces the csbSLAViolation notification.	Cisco SBC SLA violation off trap
csbSLAViolationRev1	6	10	1.3.6.1.4.1.9.9.658	1.3.6.1.4.1.9.9.658.1.2	!= (1 or 7)	This notification is generated when there is a violation of Service Level Agreement as described in the policy tables. The typical service level agreements include maximum number of calls allowed, max call rate, max bandwidth etc. This notification replaces the csbSLAViolation notification.	Cisco SBC SLA violation on trap

Table 16-3 Cisco IOS V1 Traps (continued)

Trap Name	Generic Type	Specific Type	Enterprise OID	Subtype Varbind OID	Subtype Varbind Value	Description	Short Description
csbSLAViolationRev1	6	10	1.3.6.1.4.1.9.9.658	1.3.6.1.4.1.9.9.658.1.2	= 7	This notification is generated when there is a violation of Service Level Agreement as described in the policy tables. The typical service level agreements include maximum number of calls allowed, max call rate, max bandwidth etc. This notification replaces the csbSLAViolation notification.	Cisco SBC SLA violation informational trap
csbRadiusConnectionStatus	6	7	1.3.6.1.4.1.9.9.658	1.3.6.1.4.1.9.9.658.1.2	= 1	This notification is generated when the connection to the radius server changes (connected or disconnected).	Cisco SBC radius connection state up trap
csbRadiusConnectionStatus	6	7	1.3.6.1.4.1.9.9.658	1.3.6.1.4.1.9.9.658.1.2	!= (1 or 7)	This notification is generated when the connection to the radius server changes (connected or disconnected).	Cisco SBC radius connection state down trap
csbRadiusConnectionStatus	6	7	1.3.6.1.4.1.9.9.658	1.3.6.1.4.1.9.9.658.1.2	= 7	This notification is generated when the connection to the radius server changes (connected or disconnected).	Cisco SBC radius connection state informational trap
csbH248ControllerStatus	6	9	1.3.6.1.4.1.9.9.658	1.3.6.1.4.1.9.9.658.1.2	= 1	This notification is generated when in distributed deployment model, a DBE is attached or detached from the SBC.	Cisco SBC H248 controller state up trap

Table 16-3 Cisco IOS V1 Traps (continued)

Trap Name	Generic Type	Specific Type	Enterprise OID	Subtype Varbind OID	Subtype Varbind Value	Description	Short Description
csbH248Controller Status	6	9	1.3.6.1.4.1.9.9.658	1.3.6.1.4.1.9.9.658.1.2	!= (1 or 7)	This notification is generated when in distributed deployment model, a DBE is attached or detached from the SBC.	Cisco SBC H248 controller state down trap
csbH248Controller Status	6	9	1.3.6.1.4.1.9.9.658	1.3.6.1.4.1.9.9.658.1.2	= 7	This notification is generated when in distributed deployment model, a DBE is attached or detached from the SBC.	Cisco SBC H248 controller state informational trap

Cisco IOS V2/V3 Traps

Table 16-4 lists the Cisco IOS SNMP V2/V3 traps supported in Prime Network. For associated event types, event subtypes, and Prime Network registry parameters, use the link under Short Description or see Table 16-20.

Table 16-4 Cisco IOS V2/V3 Traps

Trap Name	Trap OID	Subtype Varbind OID	Subtype Varbind Value	Description	Short Description
cbfDefineFile Completion	1.3.6.1.4.1.9.9.81.2.0.1	N/A	N/A	A cbfDefineFileCompletion notification is sent on the following conditions: completion of a file consumption operation in case of ephemeral files: completion of file creation operation in case of volatile or permanent files: any error during file creation.	CBF File operation state indicator
cbgpBackwardTransition	1.3.6.1.4.1.9.9.187.0.2	1.3.6.1.4.1.9.9.187.0.2	!= (1or 6)	The cbgpBackwardTransition Event is generated when the BGP FSM moves from a higher numbered state to a lower numbered state. The bgpPeerRemoteAddr value is attached to the notification Object Identifier.	Cisco BGP backward transition trap
cbgpFsmStateChange	1.3.6.1.4.1.9.9.187.0.1	1.3.6.1.4.1.9.9.187.0.2	= 1	The BGP cbgpFsmStateChange notification is generated for every BGP FSM state change.	Cisco BGP down trap

Table 16-4 Cisco IOS V2/V3 Traps (continued)

Trap Name	Trap OID	Subtype Varbind OID	Subtype Varbind Value	Description	Short Description
cbgpFsmStateChange	1.3.6.1.4.1.9.9.187.0.1	1.3.6.1.4.1.9.9.187.0.2	= 6	The BGP cbgpFsmStateChange notification is generated for every BGP FSM state change.	Cisco BGP established trap
cbgpPrefixThresholdExceeded	1.3.6.1.4.1.9.9.187.0.3	N/A	N/A	The cbgpPrfefixMaxThresholdExceeded notification is generated when prefix count exceeds the configured warning threshold on a session for an address family	Cisco BGP prefix threshold exceeded
cbgpPrefixThresholdClear	1.3.6.1.4.1.9.9.187.0.4	N/A	N/A	The cbgpPrefixThresholdClear notification is generated when prefix count drops below the configured clear threshold on a session for an address family once cbgpPrefixThresholdExceeded is generated. This won't be generated if the peer session goes down after the generation of bgpPrefixThresholdExceeded. The bgpPeerRemoteAddr, bgpPeerAddrFamilyAfi and cbgpPeerAddrFamilySafi values are attached to the notification Object Identifier.	Cisco BGP prefix threshold clear
ccCopyCompletion	1.3.6.1.4.1.9.9.96.2.1.1	N/A	N/A	A ccCopyCompletion trap is sent at the completion of a config-copy request. The ccCopyFailCause is not instantiated, and hence not included in a trap, when the ccCopyState is success	Config-copy request completion
ciscoConfigManEvent	1.3.6.1.4.1.9.9.43.2.0.1	N/A	N/A	Notification of a configuration management event as recorded in ccmHistoryEventTable.	Cisco Configuration management event notification
cefcFanTrayStatusChange	1.3.6.1.4.1.9.9.117.2.0.6	1.3.6.1.4.1.9.9.117.1.4.1.1.1	!=2	This notification is generated when the value of cefcFanTrayOperStatus changes.	cefc fan-tray oper status down
cefcFanTrayStatusChange	1.3.6.1.4.1.9.9.117.2.0.6	1.3.6.1.4.1.9.9.117.1.4.1.1.1	=2	This notification is generated when the value of cefcFanTrayOperStatus changes.	cefc fan-tray oper status up
cefcFRUInserted	1.3.6.1.4.1.9.9.117.2.0.3	N/A	N/A	The cecfFRUInserted notification indicates that a FRU was inserted. The varbind for this notification indicates the entPhysicalIndex of the inserted FRU, and the entPhysicalIndex of the FRU's container.	cefc FRU inserted

Table 16-4 Cisco IOS V2/V3 Traps (continued)

Trap Name	Trap OID	Subtype Varbind OID	Subtype Varbind Value	Description	Short Description
cefcFRURemoved	1.3.6.1.4.1.9.9.117.2.0.4	N/A	N/A	The cefcFRURemoved notification indicates that a FRU was removed. The varbind for this notification indicates the entPhysicalIndex of the removed FRU, and the entPhysicalIndex of the FRU's container.	cefc FRU removed
cefcModuleStatusChange	1.3.6.1.4.1.9.9.117.2.0.1	1.3.6.1.4.1.9.9.117.1.2.1.1.2	!=2	This notification is generated when the value of cefcModuleOperStatus changes. It can be utilized by an NMS to update the status of the module it is managing.	cefc module oper status down
cefcModuleStatusChange	1.3.6.1.4.1.9.9.117.2.0.1	1.3.6.1.4.1.9.9.117.1.2.1.1.2	=2	This notification is generated when the value of cefcModuleOperStatus changes. It can be utilized by an NMS to update the status of the module it is managing.	cefc module oper status up
cefcPowerStatusChange	1.3.6.1.4.1.9.9.117.2.0.2	1.3.6.1.4.1.9.9.117.1.1.2.1.2	!=2	The cefcFRUPowerStatusChange notification indicates that the power status of a FRU has changed. The varbind for this notification indicates the entPhysicalIndex of the FRU, and the new operational-status of the FRU.	cefc power status down
cefcPowerStatusChange	1.3.6.1.4.1.9.9.117.2.0.2	1.3.6.1.4.1.9.9.117.1.1.2.1.2	=2	The cefcFRUPowerStatusChange notification indicates that the power status of a FRU has changed. The varbind for this notification indicates the entPhysicalIndex of the FRU, and the new operational-status of the FRU.	cefc power status up
entSensorThresholdNotification	1.3.6.1.4.1.9.9.91.2.0.1	N/A	N/A	The sensor value crossed the threshold listed in entSensorThresholdTable. This notification is generated once each time the sensor value crossesthe threshold.	sensor value crossed threshold in entSensorThresholdTable
ciscoFlashCopyCompletionTrap	1.3.6.1.4.1.9.9.10.1.3.0.1	1.3.6.1.4.1.9.9.10.1.2.1.1.8	!= (0 or 1 or 2)	A ciscoFlashCopyCompletionTrap is sent at the completion of a flash copy operation if such a trap was requested when the operation was initiated.	Cisco flash copy failed
ciscoFlashCopyCompletionTrap	1.3.6.1.4.1.9.9.10.1.3.0.1	1.3.6.1.4.1.9.9.10.1.2.1.1.8	=2	A ciscoFlashCopyCompletionTrap is sent at the completion of a flash copy operation if such a trap was requested when the operation was initiated.	Cisco flash copy completion
ciscoFlashCopyCompletionTrap	1.3.6.1.4.1.9.9.10.1.3.0.1	1.3.6.1.4.1.9.9.10.1.2.1.1.8	=(0 or 1)	A ciscoFlashCopyCompletionTrap is sent at the completion of a flash copy operation if such a trap was requested when the operation was initiated.	Cisco flash copy in progress

Table 16-4 Cisco IOS V2/V3 Traps (continued)

Trap Name	Trap OID	Subtype Varbind OID	Subtype Varbind Value	Description	Short Description
ciscoFlashDeviceChangeTrap	1.3.6.1.4.1.9.9.10.1.3.0.4	N/A	N/A	A ciscoFlashDeviceChangeTrap is sent whenever a removable Flash device is inserted or removed.	Cisco Flash device changed
ciscoFlashDeviceInsertedNotif	1.3.6.1.4.1.9.9.10.1.3.0.5	N/A	N/A	A ciscoFlashDeviceInsertedNotif notification is sent whenever a removable Flash device is inserted.	Cisco Flash device inserted
ciscoFlashDeviceRemovedNotif	1.3.6.1.4.1.9.9.10.1.3.0.6	N/A	N/A	A ciscoFlashDeviceRemovedNotif notification is sent whenever a removable Flash device is removed.	Cisco Flash device removed
ciscoFlashDeviceInsertedNotifRev1	1.3.6.1.4.1.9.9.10.1.3.0.7	N/A	N/A	A ciscoFlashDeviceInsertedNotifRev1 notification is sent whenever a removable Flash device is inserted.The ciscoFlashDeviceInsertedNotifRev1 depcrecates ciscoFlashDeviceInsertedNotif since it uses ciscoFlashDeviceName as a varbind which is deprecated.	Cisco Flash device inserted
ciscoFlashDeviceRemovedNotifRev1	1.3.6.1.4.1.9.9.10.1.3.0.8	N/A	N/A	A ciscoFlashDeviceRemovedNotifRev1 notification is sent whenever a removable Flash device is removed. The ciscoFlashDeviceRemovedNotifRev1 depcrecates ciscoFlashDeviceRemovedNotif since it uses ciscoFlashDeviceName as a varbind which is deprecated.	Cisco Flash device removed
ciscoFlashMiscOpCompletionTrap	1.3.6.1.4.1.9.9.10.1.3.0.3	1.3.6.1.4.1.9.9.10.1.2.3.1.4	!= (1 or 2)	A ciscoFlashMiscOpCompletionTrap is sent at the completion of a miscellaneous flash operation (enumerated in ciscoFlashMiscOpCommand) if such a trap was requested when the operation was initiated.	Cisco Flash miscellaneous operation failed
ciscoFlashMiscOpCompletionTrap	1.3.6.1.4.1.9.9.10.1.3.0.3	1.3.6.1.4.1.9.9.10.1.2.3.1.4	=2	A ciscoFlashMiscOpCompletionTrap is sent at the completion of a miscellaneous flash operation (enumerated in ciscoFlashMiscOpCommand) if such a trap was requested when the operation was initiated.	Cisco Flash miscellaneous operation completed
ciscoFlashMiscOpCompletionTrap	1.3.6.1.4.1.9.9.10.1.3.0.3	1.3.6.1.4.1.9.9.10.1.2.3.1.4	=1	A ciscoFlashMiscOpCompletionTrap is sent at the completion of a miscellaneous flash operation (enumerated in ciscoFlashMiscOpCommand) if such a trap was requested when the operation was initiated.	Cisco Flash miscellaneous operation in progress

Table 16-4 Cisco IOS V2/V3 Traps (continued)

Trap Name	Trap OID	Subtype Varbind OID	Subtype Varbind Value	Description	Short Description
chassisAlarmOff	1.3.6.1.4.1.9.5.0.6	N/A	N/A	chassis alarm trap	chassis alarm off
chassisAlarmOn	1.3.6.1.4.1.9.5.0.5	N/A	N/A	chassis alarm trap	chassis alarm on
cPimNbrLoss	1.3.6.1.4.1.9.10.119.0.2	N/A	N/A	A cPimNbrLoss trap signifies the loss of an adjacency with a neighbor. This trap should be generated when the neighbor timer expires, and the router has no other neighbors on the same interface with a lower IP address than itself.	Cisco PIM neighbor lost
ciscoPingCompletion	1.3.6.1.4.1.9.9.16.2.0.1	N/A	N/A	A ciscoPingCompleted trap is sent at the completion of a sequence of pings if such a trap was requested when the sequence was initiated.	Cisco ping completion
ciscoSonetSectionStatusChange	1.3.6.1.4.1.9.9.126.0.1	1.3.6.1.2.1.10.39.1.2.1.1.1	!=1	This notification is generated whenever the value of sonetSectionCurrentStatus changes to value more than 1.	Cisco Sonet section status changed to error
ciscoSonetSectionStatusChange	1.3.6.1.4.1.9.9.126.0.1	1.3.6.1.2.1.10.39.1.2.1.1.1	=1	This notification is generated whenever the value of sonetSectionCurrentStatus changes to value 1.	Cisco Sonet section status changed to clear
ciscoSonetLineStatusChange	1.3.6.1.4.1.9.9.126.0.2	1.3.6.1.2.1.10.39.1.3.1.1.1	!=1	This notification is generated whenever the value of sonetLineCurrentStatus changes to value more than 1.	Cisco Sonet line status changed to error
ciscoSonetLineStatusChange	1.3.6.1.4.1.9.9.126.0.2	1.3.6.1.2.1.10.39.1.3.1.1.1	=1	This notification is generated whenever the value of sonetLineCurrentStatus changes to value 1.	Cisco Sonet line status changed to clear
ciscoSonetPathStatusChange	1.3.6.1.4.1.9.9.126.0.3	1.3.6.1.2.1.10.39.2.1.1.1.2	!=1	This notification is generated whenever the value of sonetPathCurrentStatus changes to value more than 1.	Cisco Sonet path status changed to error
ciscoSonetPathStatusChange	1.3.6.1.4.1.9.9.126.0.3	1.3.6.1.2.1.10.39.2.1.1.1.2	=1	This notification is generated whenever the value of sonetPathCurrentStatus changes to value 1.	Cisco Sonet path status changed to clear
mplsLdpFailedInitSessionThresholdExceeded	1.3.6.1.4.1.9.10.65.2.0.1	N/A	N/A	This notification is generated when the value of the 'mplsLdpEntityPVLimitMismatchTrapEnable' object is 'enabled(1)' and the value of the object, 'mplsLdpEntityFailedInitSessionThreshold' has been exceeded.	MPLS LDP init session threshold exceeded Trap

Table 16-4 Cisco IOS V2/V3 Traps (continued)

Trap Name	Trap OID	Subtype Varbind OID	Subtype Varbind Value	Description	Short Description
mplsLdpSessionDown	1.3.6.1.4.1.9.10.65.2.0.4	N/A	N/A	Generation of this trap occurs when the 'mplsLdpSessionUpDownTrapEnable' object is 'enabled(1)' and the value of mplsLdpSessionState changes from 'operational(5)' to any other state.	MPLS LDP session down Trap
mplsLdpSessionUp	1.3.6.1.4.1.9.10.65.2.0.3	N/A	N/A	Generation of this trap occurs when the 'mplsLdpSessionUpDownTrapEnable' object is 'enabled(1)' and the value of mplsLdpSessionState changes from any state accept 'nonexistent(1)' to 'operational.	MPLS LDP session up Trap
mplsTunnelUp	1.3.6.1.3.95.3.0.1	N/A	N/A	This notification is generated when a mplsTunnelOperStatus object for one of the configured tunnels is about to leave the down state and transition into some other state (but not into the notPresent state). This other state is indicated by the included value of mplsTunnelOperStatus.	MPLS TE tunnel up trap
mplsTunnelDown	1.3.6.1.3.95.3.0.2	N/A	N/A	This notification is generated when a mplsTunnelOperStatus object for one of the configured tunnels is about to enter the down state from some other state (but not from the notPresent state). This other state is indicated by the included value of mplsTunnelOperStatus.	MPLS TE tunnel down trap
mplsTunnelRerouted	1.3.6.1.3.95.3.0.3	N/A	N/A	This notification is generated when a tunnel is rerouted or re-optimized. If the Actual Path is used, then this object MAY contain the new path for this tunnel some time after this trap is issued by the agent	MPLS TE tunnel rerouted trap
ciscoIpMRouteMissingHeartBeats	1.3.6.1.4.1.9.10.2.3.1.0.1	N/A	N/A	A notification is sent if a multicast router with this feature enabled failed to receive configured number of heartbeat packets from heartbeat sources within a configured time interval	Failed receive multicast router heartbeat
ciscoRFProgressionNotif	1.3.6.1.4.1.9.9.176.2.0.2	1.3.6.1.4.1.9.9.176.1.1.4.0	2	VSL link goes down or one of the chassis reloads	Cisco VSS Shelf 1 is Disabled
ciscoRFProgressionNotif	1.3.6.1.4.1.9.9.176.2.0.2	1.3.6.1.4.1.9.9.176.1.1.4.0	5	VSL link goes down or one of the chassis reloads	Cisco VSS Shelf 1 is Standby Cold

Table 16-4 Cisco IOS V2/V3 Traps (continued)

Trap Name	Trap OID	Subtype Varbind OID	Subtype Varbind Value	Description	Short Description
ciscoRFProgressionNotif	1.3.6.1.4.1.9.9.176.2.0.2	1.3.6.1.4.1.9.9.176.1.1.4.0	9	VSL link goes down or one of the chassis reloads	Cisco VSS Shelf 1 is Standby Hot
ciscoRFProgressionNotif	1.3.6.1.4.1.9.9.176.2.0.2	1.3.6.1.4.1.9.9.176.1.1.4.0	2	VSL link goes down or one of the chassis reloads	Cisco VSS Shelf 2 is Disabled
ciscoRFProgressionNotif	1.3.6.1.4.1.9.9.176.2.0.2	1.3.6.1.4.1.9.9.176.1.1.4.0	5	VSL link goes down or one of the chassis reloads	Cisco VSS Shelf 2 is Standby Cold
ciscoRFProgressionNotif	1.3.6.1.4.1.9.9.176.2.0.2	1.3.6.1.4.1.9.9.176.1.1.4.0	9	VSL link goes down or one of the chassis reloads	Cisco VSS Shelf 2 is Standby Hot
cvsVSLConnectionChangeNotif	1.3.6.1.4.1.9.9.388.0.1	1.3.6.1.4.1.9.9.388.1.3.1.1.3.71	0	when VSL connection is down	VSL Connection Changed: Down
cvsVSLConnectionChangeNotif	1.3.6.1.4.1.9.9.388.0.1	1.3.6.1.4.1.9.9.388.1.3.1.1.3.71	1	when VSL connection is up	VSL Connection Change: Up
topologyChange	1.3.6.1.2.1.17.0.2	N/A	N/A	This Notification is sent by a bridge when any of its configured ports transitions from the Learning state to the Forwarding state, or from the Forwarding state to the Blocking state.	dot1qBridge trap
cEtherCfmCcMepUp	1.3.6.1.4.1.9.9.461.0.0.1	N/A	N/A	This notification is generated in the following cases: when a remote MEP first comes up, that is when we receive CC message from that MEP for the first time; when the device receives a CC message from a MEP for which it has an expired CCDB entry; when a CC message is received for a remote MEP for which the device already has a CCDB entry and the port-state in the received CC message is different from the cached previous state	Mep up trap
cEtherCfmCcMepDown	1.3.6.1.4.1.9.9.461.0.0.2	N/A	N/A	This notification is generated when a remote MEP goes down; i.e. the entry in CCDB corresponding to this MEP times out or the device receives a CC message with zero hold-time	Mep down trap

Table 16-4 Cisco IOS V2/V3 Traps (continued)

Trap Name	Trap OID	Subtype Varbind OID	Subtype Varbind Value	Description	Short Description
coldStart	1.3.6.1.2.1.11.0.0	N/A	N/A	This trap signifies that the sending protocol entity is reinitializing itself such that the agent s configuration or the protocol entity implementation may be altered.	Cold start trap
cHsrpStateChange	1.3.6.1.4.1.9.9.106.2.0.1	1.3.6.1.4.1.9.9.106.1.2.1.1.15	= 5	A cHsrpStateChange notification is sent when a cHsrpGrpStandbyState transitions to either active or standby state, or leaves active or standby state. There will be only one notification issued when the state change is from standby to active and vice versa.	Cisco hsrp state standby
cHsrpStateChange	1.3.6.1.4.1.9.9.106.2.0.1	1.3.6.1.4.1.9.9.106.1.2.1.1.15	= 5	A cHsrpStateChange notification is sent when a cHsrpGrpStandbyState transitions to either active or standby state, or leaves active or standby state. There will be only one notification issued when the state change is from standby to active and vice versa.	Cisco hsrp state non active
cHsrpStateChange	1.3.6.1.4.1.9.9.106.2.0.1	1.3.6.1.4.1.9.9.106.1.2.1.1.15	= 6	A cHsrpStateChange notification is sent when a cHsrpGrpStandbyState transitions to either active or standby state, or leaves active or standby state. There will be only one notification issued when the state change is from standby to active and vice versa.	Cisco hsrp state active
ciscoEnvMonFanNotification	1.3.6.1.4.1.9.9.13.3.0.4	1.3.6.1.4.1.9.9.13.1.4.1.3	= 3	A ciscoEnvMonFanNotification is sent if any one of the fans in the fan array (where existent) fails. Since such a notification is usually generated before the shutdown state is reached, it can convey more data and has a better chance of being sent than does the ciscoEnvMonShutdownNotification.	Cisco Environment Monitoring Fan Notification - Critical
ciscoEnvMonFanNotification	1.3.6.1.4.1.9.9.13.3.0.4	1.3.6.1.4.1.9.9.13.1.4.1.3	= 1	A ciscoEnvMonFanNotification is sent if any one of the fans in the fan array (where existent) fails. Since such a notification is usually generated before the shutdown state is reached, it can convey more data and has a better chance of being sent than does the ciscoEnvMonShutdownNotification.	Cisco Environment Monitoring Fan Notification - Normal
ciscoEnvMonFanNotification	1.3.6.1.4.1.9.9.13.3.0.4	1.3.6.1.4.1.9.9.13.1.4.1.3	= 6	A ciscoEnvMonFanNotification is sent if any one of the fans in the fan array (where existent) fails. Since such a notification is usually generated before the shutdown state is reached, it can convey more data and has a better chance of being sent than does the ciscoEnvMonShutdownNotification.	Cisco Environment Monitoring Fan Notification - Not Functioning

Table 16-4 Cisco IOS V2/V3 Traps (continued)

Trap Name	Trap OID	Subtype Varbind OID	Subtype Varbind Value	Description	Short Description
ciscoEnvMonFanNotification	1.3.6.1.4.1.9.9.13.3.0.4	1.3.6.1.4.1.9.9.13.1.4.1.3	= 5	A ciscoEnvMonFanNotification is sent if any one of the fans in the fan array (where existent) fails. Since such a notification is usually generated before the shutdown state is reached, it can convey more data and has a better chance of being sent than does the ciscoEnvMonShutdownNotification.	Cisco Environment Monitoring Fan Notification - Not Present
ciscoEnvMonFanNotification	1.3.6.1.4.1.9.9.13.3.0.4	1.3.6.1.4.1.9.9.13.1.4.1.3	= 4	A ciscoEnvMonFanNotification is sent if any one of the fans in the fan array (where existent) fails. Since such a notification is usually generated before the shutdown state is reached, it can convey more data and has a better chance of being sent than does the ciscoEnvMonShutdownNotification.	Cisco Environment Monitoring Fan Notification - Shutdown
ciscoEnvMonFanNotification	1.3.6.1.4.1.9.9.13.3.0.4	1.3.6.1.4.1.9.9.13.1.4.1.3	= 2	A ciscoEnvMonFanNotification is sent if any one of the fans in the fan array (where existent) fails. Since such a notification is usually generated before the shutdown state is reached, it can convey more data and has a better chance of being sent than does the ciscoEnvMonShutdownNotification.	Cisco Environment Monitoring Fan Notification - Warning
ciscoEnvMonRedundantSupplyNotification	1.3.6.1.4.1.9.9.13.3.0.5	1.3.6.1.4.1.9.9.13.1.5.1.3	= 3	A ciscoEnvMonRedundantSupplyNotification is sent if the redundant power supply (where exists) fails. Since such a notification is usually generated before the shutdown state is reached, it can convey more data and has a better chance of being sent than does the ciscoEnvMonShutdownNotification.	Redundant Supply State - Critical
ciscoEnvMonRedundantSupplyNotification	1.3.6.1.4.1.9.9.13.3.0.5	1.3.6.1.4.1.9.9.13.1.5.1.3	= 1	A ciscoEnvMonRedundantSupplyNotification is sent if the redundant power supply (where exists) fails. Since such a notification is usually generated before the shutdown state is reached, it can convey more data and has a better chance of being sent than does the ciscoEnvMonShutdownNotification.	Redundant Supply State - Normal

Table 16-4 Cisco IOS V2/V3 Traps (continued)

Trap Name	Trap OID	Subtype Varbind OID	Subtype Varbind Value	Description	Short Description
ciscoEnvMonRedundantSupplyNotification	1.3.6.1.4.1.9.9.13.3.0.5	1.3.6.1.4.1.9.9.13.1.5.1.3	= 6	A ciscoEnvMonRedundantSupplyNotification is sent if the redundant power supply (where exists) fails. Since such a notification is usually generated before the shutdown state is reached, it can convey more data and has a better chance of being sent than does the ciscoEnvMonShutdownNotification.	Redundant Supply State - Not Functioning
ciscoEnvMonRedundantSupplyNotification	1.3.6.1.4.1.9.9.13.3.0.5	1.3.6.1.4.1.9.9.13.1.5.1.3	= 5	A ciscoEnvMonRedundantSupplyNotification is sent if the redundant power supply (where exists) fails. Since such a notification is usually generated before the shutdown state is reached, it can convey more data and has a better chance of being sentthan does the ciscoEnvMonShutdownNotification.	Redundant Supply State - Not Present
ciscoEnvMonRedundantSupplyNotification	1.3.6.1.4.1.9.9.13.3.0.5	1.3.6.1.4.1.9.9.13.1.5.1.3	= 4	A ciscoEnvMonRedundantSupplyNotification is sent if the redundant power supply (where exists) fails. Since such a notification is usually generated before the shutdown state is reached, it can convey more data and has a better chance of being sent than does the ciscoEnvMonShutdownNotification.	Redundant Supply State - Shutdown
ciscoEnvMonRedundantSupplyNotification	1.3.6.1.4.1.9.9.13.3.0.5	1.3.6.1.4.1.9.9.13.1.5.1.3	= 2	A ciscoEnvMonRedundantSupplyNotification is sent if the redundant power supply (where exists) fails. Since such a notification is usually generated before the shutdown state is reached, it can convey more data and has a better chance of being sent than does the ciscoEnvMonShutdownNotification.	Redundant Supply State - Warning
ciscoEnvMonTemperatureNotification	1.3.6.1.4.1.9.9.13.3.0.3	1.3.6.1.4.1.9.9.13.1.3.1.6	= 3	A ciscoEnvMonTemperatureNotification is sent if the temperature measured at a given test point is outside the normal range for the test point (i.e. is at the warning, critical, or shutdown stage). Since such a Notification is usually generated before the shutdown state is reached, it can convey more data and has a better chance of being sent than does the ciscoEnvMonShutdownNotification.	Critical Temperature

Table 16-4 Cisco IOS V2/V3 Traps (continued)

Trap Name	Trap OID	Subtype Varbind OID	Subtype Varbind Value	Description	Short Description
ciscoEnvMon TemperatureN otification	1.3.6.1.4.1.9.9.1 3.3.0.3	1.3.6.1.4.1 .9.9.13.1.3 .1.6	= 1	A ciscoEnvMonTemperatureNotification is sent if the temperature measured at a given test point is outside the normal range for the test point (i.e. is at the warning, critical, or shutdown stage). Since such a Notification is usually generated before the shutdown state is reached, it can convey more data and has a better chance of being sent than does the ciscoEnvMonShutdownNotification.	Normal Temperature
ciscoEnvMon TemperatureN otification	1.3.6.1.4.1.9.9.1 3.3.0.3	1.3.6.1.4.1 .9.9.13.1.3 .1.6	= 6	A ciscoEnvMonTemperatureNotification is sent if the temperature measured at a given test point is outside the normal range for the test point (i.e. is at the warning, critical, or shutdown stage). Since such a Notification is usually generated before the shutdown state is reached, it can convey more data and has a better chance of being sent than does the ciscoEnvMonShutdownNotification.	Not Functioning
ciscoEnvMon TemperatureN otification	1.3.6.1.4.1.9.9.1 3.3.0.3	1.3.6.1.4.1 .9.9.13.1.3 .1.6	= 5	A ciscoEnvMonTemperatureNotification is sent if the temperature measured at a given test point is outside the normal range for the test point (i.e. is at the warning, critical, or shutdown stage). Since such a Notification is usually generated before the shutdown state is reached, it can convey more data and has a better chance of being sent than does the ciscoEnvMonShutdownNotification.	Not Present
ciscoEnvMon TemperatureN otification	1.3.6.1.4.1.9.9.1 3.3.0.3	1.3.6.1.4.1 .9.9.13.1.3 .1.6	= 4	A ciscoEnvMonTemperatureNotification is sent if the temperature measured at a given test point is outside the normal range for the test point (i.e. is at the warning, critical, or shutdown stage). Since such a Notification is usually generated before the shutdown state is reached, it can convey more data and has a better chance of being sent than does the ciscoEnvMonShutdownNotification.	Critical Temperature - Device Shutdown

Table 16-4 Cisco IOS V2/V3 Traps (continued)

Trap Name	Trap OID	Subtype Varbind OID	Subtype Varbind Value	Description	Short Description
ciscoEnvMonTemperatureNotification	1.3.6.1.4.1.9.9.13.3.0.3	1.3.6.1.4.1.9.9.13.1.3.1.6	= 2	A ciscoEnvMonTemperatureNotification is sent if the temperature measured at a given test point is outside the normal range for the test point (i.e. is at the warning, critical, or shutdown stage). Since such a Notification is usually generated before the shutdown state is reached, it can convey more data and has a better chance of being sent than does the ciscoEnvMonShutdownNotification.	Temperature Rising
newRoot	1.3.6.1.2.1.17.0.1	N/A	N/A	The newRoot trap indicates that the sending agent has become the new root of the Spanning Tree; the trap is sent by a bridge soon after its election as the new root, e.g., upon expiration of the Topology Change Timer, immediately subsequent to its election. Implementation of this trap is optional.	new root trap
stpxInconsistencyUpdate	1.3.6.1.4.1.9.9.82.2.0.1	1.3.6.1.4.1.9.9.82.1.3.1.1.3	=1	A stpxPortInconsistencyUpdate notification is sent by a bridge when an instance of stpxInconsistentState is created or destroyed. That is, when an inconsistency is discovered in the VLAN's Spanning Tree for a particular port, or when such an inconsistency disappears. Note that the trap is not sent if the port transitions between different types of inconsistency. The stpxInconsistentState value indicates the type of inconsistency which now exists/no longer exists for the relevant VLAN on the relevant port.	stpx port inconsistency discovered
stpxInconsistencyUpdate	1.3.6.1.4.1.9.9.82.2.0.1	1.3.6.1.4.1.9.9.82.1.3.1.1.4	=2	A stpxPortInconsistencyUpdate notification is sent by a bridge when an instance of stpxInconsistentState is created or destroyed. That is, when an inconsistency is discovered in the VLAN's Spanning Tree for a particular port, or when such an inconsistency disappears. Note that the trap is not sent if the port transitions betweendifferent types of inconsistency. The stpxInconsistentState value indicates the type of inconsistency which now exists/no longer exists for the relevant VLAN on the relevant port.	stpx port inconsistency resolved

Table 16-4 Cisco IOS V2/V3 Traps (continued)

Trap Name	Trap OID	Subtype Varbind OID	Subtype Varbind Value	Description	Short Description
stpxLoopInconsistencyUpdate	1.3.6.1.4.1.9.9.82.2.0.3	1.3.6.1.4.1.9.9.82.1.8.2.1.3	= 1	A stpxLoopInconsistencyUpdate notification is sent by a bridge when an instance of stpxLoopInconsistencyState is created or destroyed. That is, when an loop-inconsistency is discovered in the VLAN's or instance's Spanning Tree for a particular port, or when such a loop-inconsistency disappears. For creation, the value of stpxLoopInconsistencyState in the notification is true(1); for deletion, the value is false(2). The object value of stpxSpanningTreeType indicates which Spanning Tree protocol is running when an instance of stpxLoopInconsistencyState is created or destroyed.	stpx loop inconsistency discovered
stpxLoopInconsistencyUpdate	1.3.6.1.4.1.9.9.82.2.0.3	1.3.6.1.4.1.9.9.82.1.8.2.1.3	= 2	A stpxLoopInconsistencyUpdate notification is sent by abridge when an instance of stpxLoopInconsistencyState is created or destroyed. That is, when an loop-inconsistency is discovered in the VLAN's or instance's Spanning Tree for a particular port, or when such a loop-inconsistency disappears. For creation, the value of stpxLoopInconsistencyState in the notification is true(1); for deletion, the value is false(2). The object value of stpxSpanningTreeType indicates which Spanning Tree protocol is running when an instance of stpxLoopInconsistencyState is created or destroyed.	stpx loop inconsistency resolved
stpxRootInconsistencyUpdate	1.3.6.1.4.1.9.9.82.2.0.2	1.3.6.1.4.1.9.9.82.1.5.2.1.3	= 1	A stpxRootInconsistencyUpdate notification is sent by a bridge when an instance of stpxRootInconsistencyState is created or destroyed. That is, when an root-inconsistency is discovered in the VLAN's or instance's Spanning Tree for a particular port, or when such an root-inconsistency disappears. For creation, the value of stpxRootInconsistencyState in the notification is true(1); for deletion, the value is false(2). The object value of stpxSpanningTreeType indicates which Spanning Tree protocol is running when an instance of stpxRootInconsistencyState is created or destroyed.	stpx root inconsistency discovered

Table 16-4 Cisco IOS V2/V3 Traps (continued)

Trap Name	Trap OID	Subtype Varbind OID	Subtype Varbind Value	Description	Short Description
stpxRootInconsistencyUpdate	1.3.6.1.4.1.9.9.82.2.0.2	1.3.6.1.4.1.9.9.82.1.5.2.1.3	= 2	A stpxRootInconsistencyUpdate notification is sent by a bridge when an instance of stpxRootInconsistencyState is created or destroyed. That is, when an root-inconsistency is discovered in the VLAN's or instance's Spanning Tree for a particular port, or when such an root-inconsistency disappears. For creation, the value of stpxRootInconsistencyState in the notification is true(1); for deletion, the value is false(2). The object value of stpxSpanningTreeType indicates which Spanning Tree protocol is running when an instance of stpxRootInconsistencyState is created or destroyed.	stpx root inconsistency resolved
vtpConfigRevNumberError	1.3.6.1.4.1.9.9.46.2.0.1	N/A	N/A	A configuration revision number error notification signifies that a device has incremented its vtpConfigRevNumberErrors counter. Generation of this notification is suppressed if the vtpNotificationsEnabled has the value 'false'. The device must throttle the generation of consecutive vtpConfigRevNumberError notifications so that there is at least a five-second gap between notification of this type. When notification are throttled, they are dropped, not queued for sending at a future time. (Note that 'generating' a notification means sending to all configured recipients.)	vtp configuration revision number error trap
vtpConfigDigestError	1.3.6.1.4.1.9.9.46.2.0.2	N/A	N/A	A configuration digest error notification signifies that a device has incremented its vtpConfigDigestErrors counter. Generation of this notification is suppressed if the vtpNotificationsEnabled has the value 'false'. The device must throttle the generation of consecutive vtpConfigDigestError notifications so that there is at least a five-second gap between notification of this type. When notification are throttled, they are dropped, not queued for sending at a future time. (Note that 'generating' a notification means sending to all configured recipients).	vtp configuration digest error trap

Table 16-4 Cisco IOS V2/V3 Traps (continued)

Trap Name	Trap OID	Subtype Varbind OID	Subtype Varbind Value	Description	Short Description
ciscoEnvMonShutdownNotification	1.3.6.1.4.1.9.9.13.3.0.1	N/A	N/A	A ciscoEnvMonShutdownNotification is sent if the environmental monitor detects a test point reaching a critical state and is about to initiate a shutdown. This notification contains no objects so that it may be encoded and sent in the shortest amount of time possible. Even so, management applications should not rely on receiving such a notification as it may not be sent before the shutdown completes.	cisco EnvMon Shutdown Notification Trap
caemTemperatureNotification	1.3.6.1.4.1.9.9.61.2.0.1	N/A	N/A	A caemTemperatureNotification is sent if the over temperature condition is detected in the managed system. This is a replacement for the ciscoEnvMonTemperatureNotification trap because the information 'ciscoEnvMonTemperatureStatusValue' required by the trap is not available in the managed system.	caem Temperature Notification Trap
caemVoltageNotification	1.3.6.1.4.1.9.9.61.2.0.2	N/A	N/A	A caemVoltageNotification is sent if the over voltage condition is detected and ciscoEnvMonVoltageState is not set to 'notPresent' in the managed system. This is a replacement for the ciscoEnvMonVoltageNotification trap because the information 'ciscoEnvMonVoltageStatusValue' required by the trap is not available in the managed system.	caem Voltage Notification Trap
cmnMacChangedNotification	1.3.6.1.4.1.9.9.215.2.0.1	N/A	N/A	This notification is generated when there is enough MAC address information to fully occupy a maximum size SNMP trap message. This notification is also generated when there is at least one MAC address changed or removed and the amount of time elapsed from the previous notification is greater than the maximum wait time denoted by cmnNotificationInterval object. If there are more MAC addresses information than can fit into one cmmHistTrapContent object, then multiple notifications will be generated.	cmn Mac Changed Notification Trap
cmnMacMoveNotification	1.3.6.1.4.1.9.9.215.2.0.2	N/A	N/A	cmnMacMoveNotification is generated when a MAC address is moved between two interfaces.	cmn Mac Move Notification Trap

Table 16-4 Cisco IOS V2/V3 Traps (continued)

Trap Name	Trap OID	Subtype Varbind OID	Subtype Varbind Value	Description	Short Description
vtpVersionOneDeviceDetected	1.3.6.1.4.1.9.9.46.2.0.6	N/A	N/A	A VTP version one device detected notification is generated by a device when: a) a management domain has been put into version 2 mode (as accessed by managementDomainVersionInUse). b) 15 minutes has passed since a). c) a version 1 PDU is detected on a trunk on the device that is in that management domain which has a lower revision number than the current configuration.	vtp VersionOne Device Detected trap
vtpLocalModeChanged	1.3.6.1.4.1.9.9.46.2.0.8	N/A	N/A	A vtpLocalModeChanged notification is generated by a device when the value of the object managementDomainLocalMode is changed.	vtp Local Mode Changed trap
vtpVersionInUseChanged	1.3.6.1.4.1.9.9.46.2.0.9	N/A	N/A	A vtpVersionInUseChanged notification is generated by a device when the value of the object managementDomainVersionInUse is changed.	vtp VersionInUse Changed trap
vlanTrunkPortDynamicStatusChange	1.3.6.1.4.1.9.9.46.2.0.7	1.3.6.1.4.1.9.9.46.1.6.1.1.14	= 1	A vlanTrunkPortDynamicStatusChange notification is generated by a device when the value of vlanTrunkPortDynamicStatus object has been changed.	Vlan trunk port dynamic status changed to trunking
vlanTrunkPortDynamicStatusChange	1.3.6.1.4.1.9.9.46.2.0.7	1.3.6.1.4.1.9.9.46.1.6.1.1.14	2	A vlanTrunkPortDynamicStatusChange notification is generated by a device when the value of vlanTrunkPortDynamicStatus object has been changed.	Vlan trunk port dynamic status changed to not trunking
cpsSecureMacAddrViolation	1.3.6.1.4.1.9.9.315.0.0.1	N/A	N/A	The address violation notification is generated when port security address violation is detected on a secure non trunk, access interface (that carries a single vlan) and the cpsIfViolationAction is set to 'dropNotify'.	cps Secure MacAddr Violation Trap
cpsIfVlanSecureMacAddrViolation	1.3.6.1.4.1.9.9.315.0.0.3	N/A	N/A	The address violation notification is generated when port security address violation is detected on a multi-vlan interface and the cpsIfViolationAction is set to 'dropNotify'.	cps IfVlan Secure MacAddr Violation Trap
clcVlanMacLimitNotif	1.3.6.1.4.1.9.9.313.0.1	N/A	N/A	Notification is sent when the number of MAC addresses (the value of clcFdbVlanMacUsage) has crossed the configured limit of MAC addresses (clcVlanMaxMacLimit) either rising above or falling below it.	cisco L2 Control VlanMacLimit Notif Trap

Table 16-4 Cisco IOS V2/V3 Traps (continued)

Trap Name	Trap OID	Subtype Varbind OID	Subtype Varbind Value	Description	Short Description
clcVlanMacLimitHighNotif	1.3.6.1.4.1.9.9.313.0.2	N/A	N/A	Notification is sent when the number of MAC addresses (the value of clcFdbVlanMacUsage) has crossed the configured higher threshold limit of MAC addresses (clcVlanMacLimitHigh) either rising above or falling below it.	cisco L2 Control VlanMacLimit High Notif Trap
clcIfMacLimitLowNotif	1.3.6.1.4.1.9.9.313.0.3	N/A	N/A	Notification is sent when the number of MAC addresses (the value of clcFdbIfMacUsage) has crossed the configured lower threshold limit of MAC addresses (clcIfMacLimitLow) either rising above or falling below it.	cisco L2 Control IfMacLimit Low Notif Trap
clcIfMacLimitHighNotif	1.3.6.1.4.1.9.9.313.0.4	N/A	N/A	Notification is sent when the number of MAC addresses (the value of clcFdbIfMacUsage) has crossed the configured higher threshold limit of MAC addresses (clcIfMacLimitHigh) either rising above or falling below it.	cisco L2 Control IfMacLimit High Notif Trap
clcIfVlanMacLimitLowNotif	1.3.6.1.4.1.9.9.313.0.5	N/A	N/A	Notification is sent when the number of MAC addresses (the value of clcFdbIfVlanMacUsage) has crossed the configured lower threshold limit of MAC addresses (clcIfVlanMacLimitLow) either rising above or falling below it.	cisco L2 Control IfVlanMacLimit Low Notif Trap
clcIfVlanMacLimitHighNotif	1.3.6.1.4.1.9.9.313.0.6	N/A	N/A	Notification is sent when the number of MAC addresses (the value of clcFdbIfVlanMacUsage) has crossed the configured higher threshold limit of MAC addresses (clcIfVlanMacLimitHigh) either rising above or falling below it.	cisco L2 Control IfVlanMacLimit High Notif Trap
csbSourceAlertEvent	1.3.6.1.4.1.9.9.658.0.1	1.3.6.1.4.1.9.9.658.1.2	= 1	This notification is generated when after SIP/H.248 call establishment with one party, the media packets are received from some unexpected source/party (or some wrong/unexpected IP address). This is to alert that some unwanted data packets are received by the system from an undesirable IP/port.	Cisco SBC source alert off trap

Table 16-4 Cisco IOS V2/V3 Traps (continued)

Trap Name	Trap OID	Subtype Varbind OID	Subtype Varbind Value	Description	Short Description
csbSourceAlertEvent	1.3.6.1.4.1.9.9.658.0.1	1.3.6.1.4.1.9.9.658.1.2	!= (1 or 7)	This notification is generated when after SIP/H.248 call establishment with one party, the media packets are received from some unexpected source/party (or some wrong/unexpected IP address). This is to alert that some unwanted data packets are received by the system from an undesirable IP/port.	Cisco SBC source alert on trap
csbSourceAlertEvent	1.3.6.1.4.1.9.9.658.0.1	1.3.6.1.4.1.9.9.658.1.2	= 7	This notification is generated when after SIP/H.248 call establishment with one party, the media packets are received from some unexpected source/party (or some wrong/unexpected IP address). This is to alert that some unwanted data packets are received by the system from an undesirable IP/port.	Cisco SBC source alert informational trap
csbDynamicBlackListEvent	1.3.6.1.4.1.9.9.658.0.2	1.3.6.1.4.1.9.9.658.1.2	= 1	This notification is generated when a source is added to or removed from the blacklist table. Dynamic blacklists put in place automatically (subject to a set of configurable constraints) by the SBC when it detects an attempt to disrupt traffic flowing through it. Dynamic blacklisting does not require management interference. Blacklist table is restricted only to SBC service. This table is not made available to NM. For more Information on Dynamic Blacklisting refer to the following link: http://lbj.cisco.com/push_targets1/ucdit/cc/td/doc/product/ioxsoft/iox34/cgcr34/sbc_c34/sbc34dos.htm or Search cisco.com using keywords 'DoS Prevention and Dynamic Blacklisting'.	Cisco SBC dynamic blacklist trap
csbAdjacencyStatus	1.3.6.1.4.1.9.9.658.0.3	1.3.6.1.4.1.9.9.658.1.2	= 1	This notification is generated when an Adjacency is attached to (or detached from) the SBC.	Cisco SBC adjacency state up trap
csbAdjacencyStatus	1.3.6.1.4.1.9.9.658.0.3	1.3.6.1.4.1.9.9.658.1.2	!= (1 or 7)	This notification is generated when an Adjacency is attached to (or detached from) the SBC.	Cisco SBC adjacency state down trap
csbAdjacencyStatus	1.3.6.1.4.1.9.9.658.0.3	1.3.6.1.4.1.9.9.658.1.2	= 7	This notification is generated when an Adjacency is attached to (or detached from) the SBC.	Cisco SBC adjacency state informational trap

Table 16-4 Cisco IOS V2/V3 Traps (continued)

Trap Name	Trap OID	Subtype Varbind OID	Subtype Varbind Value	Description	Short Description
csbServiceStateEvent	1.3.6.1.4.1.9.9.658.0.4	1.3.6.1.4.1.9.9.658.1.28	= 1	This notification is generated when there is a change in the state of a service card. The changes in the service state are Active and Standby.	Cisco SBC service state up trap
csbServiceStateEvent	1.3.6.1.4.1.9.9.658.0.4	1.3.6.1.4.1.9.9.658.1.28	= 3	This notification is generated when there is a change in the state of a service card. The changes in the service state are Active and Standby.	Cisco SBC service state down trap
csbServiceStateEvent	1.3.6.1.4.1.9.9.658.0.4	1.3.6.1.4.1.9.9.658.1.28	= 2	This notification is generated when there is a change in the state of a service card.The changes in the service state are Active and Standby.	Cisco SBC service state informational trap
csbSystemCongestionAlarmEvent	1.3.6.1.4.1.9.9.658.0.5	1.3.6.1.4.1.9.9.658.1.2	= 1	This notification is generated when CPU/Memory congestion in SBC is raised or cleared.	Cisco SBC system congestion cleared trap
csbSystemCongestionAlarmEvent	1.3.6.1.4.1.9.9.658.0.5	1.3.6.1.4.1.9.9.658.1.2	!= (1 or 7)	This notification is generated when CPU/Memory congestion in SBC is raised or cleared.	Cisco SBC system congestion raised trap
csbSystemCongestionAlarmEvent	1.3.6.1.4.1.9.9.658.0.5	1.3.6.1.4.1.9.9.658.1.2	= 7	This notification is generated when CPU/Memory congestion in SBC is raised or cleared.	Cisco SBC system congestion informational trap
csbSLAViolationRev1	1.3.6.1.4.1.9.9.658.0.10	1.3.6.1.4.1.9.9.658.1.2	= 1	This notification is generated when there is a violation of Service Level Agreement as described in the policy tables. The typical service level agreements include maximum number of calls allowed, max call rate, max bandwidth, and so on This notification replaces the csbSLAViolation notification.	Cisco SBC SLA violation off trap
csbSLAViolationRev1	1.3.6.1.4.1.9.9.658.0.10	1.3.6.1.4.1.9.9.658.1.2	!= (1 or 7)	This notification is generated when there is a violation of Service Level Agreement as described in the policy tables. The typical service level agreements include maximum number of calls allowed, max call rate, max bandwidth, and so on.This notification replaces the csbSLAViolation notification.	Cisco SBC SLA violation on trap
csbSLAViolationRev1	1.3.6.1.4.1.9.9.658.0.10	1.3.6.1.4.1.9.9.658.1.2	= 7	This notification is generated when there is a violation of Service Level Agreement as described in the policy tables. The typical service level agreements include maximum number of calls allowed, max call rate, max bandwidth and so on This notification replaces the csbSLAViolation notification.	Cisco SBC SLA violation informational trap

Table 16-4 Cisco IOS V2/V3 Traps (continued)

Trap Name	Trap OID	Subtype Varbind OID	Subtype Varbind Value	Description	Short Description
csbRadiusConnectionStatus	1.3.6.1.4.1.9.9.658.0.7	1.3.6.1.4.1.9.9.658.1.2	= 1	This notification is generated when the connection to the radius server changes (connected or disconnected).	Cisco SBC radius connection state up trap
csbRadiusConnectionStatus	1.3.6.1.4.1.9.9.658.0.7	1.3.6.1.4.1.9.9.658.1.2	!= (1 or 7)	This notification is generated when the connection to the radius server changes (connected or disconnected).	Cisco SBC radius connection state down trap
csbRadiusConnectionStatus	1.3.6.1.4.1.9.9.658.0.7	1.3.6.1.4.1.9.9.658.1.2	= 7	This notification is generated when the connection to the radius server changes (connected or disconnected).	Cisco SBC radius connection state informational trap
csbH248ControllerStatus	1.3.6.1.4.1.9.9.658.0.9	1.3.6.1.4.1.9.9.658.1.2	= 1	This notification is generated when in distributed deployment model, a DBE is attached or detached from the SBC.	Cisco SBC H248 controller state up trap
csbH248ControllerStatus	1.3.6.1.4.1.9.9.658.0.9	1.3.6.1.4.1.9.9.658.1.2	!= (1 or 7)	This notification is generated when in distributed deployment model, a DBE is attached or detached from the SBC.	Cisco SBC H248 controller state down trap
csbH248ControllerStatus	1.3.6.1.4.1.9.9.658.0.9	1.3.6.1.4.1.9.9.658.1.2	= 7	This notification is generated when in distributed deployment model, a DBE is attached or detached from the SBC.	Cisco SBC H248 controller state informational trap
rttMonConnectionChangeNotification	1.3.6.1.4.1.9.9.42.2.0.1	N/A	N/A	This notification is only valid when the RttMonRttType is 'echo' or 'pathEcho'.A rttMonConnectionChangeNotification indicates that a connection to a target (not to a hop along the path to a target) has failed on establishment or been lost and when reestablished. Precisely, this has resulted in rttMonCtrlOperConnectionLostOccurred changing value.	RTT Connection Change
rttMonTimeoutNotification	1.3.6.1.4.1.9.9.42.2.0.2	N/A	N/A	A rttMonTimeoutNotification indicates the occurrence of a timeout for a RTT operation, and it indicates the clearing of such a condition by a subsequent RTT operation. Precisely, this has resulted in rttMonCtrlOperTimeoutOccurred changing value. When the RttMonRttType is 'pathEcho', this notification will only be sent when the timeout occurs during an operation to the target and not to a hop along the path to the target. This also applies to the clearing of the timeout.	RTT Operation Timeout

Table 16-4 Cisco IOS V2/V3 Traps (continued)

Trap Name	Trap OID	Subtype Varbind OID	Subtype Varbind Value	Description	Short Description
rttMonThresholdNotification	1.3.6.1.4.1.9.9.42.2.0.3	N/A	N/A	A rttMonThresholdNotification indicates the occurrence of a threshold violation for a RTT operation, and it indicates the previous violation has subsided for a subsequent RTT operation. Precisely, this has resulted in rttMonCtrlOperOverThresholdOccurred changing value. When the RttMonRttType is 'pathEcho', this notification will only be sent when the threshold violation occurs during an operation to the target and not to a hop along the path to the target. This also applies to the subsiding of a threshold condition.	RTT Operation Threshold Violation
rttMonVerifyErrorNotification	1.3.6.1.4.1.9.9.42.2.0.4	N/A	N/A	A rttMonVerifyErrorNotification indicates the occurrence of a data corruption in an RTT operation.	RTT Verify Error
rttMonNotification	1.3.6.1.4.1.9.9.42.2.0.5	N/A	N/A	A rttMonNotification indicates the occurrence of a threshold violation, and it indicates the previous violation has subsided for a subsequent operation.	RTT threshold violation or clearance
rttMonLpdDiscoveryNotification	1.3.6.1.4.1.9.9.42.2.0.6	N/A	N/A	A rttMonLpdDiscoveryNotification indicates that the LSP Path Discovery to the target PE has failed, and it also indicates the clearing of such condition. Precisely this has resulted in rttMonLpdGrpStatsLPDFailOccurred changing value. When the rttMonLpdGrpStatsLPDFailOccurred is 'false', the instance value for rttMonLpdGrpStatsLPDFailCause is not valid.	RTT Lpd Discovery
rttMonLpdGrpStatusNotification	1.3.6.1.4.1.9.9.42.2.0.7	N/A	N/A	A rttMonLpdGrpStatusNotification indicates that the LPD Group status rttMonLpdGrpStatsGroupStatus has changed indicating some connectivity change to the target PE. This has resulted in rttMonLpdGrpStatsGroupStatus changing value.	RTT Lpd Grp Status
imaFailureAlarm	1.3.6.1.4.1.353.5.7.1.2.0.1	1.3.6.1.4.1.353.5.7.1.1.6	10,12,15	ima-Group-FailureAlarm v2	IMA Group Remote Failure

Table 16-4 Cisco IOS V2/V3 Traps (continued)

Trap Name	Trap OID	Subtype Varbind OID	Subtype Varbind Value	Description	Short Description
imaFailureAlarm	1.3.6.1.4.1.353.5.7.1.2.0.1	1.3.6.1.4.1.353.5.7.1.1.6	14	ima-Group-FailureAlarm v2	IMA Group Remote insufficient links trap
imaFailureAlarm	1.3.6.1.4.1.353.5.7.1.2.0.1	1.3.6.1.4.1.353.5.7.1.1.5	1	ima-Group-ClearingAlarm v2	IMA Group Up Trap
imaFailureAlarm	1.3.6.1.4.1.353.5.7.1.2.0.1	1.3.6.1.4.1.353.5.7.1.1.6	11,16	ima-Group-FailureAlarm v2	IMA Group local Failure
imaFailureAlarm	1.3.6.1.4.1.353.5.7.1.2.0.1	1.3.6.1.4.1.353.5.7.1.1.6	13	ima-Group-FailureAlarm v2	IMA Group local insufficient links trap
imaFailureAlarm	1.3.6.1.4.1.353.5.7.1.2.0.1	1.3.6.1.4.1.353.5.7.1.1.6	2	ima Link FailureAlarm v2	Ima Link Loss of delay Frame Trap
imaFailureAlarm	1.3.6.1.4.1.353.5.7.1.2.0.1	1.3.6.1.4.1.353.5.7.1.1.6	1	ima Link FailureAlarm v2	Ima Link Loss of ima Frame Trap
imaFailureAlarm	1.3.6.1.4.1.353.5.7.1.2.0.1	1.3.6.1.4.1.353.5.7.1.1.6	5,7,9	ima Link FailureAlarm v2	Ima Link Rcv Failure Trap
imaFailureAlarm	1.3.6.1.4.1.353.5.7.1.2.0.1	1.3.6.1.4.1.353.5.7.1.1.6	3	ima Link FailureAlarm v2	Ima Link Remote Failure Trap
imaFailureAlarm	1.3.6.1.4.1.353.5.7.1.2.0.1	1.3.6.1.4.1.353.5.7.1.1.5	1	ima-Link-ClearingAlarm v2	Ima Link Up Trap
imaFailureAlarm	1.3.6.1.4.1.353.5.7.1.2.0.1	1.3.6.1.4.1.353.5.7.1.1.6	4,6,8	ima Link FailureAlarm v2	Ima Link Xmt Failure Trap
Cisco-UMT-state-change-v2	1.3.6.1.4.1.9.9.483.0.2	N/A	N/A	The state of the connection between the UMTS interfaces.	Cisco UMT state Change trap
Cisco-GSM-state-change-trap-v2	1.3.6.1.4.1.9.9.483.0.1	N/A	N/A	The state of the connection between the GSM interfaces.	Cisco GSM state Change trap
Cisco-IPRAN-Backhaul-received-util-v2	1.3.6.1.4.1.9.9.483.0.3	1.3.6.1.4.1.9.9.483.1.2.2.1.1.1.3	1	When Rcvd. util changes from or to any of the following : acceptable, warning, overloaded.	IPRAN Backhaul Received Util Acceptable Trap

Table 16-4 Cisco IOS V2/V3 Traps (continued)

Trap Name	Trap OID	Subtype Varbind OID	Subtype Varbind Value	Description	Short Description
Cisco-IPRAN-Backhaul-received-util-v2	1.3.6.1.4.1.9.9.483.0.3	1.3.6.1.4.1.9.9.483.1.2.2.1.1.1.3	2	When Rcvd. util changes from or to any of the following : acceptable, warning, overloaded.	IPRAN Backhaul Received Util Warning Trap
Cisco-IPRAN-Backhaul-received-util-v2	1.3.6.1.4.1.9.9.483.0.3	1.3.6.1.4.1.9.9.483.1.2.2.1.1.1.3	3	When Rcvd. util changes from or to any of the following : acceptable, warning, overloaded.	IPRAN Backhaul Received Util Overloaded Trap
Cisco-IPRAN-Backhaul-sent-util-v2	1.3.6.1.4.1.9.9.483.0.4	1.3.6.1.4.1.9.9.483.1.2.2.1.1.1.4	1	When sent util changes from or to any of the following : acceptable, warning, overloaded.	IPRAN Backhaul Sent Util Acceptable Trap
Cisco-IPRAN-Backhaul-sent-util-v2	1.3.6.1.4.1.9.9.483.0.4	1.3.6.1.4.1.9.9.483.1.2.2.1.1.1.4	2	When sent util changes from or to any of the following : acceptable, warning, overloaded.	IPRAN Backhaul Sent Util Overloaded Trap
Cisco-IPRAN-Backhaul-sent-util-v2	1.3.6.1.4.1.9.9.483.0.4	1.3.6.1.4.1.9.9.483.1.2.2.1.1.1.4	3	When sent util changes from or to any of the following : acceptable, warning, overloaded.	IPRAN Backhaul Sent Util Warning Trap
rttMonConnectionChangeNotification	1.3.6.1.4.1.9.9.42.2.0.1	1.3.6.1.4.1.9.9.42.1.2.9.1.5	1	IPSLA echo ConnLoss Trap v2	Connection Loss detected by ipsla icmp echo trap
rttMonConnectionChangeNotification	1.3.6.1.4.1.9.9.42.2.0.1	1.3.6.1.4.1.9.9.42.1.2.9.1.5	2	IPSLA echo ConnLoss Trap v2	Connection re-establish detected by ipsla icmp echo trap
rttMonTimeoutNotification	1.3.6.1.4.1.9.9.42.2.0.2	1.3.6.1.4.1.9.9.42.1.2.9.1.6	1	IPSLA IP or LSP echo Timeout trap v2	Timeout detected by ipsla icmp echo trap
rttMonTimeoutNotification	1.3.6.1.4.1.9.9.42.2.0.2	1.3.6.1.4.1.9.9.42.1.2.9.1.6	2	IPSLA IP or LSP echo Timeout trap v2	Connection re-establish detected by ipsla icmp echo trap
rttMonThresholdNotification	1.3.6.1.4.1.9.9.42.2.0.3	1.3.6.1.4.1.9.9.42.1.2.9.1.7	1	IPSLA Threshold Notification trap v2	Threshold crossing under trap
rttMonThresholdNotification	1.3.6.1.4.1.9.9.42.2.0.3	1.3.6.1.4.1.9.9.42.1.2.9.1.7	2	IPSLA Threshold Notification trap v2	Threshold crossing over trap
rttMonVerifyErrorNotification	1.3.6.1.4.1.9.9.42.2.0.4	1.3.6.1.4.1.9.9.42.1.2.9.1.11	1	IPSLA Threshold Notification deprecated trap v2	Data corruption in rtt operation trap
rttMonVerifyErrorNotification	1.3.6.1.4.1.9.9.42.2.0.4	1.3.6.1.4.1.9.9.42.1.2.9.1.11	2	IPSLA Threshold Notification deprecated trap v2	Data corruption cleared in rtt operation trap

Table 16-4 Cisco IOS V2/V3 Traps (continued)

Trap Name	Trap OID	Subtype Varbind OID	Subtype Varbind Value	Description	Short Description
rttMonNotification	1.3.6.1.4.1.9.9.42.2.2.0.5	1.3.6.1.4.1.9.9.42.1.2.19.1.2, 1.3.6.1.4.1.9.9.42.1.2.2.1.33, 1.3.6.1.4.1.9.9.42.1.2.19.1.10	8, null, 1	RTT MON notification	Connection Loss detected by ipsla icmp echo trap
rttMonNotification	1.3.6.1.4.1.9.9.42.2.2.0.5	1.3.6.1.4.1.9.9.42.1.2.19.1.2, 1.3.6.1.4.1.9.9.42.1.2.2.1.33, 1.3.6.1.4.1.9.9.42.1.2.19.1.10	8, not null, 1	RTT MON notification	Connection Loss detected by ipsla LSP icmp echo trap
rttMonNotification	1.3.6.1.4.1.9.9.42.2.2.0.5	1.3.6.1.4.1.9.9.42.1.2.19.1.2, 1.3.6.1.4.1.9.9.42.1.2.2.1.33, 1.3.6.1.4.1.9.9.42.1.2.19.1.10	8, null, 2	RTT MON notification	Connection re-establish detected by ipsla icmp echo trap
rttMonNotification	1.3.6.1.4.1.9.9.42.2.2.0.5	1.3.6.1.4.1.9.9.42.1.2.19.1.2, 1.3.6.1.4.1.9.9.42.1.2.2.1.33, 1.3.6.1.4.1.9.9.42.1.2.19.1.10	8, not null, 2	RTT MON notification	Connection re-establish detected by ipsla LSP icmp echo trap

Table 16-4 Cisco IOS V2/V3 Traps (continued)

Trap Name	Trap OID	Subtype Varbind OID	Subtype Varbind Value	Description	Short Description
rttMonNotification	1.3.6.1.4.1.9.9.42.2.2.0.5	1.3.6.1.4.1.9.9.42.1.2.19.1.2, 1.3.6.1.4.1.9.9.42.1.2.2.1.33, 1.3.6.1.4.1.9.9.42.1.2.19.1.10	7, null, 1	RTT MON notification	Timeout detected by ipsla icmp echo trap
rttMonNotification	1.3.6.1.4.1.9.9.42.2.2.0.5	1.3.6.1.4.1.9.9.42.1.2.19.1.2, 1.3.6.1.4.1.9.9.42.1.2.2.1.33, 1.3.6.1.4.1.9.9.42.1.2.19.1.10	7, not null, 1	RTT MON notification	Timeout detected by ipsla LSP icmp echo trap
rttMonNotification	1.3.6.1.4.1.9.9.42.2.2.0.5	1.3.6.1.4.1.9.9.42.1.2.19.1.2, 1.3.6.1.4.1.9.9.42.1.2.2.1.33, 1.3.6.1.4.1.9.9.42.1.2.19.1.10	7, null, 2	RTT MON notification	Connection re-establish detected by ipsla icmp echo trap
rttMonNotification	1.3.6.1.4.1.9.9.42.2.2.0.5	1.3.6.1.4.1.9.9.42.1.2.19.1.2, 1.3.6.1.4.1.9.9.42.1.2.2.1.33, 1.3.6.1.4.1.9.9.42.1.2.19.1.10	7, not null, 2	RTT MON notification	Connection re-establish detected by ipsla LSP icmp echo trap
rttMonNotification	1.3.6.1.4.1.9.9.42.2.2.0.5	1.3.6.1.4.1.9.9.42.1.2.19.1.2, 1.3.6.1.4.1.9.9.42.1.2.19.1.10	1, 1	RTT MON notification	RTT threshold crossing over trap

Table 16-4 Cisco IOS V2/V3 Traps (continued)

Trap Name	Trap OID	Subtype Varbind OID	Subtype Varbind Value	Description	Short Description
rttMonNotification	1.3.6.1.4.1.9.9.42.2.2.0.5	1.3.6.1.4.1.9.9.42.1.2.19.1.2, 1.3.6.1.4.1.9.9.42.1.2.19.1.10	1, 2	RTT MON notification	RTT threshold crossing under trap
rttMonLpdDiscoveryNotification	1.3.6.1.4.1.9.9.42.2.2.0.6	1.3.6.1.4.1.9.9.42.1.3.7.1.13	1	IPSLA LPD Discovery trap v2	IPSLA LSP path discovery failure trap
rttMonLpdDiscoveryNotification	1.3.6.1.4.1.9.9.42.2.2.0.6	1.3.6.1.4.1.9.9.42.1.3.7.1.13	2	IPSLA LPD Discovery trap v2	IPSLA LSP path rediscovery trap
rttMonLpdGrpStatusNotification	1.3.6.1.4.1.9.9.42.2.2.0.7	1.3.6.1.4.1.9.9.42.1.3.7.1.16	3,4	IPSLA LDP Group Status trap v2	IPSLA LDP group status failure trap
rttMonLpdGrpStatusNotification	1.3.6.1.4.1.9.9.42.2.2.0.7	1.3.6.1.4.1.9.9.42.1.3.7.1.16	2	IPSLA LDP Group Status trap v2	IPSLA LDP group status restoration trap
cmplsFrrProtected	1.3.6.1.4.1.9.10.98.0.1			TE FRR trigger notification - protected trap v2	FRR Protected Trap
cmplsFrrUnProtected	1.3.6.1.4.1.9.10.98.0.2			TE FRR trigger notification - unprotected trap v2	FRR Unprotected Trap
cpwVcUp	1.3.6.1.4.1.9.10.106.2.2	N/A	N/A	This notification is generated when the cpwVcOperStatus object for one or more contiguous entries in cpwVcTable are about to enter the up(1) state from some other state.	Pseudo wire tunnel up
cpwVcDown	1.3.6.1.4.1.9.10.106.2.1	N/A	N/A	This notification is generated when the cpwVcOperStatus object for one or more contiguous entries in cpwVcTable are about to enter the down(2) state from some other state.	Pseudo wire tunnel down
crepLinkStatus	.1.3.6.1.4.1.9.9.601.0.1	1.3.6.1.4.1.9.9.601.1.2.1.1.3	5	Cisco REP link status change trap	REP port state fully operational Trap
crepLinkStatus	.1.3.6.1.4.1.9.9.601.0.1	1.3.6.1.4.1.9.9.601.1.2.1.1.3	!=5	Cisco REP link status change trap	REP port state not operational Trap
crepPortRoleChange	.1.3.6.1.4.1.9.9.601.0.3	1.3.6.1.4.1.9.9.601.1.2.1.1.4	1	Cisco REP port role change trap	REP port role failed Trap

Table 16-4 Cisco IOS V2/V3 Traps (continued)

Trap Name	Trap OID	Subtype Varbind OID	Subtype Varbind Value	Description	Short Description
crepPortRole Change	.1.3.6.1.4.1.9.9.601.0.3	1.3.6.1.4.1.9.9.601.1.2.1.1.4	!=1	Cisco REP port role change trap	REP port role clear Trap
ciscoSonetVT StatusChange	.1.3.6.1.4.1.9.9.126.0.4	1.3.6.1.2.1.10.39.3.1.1.1.2	!=1	VT Status is down	Cisco Sonet vt status changed to error
ciscoSonetVT StatusChange	.1.3.6.1.4.1.9.9.126.0.4	1.3.6.1.2.1.10.39.3.1.1.1.2	1	VT Status is down	Cisco Sonet vt status changed to clear
cEtherCfmCc MepUp	.1.3.6.1.4.1.9.9.461.0.0.1			mep up	CFM cc mep up trap
cEtherCfmCc MepDown	.1.3.6.1.4.1.9.9.461.0.0.2	.1.3.6.1.4.1.9.9.461.1.1.2.1.16	5	timeout	CFM cc mep down due to timeout trap
cEtherCfmCc MepDown	.1.3.6.1.4.1.9.9.461.0.0.2	.1.3.6.1.4.1.9.9.461.1.1.2.1.16	4	lastgasp	CFM cc mep down due to last gasp trap
cEtherCfmCc Crossconnect	.1.3.6.1.4.1.9.9.461.0.0.3	N/A	N/A	cross-connected service error trap	CFM cc cross-connected service error trap
cEtherCfmCc MepDown	.1.3.6.1.4.1.9.9.461.0.0.2	.1.3.6.1.4.1.9.9.461.1.1.2.1.16	8	cross-connected service error trap clear	CFM cc cross-connected service error trap clear
cEtherCfmCc Loop	.1.3.6.1.4.1.9.9.461.0.0.4	N/A	N/A	loop trap	CFM cc loop trap
cEtherCfmCc MepDown	.1.3.6.1.4.1.9.9.461.0.0.2	.1.3.6.1.4.1.9.9.461.1.1.2.1.16	7	loop trap clear	CFM cc loop trap clear
cEtherCfmCc ConfigError	.1.3.6.1.4.1.9.9.461.0.0.5	N/A	N/A	config error trap	CFM cc config error trap
cEtherCfmCc MepDown	.1.3.6.1.4.1.9.9.461.0.0.2	.1.3.6.1.4.1.9.9.461.1.1.2.1.16	6	config error trap clear	CFM cc config error trap clear
cEtherCfmXC heckMissing	.1.3.6.1.4.1.9.9.461.0.0.6	N/A	N/A	mep missing trap	CFM crossconnect mep missing trap
cEtherCfmXC heckUnknow n	.1.3.6.1.4.1.9.9.461.0.0.7	N/A	N/A	mep unknown trap	CFM crossconnect mep unknown trap

Table 16-4 Cisco IOS V2/V3 Traps (continued)

Trap Name	Trap OID	Subtype Varbind OID	Subtype Varbind Value	Description	Short Description
cEtherCfmCcMepDown	.1.3.6.1.4.1.9.9.461.0.0.2	.1.3.6.1.4.1.9.9.461.1.1.2.1.16	9	mep unknown trap clear	CFM crossconnect mep unknown trap clear
cEtherCfmXCheckServiceUp	.1.3.6.1.4.1.9.9.461.0.0.8	N/A	N/A	mep service up trap	CFM crossconnect mep service up trap
vrrpTrapAuthFailure	1.3.6.1.2.1.68.0.2			vrrp trap auth failure trap	Vrrp trap auth failure trap
vrrpTrapNewMaster	1.3.6.1.2.1.68.0.1			vrrp trap new master trap	Vrrp trap new master trap
cdot3OamNonThresholdEvent	1.3.6.1.4.1.9.10.136.0.2	1.3.6.1.4.1.9.10.136.1.6.1.4	256	Local or remote non-threshold crossing event is detected	OAM Non-threshold crossing link fault trap
cdot3OamNonThresholdEvent	1.3.6.1.4.1.9.10.136.0.2	1.3.6.1.4.1.9.10.136.1.6.1.4	257	Local or remote non-threshold crossing event is detected	OAM Non-threshold crossing dying gasp trap
cdot3OamNonThresholdEvent	1.3.6.1.4.1.9.10.136.0.2	1.3.6.1.4.1.9.10.136.1.6.1.4	258	Local or remote non-threshold crossing event is detected	OAM Non-threshold crossing critical Link trap
cdot3OamThresholdEvent	1.3.6.1.4.1.9.10.136.0.1	1.3.6.1.4.1.9.10.136.1.6.1.4	1	Local or remote threshold crossing event is detected	OAM threshold errored Symbol trap
cdot3OamThresholdEvent	1.3.6.1.4.1.9.10.136.0.1	1.3.6.1.4.1.9.10.136.1.6.1.4	2	Local or remote threshold crossing event is detected	OAM threshold errored Frame Period trap
cdot3OamThresholdEvent	1.3.6.1.4.1.9.10.136.0.1	1.3.6.1.4.1.9.10.136.1.6.1.4	3	Local or remote threshold crossing event is detected	OAM threshold errored Frame trap
cdot3OamThresholdEvent	1.3.6.1.4.1.9.10.136.0.1	1.3.6.1.4.1.9.10.136.1.6.1.4	4	Local or remote threshold crossing event is detected	OAM threshold errored Frame Seconds trap
ciscoEnvMonSuppStatusChangeNotif	1.3.6.1.4.1.9.9.13.3.0.9	1.3.6.1.4.1.9.9.13.1.5.1.3	3	Cisco EnvMon Supply State Notification Trap	Power Supply - Critical
ciscoEnvMonSuppStatusChangeNotif	1.3.6.1.4.1.9.9.13.3.0.9	1.3.6.1.4.1.9.9.13.1.5.1.3	1	Cisco EnvMon Supply State Notification Trap	Power Supply - Normal

Table 16-4 Cisco IOS V2/V3 Traps (continued)

Trap Name	Trap OID	Subtype Varbind OID	Subtype Varbind Value	Description	Short Description
ciscoEnvMonSuppStatusChangeNotif	1.3.6.1.4.1.9.9.13.3.0.9	1.3.6.1.4.1.9.9.13.1.5.1.3	6	Cisco EnvMon Supply State Notification Trap	Power Supply - Not Functioning
ciscoEnvMonSuppStatusChangeNotif	1.3.6.1.4.1.9.9.13.3.0.9	1.3.6.1.4.1.9.9.13.1.5.1.3	5	Cisco EnvMon Supply State Notification Trap	Power Supply - Not Present
ciscoEnvMonSuppStatusChangeNotif	1.3.6.1.4.1.9.9.13.3.0.9	1.3.6.1.4.1.9.9.13.1.5.1.3	4	Cisco EnvMon Supply State Notification Trap	Power Supply - Shutdown
ciscoEnvMonSuppStatusChangeNotif	1.3.6.1.4.1.9.9.13.3.0.9	1.3.6.1.4.1.9.9.13.1.5.1.3	2	Cisco EnvMon Supply State Notification Trap	Power Supply - Warning

Cisco IOX V1 Traps

Table 16-5 lists the Cisco IOX SNMP V1 traps supported in Prime Network. For associated event types, event subtypes, and Prime Network registry parameters, use the link under Short Description or see Table 16-21.

Table 16-5 Cisco IOX V1 Traps

Trap Name	Generic Type	Specific Type	Enterprise OID	Subtype Varbind OID	Subtype Varbind Value	Description	Short Description
cpwVcUp	6	2	1.3.6.1.4.1.9.10.106.2	N/A	N/A	This notification is generated when the cpwVcOperStatus object for one or more contiguous entries in cpwVcTable are about to enter the up(1) state from some other state.	Pseudo wire tunnel up
cpwVcDown	6	1	1.3.6.1.4.1.9.10.106.2	N/A	N/A	This notification is generated when the cpwVcOperStatus object for one or more contiguous entries in cpwVcTable are about to enter the up(1) state from some other state.	Pseudo wire tunnel down

Table 16-5 Cisco IOX V1 Traps (continued)

Trap Name	Generic Type	Specific Type	Enterprise OID	Subtype Varbind OID	Subtype Varbind Value	Description	Short Description
MIB2 V1 link down	2	0	1.3.6.1.6.3.1.1.5	N/A	N/A	A linkDown trap signifies that the sending protocol entity recognizes a failure in one of the communication links represented in the configuration of the agent. The Trap-PDU of type linkDown contains as the first element of the variable-bindings, the name and value of the ifIndex instance for the affected interface.	SNMP Link down
MIB2 V1 link up	3	0	1.3.6.1.6.3.1.1.5	N/A	N/A	A linkUp trap signifies that the sending protocol entity recognizes that one of the communication links represented in the agent's configuration has come up. The Trap-PDU of type linkUp contains as the first element of its variable-bindings, the name and value of the ifIndex instance for the affected interface.	SNMP Link up
rttMonConnectionChangeNotification	6	1	1.3.6.1.4.1.9.9.42.2	1.3.6.1.4.1.9.9.42.1.2.9.1.5	1	IPSLA echo ConnLoss Trap v2	Connection Loss detected by ipsla icmp echo trap
rttMonConnectionChangeNotification	6	1	1.3.6.1.4.1.9.9.42.2	1.3.6.1.4.1.9.9.42.1.2.9.1.5	2	IPSLA echo ConnLoss Trap v2	Connection re-establish detected by ipsla icmp echo trap
rttMonTimeoutNotification	6	2	1.3.6.1.4.1.9.9.42.2	1.3.6.1.4.1.9.9.42.1.2.9.1.6	1	IPSLA IP or LSP echo Timeout trap v2	Timeout detected by ipsla icmp echo trap
rttMonTimeoutNotification	6	2	1.3.6.1.4.1.9.9.42.2	1.3.6.1.4.1.9.9.42.1.2.9.1.6	2	IPSLA IP or LSP echo Timeout trap v2	Connection re-establish detected by ipsla icmp echo trap

Table 16-5 Cisco IOX V1 Traps (continued)

Trap Name	Generic Type	Specific Type	Enterprise OID	Subtype Varbind OID	Subtype Varbind Value	Description	Short Description
rttMonThresholdNotification	6	3	1.3.6.1.4.1.9.9.42.2	1.3.6.1.4.1.9.9.42.1.2.9.1.7	1	IPSLA Threshold Notification trap v2	Threshold crossing under trap
rttMonThresholdNotification	6	3	1.3.6.1.4.1.9.9.42.2	1.3.6.1.4.1.9.9.42.1.2.9.1.7	2	IPSLA Threshold Notification trap v2	Threshold crossing over trap
rttMonVerifyErrorNotification	6	4	1.3.6.1.4.1.9.9.42.2	1.3.6.1.4.1.9.9.42.1.2.9.1.11	1	IPSLA Threshold Notification deprecated trap v2	Data corruption in rtt operation trap
rttMonVerifyErrorNotification	6	4	1.3.6.1.4.1.9.9.42.2	1.3.6.1.4.1.9.9.42.1.2.9.1.11	2	IPSLA Threshold Notification deprecated trap v2	Data corruption cleared in rtt operation trap
rttMonNotification	6	5	1.3.6.1.4.1.9.9.42.2	1.3.6.1.4.1.9.9.42.1.2.19.1.2, 1.3.6.1.4.1.9.9.42.1.2.2.1.33, 1.3.6.1.4.1.9.9.42.1.2.19.1.10	8, null, 1	RTT MON notification	Connection Loss detected by ipsla icmp echo trap
rttMonNotification	6	5	1.3.6.1.4.1.9.9.42.2	1.3.6.1.4.1.9.9.42.1.2.19.1.2, 1.3.6.1.4.1.9.9.42.1.2.2.1.33, 1.3.6.1.4.1.9.9.42.1.2.19.1.10	8, not null, 1	RTT MON notification	Connection Loss detected by ipsla LSP icmp echo trap
rttMonNotification	6	5	1.3.6.1.4.1.9.9.42.2	1.3.6.1.4.1.9.9.42.1.2.19.1.2, 1.3.6.1.4.1.9.9.42.1.2.2.1.33, 1.3.6.1.4.1.9.9.42.1.2.19.1.10	8, null, 2	RTT MON notification	Connection re-establish detected by ipsla icmp echo trap

Table 16-5 Cisco IOX V1 Traps (continued)

Trap Name	Generic Type	Specific Type	Enterprise OID	Subtype Varbind OID	Subtype Varbind Value	Description	Short Description
rttMonNotification	6	5	1.3.6.1.4.1.9.9.42.2	1.3.6.1.4.1.9.9.42.1.2.19.1.2, 1.3.6.1.4.1.9.9.42.1.2.2.1.33, 1.3.6.1.4.1.9.9.42.1.2.19.1.10	8, not null, 2	RTT MON notification	Connection re-establish detected by ipsla LSP icmp echo trap
rttMonNotification	6	5	1.3.6.1.4.1.9.9.42.2	1.3.6.1.4.1.9.9.42.1.2.19.1.2, 1.3.6.1.4.1.9.9.42.1.2.2.1.33, 1.3.6.1.4.1.9.9.42.1.2.19.1.10	7, null, 1	RTT MON notification	Timeout detected by ipsla icmp echo trap
rttMonNotification	6	5	1.3.6.1.4.1.9.9.42.2	1.3.6.1.4.1.9.9.42.1.2.19.1.2, 1.3.6.1.4.1.9.9.42.1.2.2.1.33, 1.3.6.1.4.1.9.9.42.1.2.19.1.10	7, not null, 1	RTT MON notification	Timeout detected by ipsla LSP icmp echo trap
rttMonNotification	6	5	1.3.6.1.4.1.9.9.42.2	1.3.6.1.4.1.9.9.42.1.2.19.1.2, 1.3.6.1.4.1.9.9.42.1.2.2.1.33, 1.3.6.1.4.1.9.9.42.1.2.19.1.10	7, null, 2	RTT MON notification	Connection re-establish detected by ipsla icmp echo trap
rttMonNotification	6	5	1.3.6.1.4.1.9.9.42.2	1.3.6.1.4.1.9.9.42.1.2.19.1.2, 1.3.6.1.4.1.9.9.42.1.2.2.1.33, 1.3.6.1.4.1.9.9.42.1.2.19.1.10	7, not null, 2	RTT MON notification	Connection re-establish detected by ipsla LSP icmp echo trap

Table 16-5 Cisco IOX V1 Traps (continued)

Trap Name	Generic Type	Specific Type	Enterprise OID	Subtype Varbind OID	Subtype Varbind Value	Description	Short Description
rttMonNotification	6	5	1.3.6.1.4.1.9.9.42.2	1.3.6.1.4.1.9.9.42.1.2.19.1.2, 1.3.6.1.4.1.9.9.42.1.2.19.1.10	1, 1	RTT MON notification	RTT threshold crossing over trap
rttMonNotification	6	5	1.3.6.1.4.1.9.9.42.2	1.3.6.1.4.1.9.9.42.1.2.19.1.2, 1.3.6.1.4.1.9.9.42.1.2.19.1.10	1, 2	RTT MON notification	RTT threshold crossing under trap
rttMonLpdDiscoveryNotification	6	6	1.3.6.1.4.1.9.9.42.2	1.3.6.1.4.1.9.9.42.1.3.7.1.13	1	IPSLA LPD Discovery trap v2	IPSLA LSP path discovery failure trap
rttMonLpdDiscoveryNotification	6	6	1.3.6.1.4.1.9.9.42.2	1.3.6.1.4.1.9.9.42.1.3.7.1.13	2	IPSLA LPD Discovery trap v2	IPSLA LSP path rediscovery trap
rttMonLpdGrpStatusNotification	6	7	1.3.6.1.4.1.9.9.42.2	1.3.6.1.4.1.9.9.42.1.3.7.1.16	3,4	IPSLA LDP Group Status trap v2	IPSLA LDP group status failure trap
rttMonLpdGrpStatusNotification	6	7	1.3.6.1.4.1.9.9.42.2	1.3.6.1.4.1.9.9.42.1.3.7.1.16	2	IPSLA LDP Group Status trap v2	IPSLA LDP group status restoration trap
cmplsFrrProtected	6	1	1.3.6.1.4.1.9.10.98	N/A	N/A	TE FRR trigger notification v1	FRR Protected Trap
cmplsFrrUnProtected	6	2	1.3.6.1.4.1.9.10.98	N/A	N/A	TE FRR trigger notification v1	FRR Unprotected Trap
DSX1 V1 Line Status Change	6	1	1.3.6.1.2.1.10.18.15	1.3.6.1.2.1.10.18.6.1.10.17	2	Indicates the line status of dsx1 interface	DSX1 Far end LOF
DSX1 V1 Line Status Change	6	1	1.3.6.1.2.1.10.18.15	1.3.6.1.2.1.10.18.6.1.10.17	4	Indicates the line status of dsx1 interface	DSX1 Near end sending LOF Indication
DSX1 V1 Line Status Change	6	1	1.3.6.1.2.1.10.18.15	1.3.6.1.2.1.10.18.6.1.10.17	8	Indicates the line status of dsx1 interface	DSX1 Far end sending AIS

Table 16-5 Cisco IOX V1 Traps (continued)

Trap Name	Generic Type	Specific Type	Enterprise OID	Subtype Varbind OID	Subtype Varbind Value	Description	Short Description
DSX1 V1 Line Status Change	6	1	1.3.6.1.2.1.10.18.15	1.3.6.1.2.1.10.18.6.1.10.17	16	Indicates the line status of dsx1 interface	DSX1 Near end sending AIS
DSX1 V1 Line Status Change	6	1	1.3.6.1.2.1.10.18.15	1.3.6.1.2.1.10.18.6.1.10.17	32	Indicates the line status of dsx1 interface	DSX1 Near end LOF
DSX1 V1 Line Status Change	6	1	1.3.6.1.2.1.10.18.15	1.3.6.1.2.1.10.18.6.1.10.17	64	Indicates the line status of dsx1 interface	DSX1 Near end Loss of Signal
DSX1 V1 Line Status Change	6	1	1.3.6.1.2.1.10.18.15	1.3.6.1.2.1.10.18.6.1.10.17	128	Indicates the line status of dsx1 interface	DSX1 Near end is looped
DSX1 V1 Line Status Change	6	1	1.3.6.1.2.1.10.18.15	1.3.6.1.2.1.10.18.6.1.10.17	256	Indicates the line status of dsx1 interface	DSX1 E1 TS16 AIS
DSX1 V1 Line Status Change	6	1	1.3.6.1.2.1.10.18.15	1.3.6.1.2.1.10.18.6.1.10.17	512	Indicates the line status of dsx1 interface	DSX1 Far End Sending TS16 LOMF
DSX1 V1 Line Status Change	6	1	1.3.6.1.2.1.10.18.15	1.3.6.1.2.1.10.18.6.1.10.17	1024	Indicates the line status of dsx1 interface	DSX1 Near End Sending TS16 LOMF
DSX1 V1 Line Status Change	6	1	1.3.6.1.2.1.10.18.15	1.3.6.1.2.1.10.18.6.1.10.17	2048	Indicates the line status of dsx1 interface	DSX1 Near End detects a test code
DSX1 V1 Line Status Change	6	1	1.3.6.1.2.1.10.18.15	1.3.6.1.2.1.10.18.6.1.10.17	4096	Indicates the line status of dsx1 interface	DSX1 any line status not defined here
DSX1 V1 Line Status Change	6	1	1.3.6.1.2.1.10.18.15	1.3.6.1.2.1.10.18.6.1.10.17	8192	Indicates the line status of dsx1 interface	DSX1 Near End in Unavailable Signal State
DSX1 V1 Line Status Change	6	1	1.3.6.1.2.1.10.18.15	1.3.6.1.2.1.10.18.6.1.10.17	16384	Indicates the line status of dsx1 interface	DSX1 Carrier Equipment Out of Service
DSX1 V1 Line Status Change	6	1	1.3.6.1.2.1.10.18.15	1.3.6.1.2.1.10.18.6.1.10.17	32768	Indicates the line status of dsx1 interface	DSX1 DS2 Payload AIS
DSX1 V1 Line Status Change	6	1	1.3.6.1.2.1.10.18.15	1.3.6.1.2.1.10.18.6.1.10.17	65536	Indicates the line status of dsx1 interface	DSX1 DS2 Performance Threshold Exceeded

Table 16-5 Cisco IOX V1 Traps (continued)

Trap Name	Generic Type	Specific Type	Enterprise OID	Subtype Varbind OID	Subtype Varbind Value	Description	Short Description
DSX1 V1 Line Status Change	6	1	1.3.6.1.2.1.10.18.15	1.3.6.1.2.1.10.18.6.1.10.17	!=(2 or 4 or 8 or 16 or 32 or 64 or 128 or 256 or 512 or 1024 or 2048 or 4096 or 8192 or 16384 or 32768 or 65536 or 1)	Indicates the line status of dsx1 interface	DSX1 combination of bitmaps due to multiple failures
DSX1 V1 Line Status Change	6	1	1.3.6.1.2.1.10.18.15	1.3.6.1.2.1.10.18.6.1.10.17	1	Indicates the line status of dsx1 interface	DSX1 No alarm present
DSX3 V1 Line Status Change	6	1	1.3.6.1.2.1.10.30.15	1.3.6.1.2.1.10.30.5.1.10.17	2	Indicates the line status of dsx1 interface	DSX3 Receiving Yellow/Remote Alarm Indication
DSX3 V1 Line Status Change	6	1	1.3.6.1.2.1.10.30.15	1.3.6.1.2.1.10.30.5.1.10.17	4	Indicates the line status of dsx1 interface	DSX3 Transmitting Yellow/Remote Alarm Indication
DSX3 V1 Line Status Change	6	1	1.3.6.1.2.1.10.30.15	1.3.6.1.2.1.10.30.5.1.10.17	8	Indicates the line status of dsx1 interface	DSX3 Receiving AIS failure state
DSX3 V1 Line Status Change	6	1	1.3.6.1.2.1.10.30.15	1.3.6.1.2.1.10.30.5.1.10.17	16	Indicates the line status of dsx1 interface	DSX3 Transmitting AIS
DSX3 V1 Line Status Change	6	1	1.3.6.1.2.1.10.30.15	1.3.6.1.2.1.10.30.5.1.10.17	32	Indicates the line status of dsx1 interface	DSX3 Receiving LOF failure state
DSX3 V1 Line Status Change	6	1	1.3.6.1.2.1.10.30.15	1.3.6.1.2.1.10.30.5.1.10.17	64	Indicates the line status of dsx1 interface	DSX3 Receiving LOS failure state
DSX3 V1 Line Status Change	6	1	1.3.6.1.2.1.10.30.15	1.3.6.1.2.1.10.30.5.1.10.17	128	Indicates the line status of dsx1 interface	DSX3 Looping the received signal

Table 16-5 Cisco IOX V1 Traps (continued)

Trap Name	Generic Type	Specific Type	Enterprise OID	Subtype Varbind OID	Subtype Varbind Value	Description	Short Description
DSX3 V1 Line Status Change	6	1	1.3.6.1.2.1.10.30.15	1.3.6.1.2.1.10.30.5.1.10.17	256	Indicates the line status of dsx1 interface	DSX3 Receiving a Test Pattern
DSX3 V1 Line Status Change	6	1	1.3.6.1.2.1.10.30.15	1.3.6.1.2.1.10.30.5.1.10.17	512	Indicates the line status of dsx1 interface	DSX3 any line status not defined here
DSX3 V1 Line Status Change	6	1	1.3.6.1.2.1.10.30.15	1.3.6.1.2.1.10.30.5.1.10.17	1024	Indicates the line status of dsx1 interface	DSX3 Near End in Unavailable Signal State
DSX3 V1 Line Status Change	6	1	1.3.6.1.2.1.10.30.15	1.3.6.1.2.1.10.30.5.1.10.17	2048	Indicates the line status of dsx1 interface	DSX3 Carrier Equipment Out of Service
DSX3 V1 Line Status Change	6	1	1.3.6.1.2.1.10.30.15	1.3.6.1.2.1.10.30.5.1.10.17	!=(2 or 4 or 8 or 16 or 32 or 64 or 128 or 256 or 512 or 1024 or 2048 or 1)	Indicates the line status of dsx1 interface	DSX3 combination of bitmaps due to multiple failures
DSX3 V1 Line Status Change	6	1	1.3.6.1.2.1.10.30.15	1.3.6.1.2.1.10.30.5.1.10.17	1	Indicates the line status of dsx1 interface	DSX3 No alarm present
entConfigChange	6	1	1.3.6.1.2.1.47.2	N/A	N/A	An entConfigChange notification is generated when the value of entLastChangeTime changes. It can be utilized by an NMS to trigger logical/physical entity table maintenance polls.	Entity table configuration changed
Frame-Relay dlci status change trap v1	6	1	1.3.6.1.2.1.10.32	1.3.6.1.2.1.10.32.2.1.3	1	This trap indicates that the indicated Virtual Circuit has changed state. It has either been created or invalidated, or has toggled between the active and inactive states.	FR DLCI status invalid trap

Table 16-5 Cisco IOX V1 Traps (continued)

Trap Name	Generic Type	Specific Type	Enterprise OID	Subtype Varbind OID	Subtype Varbind Value	Description	Short Description
Frame-Relay dlci status change trap v1	6	1	1.3.6.1.2.1.10.32	1.3.6.1.2.1.10.32.2.1.3	3	This trap indicates that the indicated Virtual Circuit has changed state. It has either been created or invalidated, or has toggled between the active and inactive states.	FR DLCI status inactive trap
Frame-Relay dlci status change trap v1	6	1	1.3.6.1.2.1.10.32	1.3.6.1.2.1.10.32.2.1.3	2	This trap indicates that the indicated Virtual Circuit has changed state. It has either been created or invalidated, or has toggled between the active and inactive states.	FR DLCI status active trap
ciscoSonetVTStatusChange	6	4	1.3.6.1.4.1.9.9.126	1.3.6.1.2.1.10.39.3.1.1.1.2	!=1	VT Status is down	Cisco Sonet vt status changed to error
ciscoSonetVTStatusChange	6	4	1.3.6.1.4.1.9.9.126	1.3.6.1.2.1.10.39.3.1.1.1.2	1	VT Status is down	Cisco Sonet vt status changed to clear
vrrpTrapAuthFailure	6	2	1.3.6.1.2.1.68	N/A	N/A	vrrp trap auth failure trap	Vrrp trap auth failure trap
vrrpTrapNewMaster	6	1	1.3.6.1.2.1.68	N/A	N/A	vrrp trap new master trap	Vrrp trap new master trap
ciscoBfdSessDown	6	2	1.3.6.1.4.1.9.10.137	N/A	N/A	Cisco-BFD-session-change-trap. This trap is also generated when an LACP timer mismatch occurs in the bundle that enables BFD. Ticket is also observed in case of LACP timer mismacth happens in bundle enabled Bfd interfaces.	Cisco bfd session down trap
ciscoBfdSessUp	6	1	1.3.6.1.4.1.9.10.137	N/A	N/A	Cisco-BFD-session-change-trap. This trap is also generated when an LACP timer mismatch occurs in the bundle that enables BFD. Ticket is also observed in case of LACP timer mismacth happens in bundle enabled Bfd interfaces	Cisco bfd session up trap

Table 16-5 Cisco IOX V1 Traps (continued)

Trap Name	Generic Type	Specific Type	Enterprise OID	Subtype Varbind OID	Subtype Varbind Value	Description	Short Description
cbgpBackwardTransition	6	2	1.3.6.1.4.1.9.9.187	1.3.6.1.4.1.9.9.187.0.2	!= (1or 6)	The cbgpBackwardTransition Event is generated when the BGP FSM moves from a higher numbered state to a lower numbered state. The bgpPeerRemoteAddr value is attached to the notification object ID.	Cisco BGP backward transition trap
cbgpFsmStateChange	6	1	1.3.6.1.4.1.9.9.187	1.3.6.1.4.1.9.9.187.0.2	= 1	The BGP cbgpFsmStateChange notification is generated for every BGP FSM state change.	Cisco BGP down trap
cbgpFsmStateChange		1	1.3.6.1.4.1.9.9.187	1.3.6.1.4.1.9.9.187.0.2	= 6	The BGP cbgpFsmStateChange notification is generated for every BGP FSM state change.	Cisco BGP established trap
ccCopyCompletion	6	1	1.3.6.1.4.1.9.9.96.2.1	N/A	N/A	A ccCopyCompletion trap is sent at the completion of a config-copy request. The ccCopyFailCause is not instantiated, and hence not included in a trap, when the ccCopyState is success	Config-copy request completion
cfhBundleDownedLinkNotification	6	3	1.3.6.1.4.1.9.9.257	1.3.6.1.4.1.9.9.257.1.2.1.1.3	!=1	Fabric bundle link notification. This notification is sent if the value of cfhBundleOperStatus is 'up' and the value of cfhBundleDownedLinks is changed from 0 to nonzero or from non-zero to zero.	cfh bundle link status down
cfhBundleDownedLinkNotification	6	3	1.3.6.1.4.1.9.9.257	1.3.6.1.4.1.9.9.257.1.2.1.1.3	=1	Fabric bundle link notification. This notification is sent if the value of cfhBundleOperStatus is 'up' and the value of cfhBundleDownedLinks is changed from 0 to nonzero or from non-zero to zero.	cfh bundle link status up

Table 16-5 Cisco IOX V1 Traps (continued)

Trap Name	Generic Type	Specific Type	Enterprise OID	Subtype Varbind OID	Subtype Varbind Value	Description	Short Description
cfhBundleStateNotification	6	2	1.3.6.1.4.1.9.9.257	N/A	N/A	Fabric bundle operational state change notification. This notification is sent when the cfhBundleOperStatus state transition occurs.	cfh Fabric bundle operational state changed to Down
cfhBundleStateNotification	6	2	1.3.6.1.4.1.9.9.257	N/A	N/A	Fabric bundle operational state change notification. This notification is sent when the cfhBundleOperStatus state transition occurs.	cfh Fabric bundle operational state changed to Up
cfhPlaneStateNotification	6	1	1.3.6.1.4.1.9.9.257	1.3.6.1.4.1.9.9.257.1.2.1.1.3	!=1	Fabric plane operational state change notification. This notification is sent when the fabric plane operational state transition occurs.	cfh Fabric plane status down
cfhPlaneStateNotification	6	1	1.3.6.1.4.1.9.9.257	1.3.6.1.4.1.9.9.257.1.2.1.1.3	=1	Fabric plane operational state change notification. This notification is sent when the fabric plane operational state transition occurs.	cfh Fabric plane status up
cpwVcUp	6	2	1.3.6.1.4.1.9.10.106.2	N/A	N/A	This notification is generated when the cpwVcOperStatus object for one or more contiguous entries in cpwVcTable are about to enter the up(1) state from some other state.	Pseudo wire tunnel up
cpwVcDown	6	1	1.3.6.1.4.1.9.10.106.2	N/A	N/A	This notification is generated when the cpwVcOperStatus object for one or more contiguous entries in cpwVcTable are about to enter the down(2) state from some other state.	Pseudo wire tunnel down

Table 16-5 Cisco IOX V1 Traps (continued)

Trap Name	Generic Type	Specific Type	Enterprise OID	Subtype Varbind OID	Subtype Varbind Value	Description	Short Description
ciscoRFSwactNotif	6	1	1.3.6.1.4.1.9.9.176.2	N/A	N/A	A SWACT notification is sent by the newly active redundant unit whenever a switch of activity occurs. In the case where a SWACT event may be indistinguishable from a reset event, a network management station should use this notification to differentiate the activity.sysUpTime is the same sysUpTime defined in the RFC-1213 MIB.	Cisco RF Swap Status - Unsupported
ciscoRFSwactNotif	6	1	1.3.6.1.4.1.9.9.176.2	N/A	N/A	A SWACT notification is sent by the newly active redundant unit whenever a switch of activity occurs. In the case where a SWACT event may be indistinguishable from a reset event, a network management station should use this notification to differentiate the activity. sysUpTime is the same sysUpTime defined in the RFC-1213 MIB.	Cisco RF Swap Status - None
ciscoRFSwactNotif	6	1	1.3.6.1.4.1.9.9.176.2	N/A	N/A	A SWACT notification is sent by the newly active redundant unit whenever a switch of activity occurs. In the case where a SWACT event may be indistinguishable from a reset event, a network management station should use this notification to differentiate the activity. sysUpTime is the same sysUpTime defined in the RFC-1213 MIB.	Cisco RF Swap Status - Not Known

Table 16-5 Cisco IOX V1 Traps (continued)

Trap Name	Generic Type	Specific Type	Enterprise OID	Subtype Varbind OID	Subtype Varbind Value	Description	Short Description
ciscoRFSwactNotif	6	1	1.3.6.1.4.1.9.9.176.2	N/A	N/A	A SWACT notification is sent by the newly active redundant unit whenever a switch of activity occurs. In the case where a SWACT event may be indistinguishable from a reset event, a network management station should use this notification to differentiate the activity. sysUpTime is the same sysUpTime defined in the RFC-1213 MIB.	Cisco RF Swap Status - UserInitiated
ciscoRFSwactNotif	6	1	1.3.6.1.4.1.9.9.176.2	N/A	N/A	A SWACT notification is sent by the newly active redundant unit whenever a switch of activity occurs. In the case where a SWACT event may be indistinguishable from a reset event, a network management station should use this notification to differentiate the activity. sysUpTime is the same sysUpTime defined in the RFC-1213 MIB.	Cisco RF Swap Status - UserForced
ciscoRFSwactNotif	6	1	1.3.6.1.4.1.9.9.176.2	N/A	N/A	A SWACT notification is sent by the newly active redundant unit whenever a switch of activity occurs. In the case where a SWACT event may be indistinguishable from a reset event, a network management station should use this notification to differentiate the activity.sysUpTime is the same sysUpTime defined in the RFC-1213 MIB.	Cisco RF Swap Status - ActiveUnitFailed

Table 16-5 Cisco IOX V1 Traps (continued)

Trap Name	Generic Type	Specific Type	Enterprise OID	Subtype Varbind OID	Subtype Varbind Value	Description	Short Description
ciscoRFSwactNotif	6	1	1.3.6.1.4.1.9.9.176.2	N/A	N/A	A SWACT notification is sent by the newly active redundant unit whenever a switch of activity occurs. In the case where a SWACT event may be indistinguishable from a reset event, a network management station should use this notification to differentiate the activity. sysUpTime is the same sysUpTime defined in the RFC-1213 MIB.	Cisco RF Swap Status - ActiveUnitRemoved
atmIntfPvcFailuresTrap	6	1	1.3.6.1.2.1.37.1.14.2.1	N/A	N/A	A notification indicating that one or more PVPLs or PVCLs on this interface has failed since the last atmPvcFailuresTrap was sent. If this trap has not been sent for the last atmIntfPvcNotificationInterval, then it will be sent on the next increment of atmIntfPvcFailures.	Atm interface PVC failures trap

Cisco IOX V2/V3 Traps

Table 16-6 lists the Cisco IOX SNMP V2/V3 traps supported in Prime Network. For associated event types, event subtypes, and Prime Network registry parameters, use the link under Short Description or see Table 16-22.

Table 16-6 Cisco IOX V2/V3 Traps

Trap Name	Trap OID	Subtype Varbind OID	Subtype Varbind Value	Description	Short Description
cbfDefineFileCompletion	1.3.6.1.4.1.9.9.81.2.0.1	N/A	N/A	A cbfDefineFileCompletion notification is sent on the following conditions :	CBF File operation state indicator
cbgpBackwardTransition	1.3.6.1.4.1.9.9.187.0.2	1.3.6.1.4.1.9.9.187.0.2	!= (1or 6)	The cbgpBackwardTransition Event is generated when the BGP FSM moves from a higher numbered state to a lower numbered state. The bgpPeerRemoteAddr value is attached to the notification Object Identifier.	Cisco BGP backward transition trap
cbgpFsmStateChange	1.3.6.1.4.1.9.9.187.0.1	1.3.6.1.4.1.9.9.187.0.2	= 1	The BGP cbgpFsmStateChange notification is generated for every BGP FSM state change.	Cisco BGP down trap
cbgpFsmStateChange	1.3.6.1.4.1.9.9.187.0.1	1.3.6.1.4.1.9.9.187.0.2	= 6	The BGP cbgpFsmStateChange notification is generated for every BGP FSM state change.	Cisco BGP established trap
cbgpPrefixThresholdExceeded	1.3.6.1.4.1.9.9.187.0.3	N/A	N/A	The cbgpPrfefixMaxThresholdExceeded notification is generated when prefix count exceeds the configured warning threshold on a session for an address family	Cisco BGP prefix threshold exceeded
cbgpPrefixThresholdClear	1.3.6.1.4.1.9.9.187.0.4	N/A	N/A	The cbgpPrefixThresholdClear notification is generated when prefix count drops below the configured clear threshold on a session for an address family once cbgpPrefixThresholdExceeded is generated. This won't be generated if the peer session goes down after the generation of bgpPrefixThresholdExceeded. The bgpPeerRemoteAddr, bgpPeerAddrFamilyAfi and cbgpPeerAddrFamilySafi values are attached to the notification Object Identifier.	Cisco BGP prefix threshold clear

Table 16-6 Cisco IOX V2/V3 Traps (continued)

Trap Name	Trap OID	Subtype Varbind OID	Subtype Varbind Value	Description	Short Description
ccCopyCompletion	1.3.6.1.4.1.9.9.96.2.1.1	N/A	N/A	A ccCopyCompletion trap is sent at the completion of a config-copy request. The ccCopyFailCause is not instantiated, and hence not included in a trap, when the ccCopyState is success	Config-copy request completion
cefcFanTrayStatusChange	1.3.6.1.4.1.9.9.117.2.0.6	1.3.6.1.4.1.9.9.117.1.4.1.1.1	!=2	This notification is generated when the value of cefcFanTrayOperStatus changes.	cefc fan-tray oper status down
cefcFanTrayStatusChange	1.3.6.1.4.1.9.9.117.2.0.6	1.3.6.1.4.1.9.9.117.1.4.1.1.1	=2	This notification is generated when the value of cefcFanTrayOperStatus changes.	cefc fan-tray oper status up
cefcFRUInserted	1.3.6.1.4.1.9.9.117.2.0.3	N/A	N/A	The cecfFRUInserted notification indicates that a FRU was inserted. The varbind for this notification indicates the entPhysicalIndex of the inserted FRU, and the entPhysicalIndex of the FRU's container.	cefc FRU inserted
cefcFRURemoved	1.3.6.1.4.1.9.9.117.2.0.4	N/A	N/A	The cefcFRURemoved notification indicates that a FRU was removed. The varbind for this notification indicates the entPhysicalIndex of the removed FRU, and the entPhysicalIndex of the FRU's container.	cefc FRU removed
cefcModuleStatusChange	1.3.6.1.4.1.9.9.117.2.0.1	1.3.6.1.4.1.9.9.117.1.2.1.1.2	!=2	This notification is generated when the value of cefcModuleOperStatus changes. It can be utilized by an NMS to update the status of the module it is managing.	cefc module oper status down
cefcModuleStatusChange	1.3.6.1.4.1.9.9.117.2.0.1	1.3.6.1.4.1.9.9.117.1.2.1.1.2	=2	This notification is generated when the value of cefcModuleOperStatus changes. It can be utilized by an NMS to update the status of the module it is managing.	cefc module oper status up
cefcPowerStatusChange	1.3.6.1.4.1.9.9.117.2.0.2	1.3.6.1.4.1.9.9.117.1.1.2.1.2	!=2	The cefcFRUPowerStatusChange notification indicates that the power status of a FRU has changed. The varbind for this notification indicates the entPhysicalIndex of the FRU, and the new operational-status of the FRU.	cefc power status down
cefcPowerStatusChange	1.3.6.1.4.1.9.9.117.2.0.2	1.3.6.1.4.1.9.9.117.1.1.2.1.2	=2	The cefcFRUPowerStatusChange notification indicates that the power status of a FRU has changed. The varbind for this notification indicates the entPhysicalIndex of the FRU, and the new operational-status of the FRU.	cefc power status up

Table 16-6 Cisco IOX V2/V3 Traps (continued)

Trap Name	Trap OID	Subtype Varbind OID	Subtype Varbind Value	Description	Short Description
cfhBundleDownedLinkNotification	1.3.6.1.4.1.9.9.257.0.3	1.3.6.1.4.1.9.9.257.1.2.1.1.3	!=1	Fabric bundle link notification. This notification is sent if the value of cfhBundleOperStatus is 'up' and the value of cfhBundleDownedLinks is changed from 0 to nonzero or from non zero to zero.	cfh bundle link status down
cfhBundleDownedLinkNotification	1.3.6.1.4.1.9.9.257.0.3	1.3.6.1.4.1.9.9.257.1.2.1.1.3	=1	Fabric bundle link notification. This notification is sent if the value of cfhBundleOperStatus is 'up' and the value of cfhBundleDownedLinks is changed from 0 to nonzero or from non zero to zero.	cfh bundle link status up
cfhBundleStateNotification	1.3.6.1.4.1.9.9.257.0.2	1.3.6.1.4.1.9.9.257.1.3.3.1.4	=2	Fabric bundle operational state change notification. This notification is sent when the cfhBundleOperStatus state transition occurs.	cfh Fabric bundle operational state changed to Down
cfhBundleStateNotification	1.3.6.1.4.1.9.9.257.0.2	1.3.6.1.4.1.9.9.257.1.3.3.1.4	=1	Fabric bundle operational state change notification. This notification is sent when the cfhBundleOperStatus state transition occurs.	cfh Fabric bundle operational state changed to Up
cfhPlaneStateNotification	1.3.6.1.4.1.9.9.257.0.1	1.3.6.1.4.1.9.9.257.1.2.1.1.3	!=1	Fabric plane operational state change notification. This notification is sent when the fabric plane operational state transition occurs.	cfh Fabric plane status down
cfhPlaneStateNotification	1.3.6.1.4.1.9.9.257.0.1	1.3.6.1.4.1.9.9.257.1.2.1.1.3	=1	Fabric plane operational state change notification. This notification is sent when the fabric plane operational state transition occurs.	cfh Fabric plane status up
ciscoConfigManEvent	1.3.6.1.4.1.9.9.43.2.0.1	N/A	N/A	Notification of a configuration management event as recorded in ccmHistoryEventTable.	Cisco Configuration management event notification
ciscoFlashCopyCompletionTrap	1.3.6.1.4.1.9.9.10.1.3.0.1	1.3.6.1.4.1.9.9.10.1.2.1.1.8	!= (0 or 1 or 2)	A ciscoFlashCopyCompletionTrap is sent at the completion of a flash copy operation if such a trap was requested when the operation was initiated.	Cisco flash copy failed
ciscoFlashCopyCompletionTrap	1.3.6.1.4.1.9.9.10.1.3.0.1	1.3.6.1.4.1.9.9.10.1.2.1.1.8	=2	A ciscoFlashCopyCompletionTrap is sent at the completion of a flash copy operation if such a trap was requested when the operation was initiated.	Cisco flash copy completion
ciscoFlashCopyCompletionTrap	1.3.6.1.4.1.9.9.10.1.3.0.1	1.3.6.1.4.1.9.9.10.1.2.1.1.8	= (0 or 1)	A ciscoFlashCopyCompletionTrap is sent at the completion of a flash copy operation if such a trap was requested when the operation was initiated.	Cisco flash copy in progress

Table 16-6 Cisco IOX V2/V3 Traps (continued)

Trap Name	Trap OID	Subtype Varbind OID	Subtype Varbind Value	Description	Short Description
ciscoFlashDeviceChangeTrap	1.3.6.1.4.1.9.9.10.1.3.0.4	N/A	N/A	A ciscoFlashDeviceChangeTrap is sent whenever a removable Flash device is inserted or removed.	Cisco Flash device changed
ciscoFlashDeviceInsertedNotif	1.3.6.1.4.1.9.9.10.1.3.0.5	N/A	N/A	A ciscoFlashDeviceInsertedNotif notification is sent whenever a removable Flash device is inserted.	Cisco Flash device inserted
ciscoFlashDeviceRemovedNotif	1.3.6.1.4.1.9.9.10.1.3.0.6	N/A	N/A	A ciscoFlashDeviceRemovedNotif notification is sent whenever a removable Flash device is removed.	Cisco Flash device removed
ciscoFlashMiscOpCompletionTrap	1.3.6.1.4.1.9.9.10.1.3.0.3	1.3.6.1.4.1.9.9.10.1.2.3.1.4	!= (1 or 2)	A ciscoFlashMiscOpCompletionTrap is sent at the completion of a miscellaneous flash operation (enumerated in ciscoFlashMiscOpCommand) if such a trap was requested when the operation was initiated.	Cisco Flash miscellaneous operation failed
ciscoFlashMiscOpCompletionTrap	1.3.6.1.4.1.9.9.10.1.3.0.3	1.3.6.1.4.1.9.9.10.1.2.3.1.4	=2	A ciscoFlashMiscOpCompletionTrap is sent at the completion of a miscellaneous flash operation (enumerated in ciscoFlashMiscOpCommand) if such a trap was requested when the operation was initiated.	Cisco Flash miscellaneous operation completed
ciscoFlashMiscOpCompletionTrap	1.3.6.1.4.1.9.9.10.1.3.0.3	1.3.6.1.4.1.9.9.10.1.2.3.1.4	=1	A ciscoFlashMiscOpCompletionTrap is sent at the completion of a miscellaneous flash operation (enumerated in ciscoFlashMiscOpCommand) if such a trap was requested when the operation was initiated.	Cisco Flash miscellaneous operation in progress
ciscoPingCompletion	1.3.6.1.4.1.9.9.16.2.0.1	N/A	N/A	A ciscoPingCompleted trap is sent at the completion of a sequence of pings if such a trap was requested when the sequence was initiated.	Cisco ping completion
ciscoSonetSectionStatusChange	1.3.6.1.4.1.9.9.126.0.1	1.3.6.1.2.1.10.39.1.2.1.1.1	!=1	This notification is generated whenever the value of sonetSectionCurrentStatus changes to value more than 1.	Cisco Sonet section status changed to error
ciscoSonetSectionStatusChange	1.3.6.1.4.1.9.9.126.0.1	1.3.6.1.2.1.10.39.1.2.1.1.1	=1	This notification is generated whenever the value of sonetSectionCurrentStatus changes to value 1.	Cisco Sonet section status changed to clear

Table 16-6 Cisco IOX V2/V3 Traps (continued)

Trap Name	Trap OID	Subtype Varbind OID	Subtype Varbind Value	Description	Short Description
ciscoSonetLine StatusChange	1.3.6.1.4.1. 9.9.126.0.2	1.3.6.1.2.1.1 0.39.1.3.1.1. 1	!=1	This notification is generated whenever the value of sonetLineCurrentStatus changes to value more than 1.	Cisco Sonet line status changed to error
ciscoSonetLine StatusChange	1.3.6.1.4.1. 9.9.126.0.2	1.3.6.1.2.1.1 0.39.1.3.1.1. 1	=1	This notification is generated whenever the value of sonetLineCurrentStatus changes to value 1.	Cisco Sonet line status changed to clear
ciscoSonetPath StatusChange	1.3.6.1.4.1. 9.9.126.0.3	1.3.6.1.2.1.1 0.39.2.1.1.1. 2	!=1	This notification is generated whenever the value of sonetPathCurrentStatus changes to value more than 1.	Cisco Sonet path status changed to error
ciscoSonetPath StatusChange	1.3.6.1.4.1. 9.9.126.0.3	1.3.6.1.2.1.1 0.39.2.1.1.1. 2	=1	This notification is generated whenever the value of sonetPathCurrentStatus changes to value 1.	Cisco Sonet path status changed to clear
clogMessageG enerated	1.3.6.1.4.1. 9.9.41.2.0.1	N/A	N/A	When a syslog message is generated by the device a clogMessageGenerated notification is sent. The sending of these notifications can be enabled/disabled via the clogNotificationsEnabled object.	Cisco syslog message generated
cPimNbrLoss	1.3.6.1.4.1. 9.10.119.0. 2	N/A	N/A	A cPimNbrLoss trap signifies the loss of an adjacency with a neighbor. This trap should be generated when the neighbor timer expires, and the router has no other neighbors on the same interface with a lower IP address than itself.	Cisco PIM neighbor lost
entSensorThres holdNotificatio n	1.3.6.1.4.1. 9.9.91.2.0.1	N/A	N/A	The sensor value crossed the threshold listed in entSensorThresholdTable. This notification is generated once each time the sensor value crosses the threshold	sensor value crossed threshold in entSensorThreshold Table
rttMonNotificat ion	1.3.6.1.4.1. 9.9.42.2.0.5	N/A	N/A	A rttMonNotification indicates the occurrence of a threshold violation, and it indicates the previous violation has subsided for a subsequent operation.	RTT threshold violation or clearance
cpwVcUp	1.3.6.1.4.1. 9.10.106.2. 2	N/A	N/A	This notification is generated when the cpwVcOperStatus object for one or more contiguous entries in cpwVcTable are about to enter the up(1) state from some other state.	Pseudo wire tunnel up

Table 16-6 Cisco IOX V2/V3 Traps (continued)

Trap Name	Trap OID	Subtype Varbind OID	Subtype Varbind Value	Description	Short Description
cpwVcDown	1.3.6.1.4.1.9.10.106.2.1	N/A	N/A	This notification is generated when the cpwVcOperStatus object for one or more contiguous entries in cpwVcTable are about to enter the down(2) state from some other state.	Pseudo wire tunnel down
ciscoRFSwactNotif	1.3.6.1.4.1.9.9.176.2.0.1	1.3.6.1.4.1.9.9.176.1.1.8.0	1	A SWACT notification is sent by the newly active redundant unit whenever a switch of activity occurs. In the case where a SWACT event may be indistinguishable from a reset event, a network management station should use this notification to differentiate the activity. sysUpTime is the same sysUpTime defined in the RFC-1213 MIB.	Cisco RF Swap Status - Unsupported
ciscoRFSwactNotif	1.3.6.1.4.1.9.9.176.2.0.1	1.3.6.1.4.1.9.9.176.1.1.8.0	2	A SWACT notification is sent by the newly active redundant unit whenever a switch of activity occurs. In the case where a SWACT event may be indistinguishable from a reset event, a network management station should use this notification to differentiate the activity. sysUpTime is the same sysUpTime defined in the RFC-1213 MIB.	Cisco RF Swap Status - None
ciscoRFSwactNotif	1.3.6.1.4.1.9.9.176.2.0.1	1.3.6.1.4.1.9.9.176.1.1.8.0	3	A SWACT notification is sent by the newly active redundant unit whenever a switch of activity occurs. In the case where a SWACT event may be indistinguishable from a reset event, a network management station should use this notification to differentiate the activity. sysUpTime is the same sysUpTime defined in the RFC-1213 MIB.	Cisco RF Swap Status - Not Known
ciscoRFSwactNotif	1.3.6.1.4.1.9.9.176.2.0.1	1.3.6.1.4.1.9.9.176.1.1.8.0	4	A SWACT notification is sent by the newly active redundant unit whenever a switch of activity occurs. In the case where a SWACT event may be indistinguishable from a reset event, a network management station should use this notification to differentiate the activity. sysUpTime is the same sysUpTime defined in the RFC-1213 MIB.	Cisco RF Swap Status - UserInitiated

Table 16-6 Cisco IOX V2/V3 Traps (continued)

Trap Name	Trap OID	Subtype Varbind OID	Subtype Varbind Value	Description	Short Description
ciscoRFSwact Notif	1.3.6.1.4.1.9.9.176.2.0.1	1.3.6.1.4.1.9.9.176.1.1.8.0	5	A SWACT notification is sent by the newly active redundant unit whenever a switch of activity occurs. In the case where a SWACT event may be indistinguishable from a reset event, a network management station should use this notification to differentiate the activity. sysUpTime is the same sysUpTime defined in the RFC-1213 MIB.	Cisco RF Swap Status - UserForced
ciscoRFSwact Notif	1.3.6.1.4.1.9.9.176.2.0.1	1.3.6.1.4.1.9.9.176.1.1.8.0	6	A SWACT notification is sent by the newly active redundant unit whenever a switch of activity occurs. In the case where a SWACT event may be indistinguishable from a reset event, a network management station should use this notification to differentiate the activity. sysUpTime is the same sysUpTime defined in the RFC-1213 MIB.	Cisco RF Swap Status - ActiveUnitFailed
ciscoRFSwact Notif	1.3.6.1.4.1.9.9.176.2.0.1	1.3.6.1.4.1.9.9.176.1.1.8.0	7	A SWACT notification is sent by the newly active redundant unit whenever a switch of activity occurs. In the case where a SWACT event may be indistinguishable from a reset event, a network management station should use this notification to differentiate the activity. sysUpTime is the same sysUpTime defined in the RFC-1213 MIB.	Cisco RF Swap Status - ActiveUnitRemoved
cefcUnrecognizedFRU	1.3.6.1.4.1.9.9.117.2.0.5	N/A	N/A	The cefcUnrecognizedFRU notification indicates that a FRU was inserted whose product ID is not supported. The varbind for this notification indicates the entPhysicalIndex of the inserted FRU, the entPhysicalClass this FRU belongs to, the entPhysicalVendorType of this FRU, the entPhysicalName of the FRU, the entPhysicalModelName of the inserted FRU, and the cefcPhysicalStatus telling the reason code for sending this notification.	cefc FRU inserted with unsupported product ID

Table 16-6 Cisco IOX V2/V3 Traps (continued)

Trap Name	Trap OID	Subtype Varbind OID	Subtype Varbind Value	Description	Short Description
cefcPowerSupplyOutputChange	1.3.6.1.4.1.9.9.117.2.0.7	N/A	N/A	The notification indicates that the power supply's output capacity has changed.This notification is triggered whenever one instance of the power supply's cefcPSOutputModeInOperation has transitioned from 'false' to 'true'.	cefc Power supply output capacity changed
rttMonConnectionChangeNotification	1.3.6.1.4.1.9.9.42.2.0.1	N/A	N/A	This notification is only valid when the RttMonRttType is 'echo' or 'pathEcho'.A rttMonConnectionChangeNotification indicates that a connection to a target (not to a hop along the path to a target) has failed on establishment or been lost and when reestablished. Precisely, this has resulted in rttMonCtrlOperConnectionLostOccurred changing value.	RTT Connection Change
rttMonTimeoutNotification	1.3.6.1.4.1.9.9.42.2.0.2	N/A	N/A	A rttMonTimeoutNotification indicates the occurrence of a timeout for a RTT operation, and it indicates the clearing of such a condition by a subsequent RTT operation. Precisely, this has resulted in rttMonCtrlOperTimeoutOccurred changing value. When the RttMonRttType is 'path Echo', this notification will only be sent when the timeout occurs during an operation to the target and not to a hop along the path to the target. This also applies to the clearing of the timeout.	RTT Operation Timeout

Table 16-6 Cisco IOX V2/V3 Traps (continued)

Trap Name	Trap OID	Subtype Varbind OID	Subtype Varbind Value	Description	Short Description
rttMonThresholdNotification	1.3.6.1.4.1.9.9.42.2.0.3	N/A	N/A	A rttMonThresholdNotification indicates the occurrence of a threshold violation for a RTT operation, and it indicates the previous violation has subsided for a subsequent RTT operation. Precisely, this has resulted in rttMonCtrlOperOverThresholdOccurred changing value. When the RttMonRttType is 'path Echo', this notification will only be sent when the threshold violation occurs during an operation to the target and not to a hop along the path to the target. This also applies to the subsiding of a threshold condition.	RTT Operation Threshold Violation
rttMonVerifyErrorNotification	1.3.6.1.4.1.9.9.42.2.0.4	N/A	N/A	A rttMonVerifyErrorNotification indicates the occurrence of a data corruption in an RTT operation.	RTT Verify Error
rttMonNotification	1.3.6.1.4.1.9.9.42.2.0.5	N/A	N/A	A rttMonNotification indicates the occurrence of a threshold violation, and it indicates the previous violation has subsided for a subsequent operation.	RTT threshold violation or clearance
rttMonLpdDiscoveryNotification	1.3.6.1.4.1.9.9.42.2.0.6	N/A	N/A	A rttMonLpdDiscoveryNotification indicates that the LSP Path Discovery to the target PE has failed, and it also indicates the clearing of such condition. Precisely this has resulted in rttMonLpdGrpStatsLPDFailOccurred changing value. When the rttMonLpdGrpStatsLPDFailOccurred is 'false', the instance value for rttMonLpdGrpStatsLPDFailCause is not valid.	RTT Lpd Discovery
rttMonLpdGrpStatusNotification	1.3.6.1.4.1.9.9.42.2.0.7	N/A	N/A	A rttMonLpdGrpStatusNotification indicates that the LPD Group status rttMonLpdGrpStatsGroupStatus has changed indicating some connectivity change to the target PE. This has resulted in rttMonLpdGrpStatsGroupStatus changing value.	RTT Lpd Grp Status
cbgpBackwardTransition	1.3.6.1.4.1.9.9.187.0.2	1.3.6.1.4.1.9.9.187.0.2	= 1	The cbgpBackwardTransition Event is generated when the IPv6 BGP FSM moves from a higher numbered state to a lower numbered state.	IPv6 BGP down trap

Table 16-6 Cisco IOX V2/V3 Traps (continued)

Trap Name	Trap OID	Subtype Varbind OID	Subtype Varbind Value	Description	Short Description
cbgpFsmStateChange	1.3.6.1.4.1.9.9.187.0.1	1.3.6.1.4.1.9.9.187.0.1	!= (1or 6)	The IPv6 BGP cbgpFsmStateChange notification is generated for every BGP FSM state change.	ipv6 BGP FSM state changed trap
cbgpFsmStateChange	1.3.6.1.4.1.9.9.187.0.1	1.3.6.1.4.1.9.9.187.0.1	= 6	The IPv6 BGP cbgpFsmStateChange notification is generated for every BGP FSM state change.	IPv6 BGP established trap
rttMonConnectionChangeNotification	1.3.6.1.4.1.9.9.42.2.0.1	1.3.6.1.4.1.9.9.42.1.2.9.1.5	1	IPSLA echo ConnLoss Trap v2	Connection Loss detected by ipsla icmp echo trap
rttMonConnectionChangeNotification	1.3.6.1.4.1.9.9.42.2.0.1	1.3.6.1.4.1.9.9.42.1.2.9.1.5	2	IPSLA echo ConnLoss Trap v2	Connection re-establish detected by ipsla icmp echo trap
rttMonTimeoutNotification	1.3.6.1.4.1.9.9.42.2.0.2	1.3.6.1.4.1.9.9.42.1.2.9.1.6	1	IPSLA IP or LSP echo Timeout trap v2	Timeout detected by ipsla icmp echo trap
rttMonTimeoutNotification	1.3.6.1.4.1.9.9.42.2.0.2	1.3.6.1.4.1.9.9.42.1.2.9.1.6	2	IPSLA IP or LSP echo Timeout trap v2	Connection re-establish detected by ipsla icmp echo trap
rttMonThresholdNotification	1.3.6.1.4.1.9.9.42.2.0.3	1.3.6.1.4.1.9.9.42.1.2.9.1.7	1	IPSLA Threshold Notification trap v2	Threshold crossing under trap
rttMonThresholdNotification	1.3.6.1.4.1.9.9.42.2.0.3	1.3.6.1.4.1.9.9.42.1.2.9.1.7	2	IPSLA Threshold Notification trap v2	Threshold crossing over trap
rttMonVerifyErrorNotification	1.3.6.1.4.1.9.9.42.2.0.4	1.3.6.1.4.1.9.9.42.1.2.9.1.11	1	IPSLA Threshold Notification deprecated trap v2	Data corruption in rtt operation trap
rttMonVerifyErrorNotification	1.3.6.1.4.1.9.9.42.2.0.4	1.3.6.1.4.1.9.9.42.1.2.9.1.11	2	IPSLA Threshold Notification deprecated trap v2	Data corruption cleared in rtt operation trap
rttMonNotification	1.3.6.1.4.1.9.9.42.2.0.5	1.3.6.1.4.1.9.9.42.1.2.19.1.2, 1.3.6.1.4.1.9.9.42.1.2.2.1.33, 1.3.6.1.4.1.9.9.42.1.2.19.1.10	8, null, 1	RTT MON notification	Connection Loss detected by ipsla icmp echo trap

Table 16-6 Cisco IOX V2/V3 Traps (continued)

Trap Name	Trap OID	Subtype Varbind OID	Subtype Varbind Value	Description	Short Description
rttMonNotification	1.3.6.1.4.1.9.9.42.2.0.5	1.3.6.1.4.1.9.9.42.1.2.19.1.2, 1.3.6.1.4.1.9.9.42.1.2.2.1.33, 1.3.6.1.4.1.9.9.42.1.2.19.1.10	8, not null, 1	RTT MON notification	Connection Loss detected by ipsla LSP icmp echo trap
rttMonNotification	1.3.6.1.4.1.9.9.42.2.0.5	1.3.6.1.4.1.9.9.42.1.2.19.1.2, 1.3.6.1.4.1.9.9.42.1.2.2.1.33, 1.3.6.1.4.1.9.9.42.1.2.19.1.10	8, null, 2	RTT MON notification	Connection re-establish detected by ipsla icmp echo trap
rttMonNotification	1.3.6.1.4.1.9.9.42.2.0.5	1.3.6.1.4.1.9.9.42.1.2.19.1.2, 1.3.6.1.4.1.9.9.42.1.2.2.1.33, 1.3.6.1.4.1.9.9.42.1.2.19.1.10	8, not null, 2	RTT MON notification	Connection re-establish detected by ipsla LSP icmp echo trap
rttMonNotification	1.3.6.1.4.1.9.9.42.2.0.5	1.3.6.1.4.1.9.9.42.1.2.19.1.2, 1.3.6.1.4.1.9.9.42.1.2.2.1.33, 1.3.6.1.4.1.9.9.42.1.2.19.1.10	7, null, 1	RTT MON notification	Timeout detected by ipsla icmp echo trap
rttMonNotification	1.3.6.1.4.1.9.9.42.2.0.5	1.3.6.1.4.1.9.9.42.1.2.19.1.2, 1.3.6.1.4.1.9.9.42.1.2.2.1.33, 1.3.6.1.4.1.9.9.42.1.2.19.1.10	7, not null, 1	RTT MON notification	Timeout detected by ipsla LSP icmp echo trap

Table 16-6 Cisco IOX V2/V3 Traps (continued)

Trap Name	Trap OID	Subtype Varbind OID	Subtype Varbind Value	Description	Short Description
rttMonNotification	1.3.6.1.4.1.9.9.42.2.0.5	1.3.6.1.4.1.9.9.42.1.2.19.1.2, 1.3.6.1.4.1.9.9.42.1.2.2.1.33, 1.3.6.1.4.1.9.9.42.1.2.19.1.10	7, null, 2	RTT MON notification	Connection re-establish detected by ipsla icmp echo trap
rttMonNotification	1.3.6.1.4.1.9.9.42.2.0.5	1.3.6.1.4.1.9.9.42.1.2.19.1.2, 1.3.6.1.4.1.9.9.42.1.2.2.1.33, 1.3.6.1.4.1.9.9.42.1.2.19.1.10	7, not null, 2	RTT MON notification	Connection re-establish detected by ipsla LSP icmp echo trap
rttMonNotification	1.3.6.1.4.1.9.9.42.2.0.5	1.3.6.1.4.1.9.9.42.1.2.19.1.2, 1.3.6.1.4.1.9.9.42.1.2.19.1.10	1, 1	RTT MON notification	RTT threshold crossing over trap
rttMonNotification	1.3.6.1.4.1.9.9.42.2.0.5	1.3.6.1.4.1.9.9.42.1.2.19.1.2, 1.3.6.1.4.1.9.9.42.1.2.19.1.10	1, 2	RTT MON notification	RTT threshold crossing under trap
rttMonLpdDiscoveryNotification	1.3.6.1.4.1.9.9.42.2.0.6	1.3.6.1.4.1.9.9.42.1.3.7.1.13	1	IPSLA LPD Discovery trap v2	IPSLA LSP path discovery failure trap
rttMonLpdDiscoveryNotification	1.3.6.1.4.1.9.9.42.2.0.6	1.3.6.1.4.1.9.9.42.1.3.7.1.13	2	IPSLA LPD Discovery trap v2	IPSLA LSP path rediscovery trap
rttMonLpdGrpStatusNotification	1.3.6.1.4.1.9.9.42.2.0.7	1.3.6.1.4.1.9.9.42.1.3.7.1.16	3,4	IPSLA LDP Group Status trap v2	IPSLA LDP group status failure trap
rttMonLpdGrpStatusNotification	1.3.6.1.4.1.9.9.42.2.0.7	1.3.6.1.4.1.9.9.42.1.3.7.1.16	2	IPSLA LDP Group Status trap v2	IPSLA LDP group status restoration trap
cmplsFrrProtected	1.3.6.1.4.1.9.10.98.0.1	N/A	N/A	TE FRR trigger notification - protected trap v2	FRR Protected Trap

Table 16-6 Cisco IOX V2/V3 Traps (continued)

Trap Name	Trap OID	Subtype Varbind OID	Subtype Varbind Value	Description	Short Description
cmplsFrrUnProtected	1.3.6.1.4.1.9.10.98.0.2	N/A	N/A	TE FRR trigger notification - unprotected trap v2	FRR Unprotected Trap
cpwVcUp	1.3.6.1.4.1.9.10.106.2.2	N/A	N/A	This notification is generated when the cpwVcOperStatus object for one or more contiguous entries in cpwVcTable are about to enter the up(1) state from some other state.	Pseudo wire tunnel up
cpwVcDown	1.3.6.1.4.1.9.10.106.2.1	N/A	N/A	This notification is generated when the cpwVcOperStatus object for one or more contiguous entries in cpwVcTable are about to enter the down(2) state from some other state.	Pseudo wire tunnel down
DSX1 V1 Line Status Change	1.3.6.1.2.1.10.18.15.0.1	1.3.6.1.2.1.10.18.6.1.10.17	2	Indicates the line status of dsx1 interface	DSX1 Far end LOF
DSX1 V1 Line Status Change	1.3.6.1.2.1.10.18.15.0.1	1.3.6.1.2.1.10.18.6.1.10.17	4	Indicates the line status of dsx1 interface	DSX1 Near end sending LOF Indication
DSX1 V1 Line Status Change	1.3.6.1.2.1.10.18.15.0.1	1.3.6.1.2.1.10.18.6.1.10.17	8	Indicates the line status of dsx1 interface	DSX1 Far end sending AIS
DSX1 V1 Line Status Change	1.3.6.1.2.1.10.18.15.0.1	1.3.6.1.2.1.10.18.6.1.10.17	16	Indicates the line status of dsx1 interface	DSX1 Near end sending AIS
DSX1 V1 Line Status Change	1.3.6.1.2.1.10.18.15.0.1	1.3.6.1.2.1.10.18.6.1.10.17	32	Indicates the line status of dsx1 interface	DSX1 Near end LOF
DSX1 V1 Line Status Change	1.3.6.1.2.1.10.18.15.0.1	1.3.6.1.2.1.10.18.6.1.10.17	64	Indicates the line status of dsx1 interface	DSX1 Near end Loss of Signal
DSX1 V1 Line Status Change	1.3.6.1.2.1.10.18.15.0.1	1.3.6.1.2.1.10.18.6.1.10.17	128	Indicates the line status of dsx1 interface	DSX1 Near end is looped
DSX1 V1 Line Status Change	1.3.6.1.2.1.10.18.15.0.1	1.3.6.1.2.1.10.18.6.1.10.17	256	Indicates the line status of dsx1 interface	DSX1 E1 TS16 AIS
DSX1 V1 Line Status Change	1.3.6.1.2.1.10.18.15.0.1	1.3.6.1.2.1.10.18.6.1.10.17	512	Indicates the line status of dsx1 interface	DSX1 Far End Sending TS16 LOMF
DSX1 V1 Line Status Change	1.3.6.1.2.1.10.18.15.0.1	1.3.6.1.2.1.10.18.6.1.10.17	1024	Indicates the line status of dsx1 interface	DSX1 Near End Sending TS16 LOMF

Table 16-6 Cisco IOX V2/V3 Traps (continued)

Trap Name	Trap OID	Subtype Varbind OID	Subtype Varbind Value	Description	Short Description
DSX1 V1 Line Status Change	1.3.6.1.2.1.10.18.15.0.1	1.3.6.1.2.1.10.18.6.1.10.17	2048	Indicates the line status of dsx1 interface	DSX1 Near End detects a test code
DSX1 V1 Line Status Change	1.3.6.1.2.1.10.18.15.0.1	1.3.6.1.2.1.10.18.6.1.10.17	4096	Indicates the line status of dsx1 interface	DSX1 any line status not defined here
DSX1 V1 Line Status Change	1.3.6.1.2.1.10.18.15.0.1	1.3.6.1.2.1.10.18.6.1.10.17	8192	Indicates the line status of dsx1 interface	DSX1 Near End in Unavailable Signal State
DSX1 V1 Line Status Change	1.3.6.1.2.1.10.18.15.0.1	1.3.6.1.2.1.10.18.6.1.10.17	16384	Indicates the line status of dsx1 interface	DSX1 Carrier Equipment Out of Service
DSX1 V1 Line Status Change	1.3.6.1.2.1.10.18.15.0.1	1.3.6.1.2.1.10.18.6.1.10.17	32768	Indicates the line status of dsx1 interface	DSX1 DS2 Payload AIS
DSX1 V1 Line Status Change	1.3.6.1.2.1.10.18.15.0.1	1.3.6.1.2.1.10.18.6.1.10.17	65536	Indicates the line status of dsx1 interface	DSX1 DS2 Performance Threshold Exceeded
DSX1 V1 Line Status Change	1.3.6.1.2.1.10.18.15.0.1	1.3.6.1.2.1.10.18.6.1.10.17	!=(2 or 4 or 8 or 16 or 32 or 64 or 128 or 256 or 512 or 1024 or 2048 or 4096 or 8192 or 16384 or 32768 or 65536 or 1)	Indicates the line status of dsx1 interface	DSX1 combination of bitmaps due to multiple failures
DSX1 V1 Line Status Change	1.3.6.1.2.1.10.18.15.0.1	1.3.6.1.2.1.10.18.6.1.10.17	1	Indicates the line status of dsx1 interface	DSX1 No alarm present
DSX3 V1 Line Status Change	1.3.6.1.2.1.10.30.15.0.1	1.3.6.1.2.1.10.30.5.1.10.17	2	Indicates the line status of dsx3 interface	DSX3 Receiving Yellow/Remote Alarm Indication
DSX3 V1 Line Status Change	1.3.6.1.2.1.10.30.15.0.1	1.3.6.1.2.1.10.30.5.1.10.17	4	Indicates the line status of dsx3 interface	DSX3 Transmitting Yellow/Remote Alarm Indication
DSX3 V1 Line Status Change	1.3.6.1.2.1.10.30.15.0.1	1.3.6.1.2.1.10.30.5.1.10.17	8	Indicates the line status of dsx3 interface	DSX3 Receiving AIS failure state
DSX3 V1 Line Status Change	1.3.6.1.2.1.10.30.15.0.1	1.3.6.1.2.1.10.30.5.1.10.17	16	Indicates the line status of dsx3 interface	DSX3 Transmitting AIS

Table 16-6 Cisco IOX V2/V3 Traps (continued)

Trap Name	Trap OID	Subtype Varbind OID	Subtype Varbind Value	Description	Short Description
DSX3 V1 Line Status Change	1.3.6.1.2.1.10.30.15.0.1	1.3.6.1.2.1.10.30.5.1.10.17	32	Indicates the line status of dsx3 interface	DSX3 Receiving LOF failure state
DSX3 V1 Line Status Change	1.3.6.1.2.1.10.30.15.0.1	1.3.6.1.2.1.10.30.5.1.10.17	64	Indicates the line status of dsx3 interface	DSX3 Receiving LOS failure state
DSX3 V1 Line Status Change	1.3.6.1.2.1.10.30.15.0.1	1.3.6.1.2.1.10.30.5.1.10.17	128	Indicates the line status of dsx3 interface	DSX3 Looping the received signal
DSX3 V1 Line Status Change	1.3.6.1.2.1.10.30.15.0.1	1.3.6.1.2.1.10.30.5.1.10.17	256	Indicates the line status of dsx3 interface	DSX3 Receiving a Test Pattern
DSX3 V1 Line Status Change	1.3.6.1.2.1.10.30.15.0.1	1.3.6.1.2.1.10.30.5.1.10.17	512	Indicates the line status of dsx3 interface	DSX3 any line status not defined here
DSX3 V1 Line Status Change	1.3.6.1.2.1.10.30.15.0.1	1.3.6.1.2.1.10.30.5.1.10.17	1024	Indicates the line status of dsx3 interface	DSX3 Near End in Unavailable Signal State
DSX3 V1 Line Status Change	1.3.6.1.2.1.10.30.15.0.1	1.3.6.1.2.1.10.30.5.1.10.17	2048	Indicates the line status of dsx3 interface	DSX3 Carrier Equipment Out of Service
DSX3 V1 Line Status Change	1.3.6.1.2.1.10.30.15.0.1	1.3.6.1.2.1.10.30.5.1.10.17	!=(2 or 4 or 8 or 16 or 32 or 64 or 128 or 256 or 512 or 1024 or 2048 or 1)	Indicates the line status of dsx3 interface	DSX3 combination of bitmaps due to multiple failures
DSX3 V1 Line Status Change	1.3.6.1.2.1.10.30.15.0.1	1.3.6.1.2.1.10.30.5.1.10.17	1	Indicates the line status of dsx3 interface	DSX3 No alarm present
entConfigChange	1.3.6.1.2.1.47.2.0.1	N/A	N/A	An entConfigChange notification is generated when the value of entLastChangeTime changes. It can be utilized by an NMS to trigger logical/physical entity table maintenance polls.	Entity table configuration changed
Frame-Relay dlci status change trap v1	1.3.6.1.2.1.10.32.0.1	1.3.6.1.2.1.10.32.2.1.3	1	This trap indicates that the indicated Virtual Circuit has changed state. It has either been created or invalidated, or has toggled between the active and inactive states.	FR DLCI status invalid trap

Table 16-6 Cisco IOX V2/V3 Traps (continued)

Trap Name	Trap OID	Subtype Varbind OID	Subtype Varbind Value	Description	Short Description
Frame-Relay dlci status change trap v1	1.3.6.1.2.1.10.32.0.1	1.3.6.1.2.1.10.32.2.1.3	3	This trap indicates that the indicated Virtual Circuit has changed state. It has either been created or invalidated, or has toggled between the active and inactive states.	FR DLCI status inactive trap
Frame-Relay dlci status change trap v1	1.3.6.1.2.1.10.32.0.1	1.3.6.1.2.1.10.32.2.1.3	2	This trap indicates that the indicated Virtual Circuit has changed state. It has either been created or invalidated, or has toggled between the active and inactive states.	FR DLCI status active trap
ciscoSonetVTStatusChange	.1.3.6.1.4.1.9.9.126.0.4	1.3.6.1.2.1.10.39.3.1.1.1.2	!=1	VT Status is down	Cisco Sonet vt status changed to error
ciscoSonetVTStatusChange	.1.3.6.1.4.1.9.9.126.0.4	1.3.6.1.2.1.10.39.3.1.1.1.2	1	VT Status is down	Cisco Sonet vt status changed to clear
vrrpTrapAuthFailure	1.3.6.1.2.1.68.0.2	N/A	N/A	vrrp trap auth failure trap	Vrrp trap auth failure trap
vrrpTrapNewMaster	1.3.6.1.2.1.68.0.1	N/A	N/A	vrrp trap new master trap	Vrrp trap new master trap
ciscoBfdSessDown	1.3.6.1.4.1.9.10.137.0.2	N/A	N/A	Cisco-BFD-session-change-trap	Cisco bfd session down trap
ciscoBfdSessUp	1.3.6.1.4.1.9.10.137.0.1	N/A	N/A	Cisco-BFD-session-change-trap	Cisco bfd session up trap
atmIntfPvcFailuresTrap	1.3.6.1.2.1.37.1.14.2.1.0.1	N/A	N/A	A notification indicating that one or more PVPLs or PVCLs on this interface has failed since the last atmPvcFailuresTrap was sent. If this trap has not been sent for the last atmIntfPvcNotificationInterval, then it will be sent on the next increment of atmIntfPvcFailures	Atm interface PVC failures trap

Cisco MIB2 V1 Traps

Table 16-7 lists the Cisco MIB2 SNMP V1 traps supported in Prime Network. For associated event types, event subtypes, and Prime Network registry parameters, use the link under Short Description or see Table 16-23.

Table 16-7 Cisco MIB2 V1 Traps

Trap Name	Generic Type	Specific Type	Enterprise OID	Subtype Varbind OID	Subtype Varbind Value	Description	Short Description
dummy ticket on sun servers	N/A	N/A	1.3.6.1.4.1 .42	N/A	N/A	This type will handle all traps sent from SUN server (the OID is the SUN SNMP mib)	dummy ticket trap
MIB2 V1 link down	2	0	1.3.6.1.6.3 .1.1.5	N/A	N/A	A linkDown trap signifies that the sending protocol entity recognizes a failure in one of the communication links represented in the agent's configuration. The Trap-PDU of type linkDown contains as the first element of its variable-bindings, the name and value of the ifIndex instance for the affected interface.	SNMP Link down
MIB2 V1 link up	3	0	1.3.6.1.6.3 .1.1.5	N/A	N/A	A linkUp trap signifies that the sending protocol entity recognizes that one of the communication links represented in the agent's configuration has come up. The Trap-PDU of type linkUp contains as the first element of its variable-bindings, the name and value of the ifIndex instance for the affected interface.	SNMP Link up
DSX1 V1 Line Status Change	6	1	1.3.6.1.2.1 .10.18.15	1.3.6.1.2.1 .10.18.6.1. 10.17	2	Indicates the line status of dsx1 interface	DSX1 Far end LOF
DSX1 V1 Line Status Change	6	1	1.3.6.1.2.1 .10.18.15	1.3.6.1.2.1 .10.18.6.1. 10.17	4	Indicates the line status of dsx1 interface	DSX1 Near end sending LOF Indication
DSX1 V1 Line Status Change	6	1	1.3.6.1.2.1 .10.18.15	1.3.6.1.2.1 .10.18.6.1. 10.17	8	Indicates the line status of dsx1 interface	DSX1 Far end sending AIS
DSX1 V1 Line Status Change	6	1	1.3.6.1.2.1 .10.18.15	1.3.6.1.2.1 .10.18.6.1. 10.17	16	Indicates the line status of dsx1 interface	DSX1 Near end sending AIS
DSX1 V1 Line Status Change	6	1	1.3.6.1.2.1 .10.18.15	1.3.6.1.2.1 .10.18.6.1. 10.17	32	Indicates the line status of dsx1 interface	DSX1 Near end LOF

Table 16-7 Cisco MIB2 V1 Traps (continued)

Trap Name	Generic Type	Specific Type	Enterprise OID	Subtype Varbind OID	Subtype Varbind Value	Description	Short Description
DSX1 V1 Line Status Change	6	1	1.3.6.1.2.1 .10.18.15	1.3.6.1.2.1 .10.18.6.1. 10.17	64	Indicates the line status of dsx1 interface	DSX1 Near end Loss of Signal
DSX1 V1 Line Status Change	6	1	1.3.6.1.2.1 .10.18.15	1.3.6.1.2.1 .10.18.6.1. 10.17	128	Indicates the line status of dsx1 interface	DSX1 Near end is looped
DSX1 V1 Line Status Change	6	1	1.3.6.1.2.1 .10.18.15	1.3.6.1.2.1 .10.18.6.1. 10.17	256	Indicates the line status of dsx1 interface	DSX1 E1 TS16 AIS
DSX1 V1 Line Status Change	6	1	1.3.6.1.2.1 .10.18.15	1.3.6.1.2.1 .10.18.6.1. 10.17	512	Indicates the line status of dsx1 interface	DSX1 Far End Sending TS16 LOMF
DSX1 V1 Line Status Change	6	1	1.3.6.1.2.1 .10.18.15	1.3.6.1.2.1 .10.18.6.1. 10.17	1024	Indicates the line status of dsx1 interface	DSX1 Near End Sending TS16 LOMF
DSX1 V1 Line Status Change	6	1	1.3.6.1.2.1 .10.18.15	1.3.6.1.2.1 .10.18.6.1. 10.17	2048	Indicates the line status of dsx1 interface	DSX1 Near End detects a test code
DSX1 V1 Line Status Change	6	1	1.3.6.1.2.1 .10.18.15	1.3.6.1.2.1 .10.18.6.1. 10.17	4096	Indicates the line status of dsx1 interface	DSX1 any line status not defined here
DSX1 V1 Line Status Change	6	1	1.3.6.1.2.1 .10.18.15	1.3.6.1.2.1 .10.18.6.1. 10.17	8192	Indicates the line status of dsx1 interface	DSX1 Near End in Unavailable Signal State
DSX1 V1 Line Status Change	6	1	1.3.6.1.2.1 .10.18.15	1.3.6.1.2.1 .10.18.6.1. 10.17	16384	Indicates the line status of dsx1 interface	DSX1 Carrier Equipment Out of Service
DSX1 V1 Line Status Change	6	1	1.3.6.1.2.1 .10.18.15	1.3.6.1.2.1 .10.18.6.1. 10.17	32768	Indicates the line status of dsx1 interface	DSX1 DS2 Payload AIS
DSX1 V1 Line Status Change	6	1	1.3.6.1.2.1 .10.18.15	1.3.6.1.2.1 .10.18.6.1. 10.17	65536	Indicates the line status of dsx1 interface	DSX1 DS2 Performance Threshold Exceeded

Table 16-7 Cisco MIB2 V1 Traps (continued)

Trap Name	Generic Type	Specific Type	Enterprise OID	Subtype Varbind OID	Subtype Varbind Value	Description	Short Description
DSX1 V1 Line Status Change	6	1	1.3.6.1.2.1 .10.18.15	1.3.6.1.2.1 .10.18.6.1. 10.17	!=(2 or 4 or 8 or 16 or 32 or 64 or 128 or 256 or 512 or 1024 or 2048 or 4096 or 8192 or 16384 or 32768 or 65536 or 1)	Indicates the line status of dsx1 interface	DSX1 combination of bitmaps due to multiple failures
DSX1 V1 Line Status Change	6	1	1.3.6.1.2.1 .10.18.15	1.3.6.1.2.1 .10.18.6.1. 10.17	1	Indicates the line status of dsx1 interface	DSX1 No alarm present
DSX3 V1 Line Status Change	6	1	.1.3.6.1.2. 1.10.30.15	1.3.6.1.2.1 .10.30.5.1. 10.17	2	Indicates the line status of dsx1 interface	DSX3 Receiving Yellow/Remote Alarm Indication
DSX3 V1 Line Status Change	6	1	.1.3.6.1.2. 1.10.30.15	1.3.6.1.2.1 .10.30.5.1. 10.17	4	Indicates the line status of dsx1 interface	DSX3 Transmitting Yellow/Remote Alarm Indication
DSX3 V1 Line Status Change	6	1	.1.3.6.1.2. 1.10.30.15	1.3.6.1.2.1 .10.30.5.1. 10.17	8	Indicates the line status of dsx1 interface	DSX3 Receiving AIS failure state
DSX3 V1 Line Status Change	6	1	.1.3.6.1.2. 1.10.30.15	1.3.6.1.2.1 .10.30.5.1. 10.17	16	Indicates the line status of dsx1 interface	DSX3 Transmitting AIS
DSX3 V1 Line Status Change	6	1	.1.3.6.1.2. 1.10.30.15	1.3.6.1.2.1 .10.30.5.1. 10.17	32	Indicates the line status of dsx1 interface	DSX3 Receiving LOF failure state
DSX3 V1 Line Status Change	6	1	.1.3.6.1.2. 1.10.30.15	1.3.6.1.2.1 .10.30.5.1. 10.17	64	Indicates the line status of dsx1 interface	DSX3 Receiving LOS failure state

Table 16-7 Cisco MIB2 V1 Traps (continued)

Trap Name	Generic Type	Specific Type	Enterprise OID	Subtype Varbind OID	Subtype Varbind Value	Description	Short Description
DSX3 V1 Line Status Change	6	1	.1.3.6.1.2.1.10.30.15	1.3.6.1.2.1.10.30.5.1.10.17	128	Indicates the line status of dsx1 interface	DSX3 Looping the received signal
DSX3 V1 Line Status Change	6	1	.1.3.6.1.2.1.10.30.15	1.3.6.1.2.1.10.30.5.1.10.17	256	Indicates the line status of dsx1 interface	DSX3 Receiving a Test Pattern
DSX3 V1 Line Status Change	6	1	.1.3.6.1.2.1.10.30.15	1.3.6.1.2.1.10.30.5.1.10.17	512	Indicates the line status of dsx1 interface	DSX3 any line status not defined here
DSX3 V1 Line Status Change	6	1	.1.3.6.1.2.1.10.30.15	1.3.6.1.2.1.10.30.5.1.10.17	1024	Indicates the line status of dsx1 interface	DSX3 Near End in Unavailable Signal State
DSX3 V1 Line Status Change	6	1	.1.3.6.1.2.1.10.30.15	1.3.6.1.2.1.10.30.5.1.10.17	2048	Indicates the line status of dsx1 interface	DSX3 Carrier Equipment Out of Service
DSX3 V1 Line Status Change	6	1	.1.3.6.1.2.1.10.30.15	1.3.6.1.2.1.10.30.5.1.10.17	!=(2 or 4 or 8 or 16 or 32 or 64 or 128 or 256 or 512 or 1024 or 2048 or 1)	Indicates the line status of dsx1 interface	DSX3 combination of bitmaps due to multiple failures
DSX3 V1 Line Status Change	6	1	.1.3.6.1.2.1.10.30.15	1.3.6.1.2.1.10.30.5.1.10.17	1	Indicates the line status of dsx1 interface	DSX3 No alarm present
entConfigChange	6	1	1.3.6.1.2.1.47.2	N/A	N/A	An entConfigChange notification is generated when the value of entLastChangeTime changes. It can be utilized by an NMS to trigger logical/physical entity table maintenance polls.	Entity table configuration changed
Frame-Relay dlci status change trap v1	6	1	1.3.6.1.2.1.10.32	1.3.6.1.2.1.10.32.2.1.3	1	This trap indicates that the indicated Virtual Circuit has changed state. It has either been created or invalidated, or has toggled between the active and inactive states.	FR DLCI status invalid trap

Table 16-7 Cisco MIB2 V1 Traps (continued)

Trap Name	Generic Type	Specific Type	Enterprise OID	Subtype Varbind OID	Subtype Varbind Value	Description	Short Description
Frame-Relay dlci status change trap v1	6	1	1.3.6.1.2.1.10.32	1.3.6.1.2.1.10.32.2.1.3	3	This trap indicates that the indicated Virtual Circuit has changed state. It has either been created or invalidated, or has toggled between the active and inactive states.	FR DLCI status inactive trap
Frame-Relay dlci status change trap v1	6	1	1.3.6.1.2.1.10.32	1.3.6.1.2.1.10.32.2.1.3	2	This trap indicates that the indicated Virtual Circuit has changed state. It has either been created or invalidated, or has toggled between the active and inactive states.	FR DLCI status active trap
coldStart	0	0	1.3.6.1.6.3.1.1.5	N/A	N/A	A coldStart trap signifies that the SNMP entity, supporting a notification originator application, is reinitializing itself and that its configuration may have been altered.	Cold start trap
bgpBackwardTransition	6	2	1.3.6.1.2.1.15.7	N/A	N/A	The BGPBackwardTransition Event is generated when the BGP FSM moves from a higher numbered state to a lower numbered state.	BGP down trap
bgpEstablished	6	1	1.3.6.1.2.1.15.7	1.3.6.1.2.1.15.3.1.2	= 6	The BGP Established event is generated when the BGP FSM enters the ESTABLISHED state.	BGP established trap
authenticationFailure	6	5	1.3.6.1.6.3.1.1.5	N/A	N/A	An authenticationFailure trap signifies that the SNMP entity has received a protocol message that is not properly authenticated. While all implementations of SNMP entities may be capable of generating this trap, the snmpEnableAuthenTraps object indicates whether this trap will be generated.	SNMP authentication failure
ospfIfStateChange	6	16	1.3.6.1.2.1.14.16.2	1.3.6.1.2.1.14.7.1.12	= 1	An ospfIfStateChange trap signifies that there has been a change in the state of a non-virtualOSPF interface. This trap should be generated when the interface state regresses (e.g., goes from Dr to Down) or progresses to a terminal state (i.e., Point-to-Point, DR Other, Dr, or Backup)	OSPF interface state changed to Down

Table 16-7 Cisco MIB2 V1 Traps (continued)

Trap Name	Generic Type	Specific Type	Enterprise OID	Subtype Varbind OID	Subtype Varbind Value	Description	Short Description
ospfIfState Change	6	16	1.3.6.1.2.1 .14.16.2	1.3.6.1.2.1 .14.7.1.12	!= 1	An ospfIfStateChange trap signifies that there has been a change in the state of a non-virtualOSPF interface. This trap should be generated when the interface state regresses (e.g., goes from Dr to Down) or progresses to a terminal state (i.e., Point-to-Point, DR Other, Dr, or Backup)	OSPF interface state changed to Up
ospfVirtIfSt ateChange	6	1	1.3.6.1.2.1 .14.16.2	N/A	N/A	An ospfIfStateChange trap signifies that there has been a change in the state of an OSPF virtual interface. This trap should be generated when the interface state regresses (e.g., goes from Point-to-Point to Down) or progresses to a terminal state (i.e., Point-to-Point).	OSPF virtual interface state changed to Down
ospfNbrStat eChange	6	2	1.3.6.1.2.1 .14.16.2	1.3.6.1.2.1 .14.10.1.6	!= 8	An ospfNbrStateChange trap signifies that there has been a change in the state of a non-virtual OSPF neighbor. This trap should be generated when the neighbor state regresses (e.g., goes from Attempt or Full to 1-Way or Down) or progresses to a terminal state (e.g., 2-Way or Full).	OSPF neighbor state down
ospfNbrStat eChange	6	2	1.3.6.1.2.1 .14.16.2	1.3.6.1.2.1 .14.10.1.6	= 8	An ospfNbrStateChange trap signifies that there has been a change in the state of a non-virtual OSPF neighbor. This trap should be generated when the neighbor state regresses (e.g., goes from Attempt or Full to 1-Way or Down) or progresses to a terminal state (e.g., 2-Way or Full).	OSPF neighbor state up
ospfVirtNbr StateChang e	6	3	1.3.6.1.2.1 .14.16.2	1.3.6.1.2.1 .14.11.1.5	!= 8	An ospfIfStateChange trap signifies that there has been a change in the state of an OSPF virtual neighbor. This trap should be generated when the neighbor state regresses (e.g., goes from Attempt or Full to 1-Way or Down) or progresses to a terminal state (e.g., Full).	OSPF virtual neighbor state down

Table 16-7 Cisco MIB2 V1 Traps (continued)

Trap Name	Generic Type	Specific Type	Enterprise OID	Subtype Varbind OID	Subtype Varbind Value	Description	Short Description
ospfVirtNbrStateChange	6	3	1.3.6.1.2.1.14.16.2	1.3.6.1.2.1.14.11.1.5	= 8	An ospfIfStateChange trap signifies that there has been a change in the state of an OSPF virtual neighbor. This trap should be generated when the neighbor state regresses (e.g., goes from Attempt or Full to 1-Way or Down) or progresses to a terminal state (e.g., Full).	OSPF virtual neighbor state up
ospfIfConfigError	6	4	1.3.6.1.2.1.14.16.2	N/A	N/A	An ospfIfConfigError trap signifies that a packet has been received on a non-virtual interface from a router whose configuration parameters conflict with this router's configuration parameters.	OSPF interface configuration error
ospfVirtIfConfigError	6	5	1.3.6.1.2.1.14.16.2	N/A	N/A	An ospfConfigError trap signifies that a packet has been received on a virtual interface from a router whose configuration parameters conflict with this router's configuration parameters.	OSPF virtual interface configuration error
ospfIfAuthFailure	6	6	1.3.6.1.2.1.14.16.2	N/A	N/A	An ospfIfAuthFailure trap signifies that a packet has been received on a non-virtual interface from a router whose authentication key or authentication type conflicts with this router's authentication key or authentication type.	OSPF interface authentication failure
ospfVirtIfAuthFailure	6	7	1.3.6.1.2.1.14.16.2	N/A	N/A	An ospfVirtIfAuthFailure trap signifies that a packet has been received on a virtual interface from a router whose authentication key or authentication type conflicts with this router's authentication key or authentication type.	OSPF virtual interface authentication failuree
ospfIfRxBadPacket	6	8	1.3.6.1.2.1.14.16.2	N/A	N/A	An ospfIfRxBadPacket trap signifies that an OSPF packet has been received on a non-virtual interface that cannot be parsed.	OSPF bad packet received
ospfVirtIfRxBadPacket	6	9	1.3.6.1.2.1.14.16.2	N/A	N/A	An ospfRxBadPacket trap signifies that an OSPF packet has been received on a virtual interface that cannot be parsed.	OSPF bad packet received on virtual interface

Table 16-7 Cisco MIB2 V1 Traps (continued)

Trap Name	Generic Type	Specific Type	Enterprise OID	Subtype Varbind OID	Subtype Varbind Value	Description	Short Description
ospfTxRetransmit	6	10	1.3.6.1.2.1.14.16.2	N/A	N/A	An ospfTxRetransmit trap signifies than an OSPF packet has been retransmitted on a non-virtual interface.	OSPF packet retransmitted
ospfVirtIfTxRetransmit	6	11	1.3.6.1.2.1.14.16.2	N/A	N/A	An ospfTxRetransmit trap signifies than an OSPF packet has been retransmitted on a virtual interface.	OSPF packet retransmitted on virtual interface
ospfOriginateLsa	6	12	1.3.6.1.2.1.14.16.2	N/A	N/A	An ospfOriginateLsa trap signifies that a new LSA has been originated by this router. This trap should not be invoked for simple refreshes of LSAs (which happens every 30 minutes), but instead will only be invoked when an LSA is (re)originated due to a topology change.	OSPF new LSA originated
ospfMaxAgeLsa	6	13	1.3.6.1.2.1.14.16.2	N/A	N/A	An ospfMaxAgeLsa trap signifies that one of the LSA in the router's link-state database has aged to MaxAge.	OSPF LSA aged to MaxAge
mteEventSetFailure	6	5	1.3.6.1.2.1.88.2	N/A	N/A	Notification that an attempt to do a set in response to an event has failed.	mte event set failure
mteTriggerFalling	6	3	1.3.6.1.2.1.88.2	N/A	N/A	Notification that the falling threshold was met for triggers with mteTriggerType 'threshold'	Cisco mte trigger falling
mteTriggerFired	6	1	1.3.6.1.2.1.88.2	N/A	N/A	Notification that the trigger indicated by the object instances has fired, for triggers with mteTriggerType 'boolean' or 'existence'.	mte trigger fired
mteTriggerRising	6	2	1.3.6.1.2.1.88.2	N/A	N/A	Notification that the rising threshold was met for triggers with mteTriggerType 'threshold'	Cisco mte trigger rising
entConfigChange	6	1	1.3.6.1.2.1.47.2	N/A	N/A	An entConfigChange notification is generated when the value of entLastChangeTime changes. It can be utilized by an NMS to trigger logical/physical entity table maintenance polls.	Entity table configuration changed

Table 16-7 Cisco MIB2 V1 Traps (continued)

Trap Name	Generic Type	Specific Type	Enterprise OID	Subtype Varbind OID	Subtype Varbind Value	Description	Short Description
ipv6IfState Change	6	1	1.3.6.1.2.1 .55.2	1.3.6.1.2.1 .55.2.0.1	N/A	An ipv6IfStateChange notification signifies that there has been a change in the state of an ipv6 interface. This notification should be generated when the interface's operational status transitions to or from the up(1) state.	ipv6 interface state changed
mplsL3Vpn NumVrfRou teMaxThres hCleared	6	6	1.3.6.1.2.1 .10.166.11	N/A	N/A	This notification is generated only after the number of routes contained by the specified VRF exceeds or attempts to exceed the maximum allowed value as indicated by mplsVrfMaxRouteThreshold, and then falls below this value.	mpls l3 vpn numvrf routemax thresh cleared Trap
mplsL3Vpn VrfDown	6	2	1.3.6.1.2.1 .10.166.11	N/A	N/A	This notification is generated when: a. One interface is associated with this VRF, and the ifOperStatus of this interface changes from up(1) to down(2). b. Multiple interfaces are associated with this VRF, and the ifOperStatus of all except one of these interfaces is equal to up(1), and the ifOperStatus of that interface changes from up(1) to down(2). c. The last interface with ifOperStatus equal to up(1) is disassociated from a VRF	mpls l3 vpn vrf Down Trap
mplsL3Vpn VrfNumVrf RouteMaxT hreshExcee ded	6	4	1.3.6.1.2.1 .10.166.11	N/A	N/A	This notification is generated when the number of routes contained by the specified VRF exceeds or attempts to exceed the maximum allowed value as indicated by mplsL3VpnVrfMaxRouteThreshold.	mpls l3 vpn vrf numvrf routemax thresh exceeded Trap
mplsL3Vpn VrfRouteMi dThreshExc eeded	6	3	1.3.6.1.2.1 .10.166.11	N/A	N/A	This notification is generated when the number of routes contained by the specified VRF exceeds the value indicated by mplsL3VpnVrfMidRouteThreshold.	mpls l3 vpn vrf routemid thresh exceeded Trap

Table 16-7 Cisco MIB2 V1 Traps (continued)

Trap Name	Generic Type	Specific Type	Enterprise OID	Subtype Varbind OID	Subtype Varbind Value	Description	Short Description
mplsL3VpnVrfUp	6	1	1.3.6.1.2.1.10.166.11	N/A	N/A	This notification is generated when: a. No interface is associated with this VRF, and the first (and only first) interface associated with it has its ifOperStatus change to up(1). b. One interface is associated with this VRF, and the ifOperStatus of this interface changes to up(1). c. Multiple interfaces are associated with this VRF, and the ifOperStatus of all interfaces is down(2), and the first of those interfaces has its ifOperStatus change to up(1).	mpls l3 vpn vrf Up Trap
mplsLdpInitSessionThresholdExceeded	6	1	1.3.6.1.2.1.10.166.4	N/A	N/A	Generated when the value of the 'mplsLdpEntityInitSessionThreshold' object is not zero, and the number of Session Initialization messages exceeds the value of the 'mplsLdpEntityInitSessionThreshold' object	MPLS LDP init session threshold exceeded Trap
mplsLdpSessionDown	6	4	1.3.6.1.2.1.10.166.4	N/A	N/A	Sent when the value of 'mplsLdpSessionState' leaves the 'operational(5)' state	MPLS LDP session down Trap
mplsLdpSessionUp	6	3	1.3.6.1.2.1.10.166.4	N/A	N/A	Sent when the value of 'mplsLdpSessionState' enters the 'operational(5)' state	MPLS LDP session up Trap
mplsTunnelRerouted	6	3	1.3.6.1.2.1.10.166.3	N/A	N/A	Generated when a tunnel is rerouted. If the mplsTunnelARHopTable is used, then this tunnel instance's entry in the mplsTunnelARHopTable MAY contain the new path for this tunnel some time after this trap is issued by the agent	MPLS-TE tunnel rerouted trap
mplsTunnelReoptimized	6	4	1.3.6.1.2.1.10.166.3	N/A	N/A	Generated when a tunnel is reoptimized. If the mplsTunnelARHopTable is used, then this tunnel instance's entry in the mplsTunnelARHopTable MAY contain the new path for this tunnel some time after this trap is issued by the agent	MPLS-TE tunnel reoptimized trap

Table 16-7 Cisco MIB2 V1 Traps (continued)

Trap Name	Generic Type	Specific Type	Enterprise OID	Subtype Varbind OID	Subtype Varbind Value	Description	Short Description
mplsTunnel Down	6	2	1.3.6.1.2.1 .10.166.3	N/A	N/A	Generated when a mplsTunnelOperStatus object for one of the configured tunnels is about to enter the down state from some other state (but not from the notPresen state). This other state is indicated by the included value of mplsTunnelOperStatus	MPLS-TE tunnel down
mplsTunnel Up	6	1	1.3.6.1.2.1 .10.166.3	N/A	N/A	Generated when a mplsTunnelOperStatus object for one of the configured tunnels is about to leave the down state and transition into some other state (but not into the notPresent state). This other state is indicated by the included value of mplsTunnelOperStatus	MPLS-TE tunnel up

Cisco MIB2 V2/V3 Traps

Table 16-8 lists the Cisco MIB2 SNMP V2/V3 traps supported in Prime Network. For associated event types, event subtypes, and Prime Network registry parameters, use the link under Short Description or see Table 16-24.

Table 16-8 Cisco MIB2 V2/V3 Traps

Trap Name	Trap OID	Subtype Varbind OID	Subtype Varbind Value	Description	Short Description
bgpBackwardTransition	1.3.6.1.2. 1.15.7.2	N/A	N/A	The BGPBackwardTransition Event is generated when the BGP FSM moves from a higher numbered state to a lower numbered state.	BGP down trap
bgpEstablished	1.3.6.1.2. 1.15.7.1	1.3.6.1.2.1.1 5.3.1.2	= 6	The BGP Established event is generated when the BGP FSM enters the ESTABLISHED state.	BGP established trap
mteEventSetFailure	1.3.6.1.2. 1.88.2.0.5	N/A	N/A	Notification that an attempt to do a set in response to an event has failed.	mte event set failure
mteTriggerFalling	1.3.6.1.2. 1.88.2.0.3	N/A	N/A	Notification that the falling threshold was met for triggers with mteTriggerType 'threshold	Cisco mte trigger falling
mteTriggerFired	1.3.6.1.2. 1.88.2.0.1	N/A	N/A	Notification that the trigger indicated by the object instances has fired, for triggers with mteTriggerType 'boolean' or 'existence'.	mte trigger fired

Table 16-8 Cisco MIB2 V2/V3 Traps (continued)

Trap Name	Trap OID	Subtype Varbind OID	Subtype Varbind Value	Description	Short Description
mteTriggerRising	1.3.6.1.2.1.88.2.0.2	N/A	N/A	Notification that the rising threshold was met for triggers with mteTriggerType 'threshold	Cisco mte trigger rising
entConfigChange	1.3.6.1.2.1.47.2.0.1	N/A	N/A	An entConfigChange notification is generated when the value of entLastChangeTime changes. It can be utilized by an NMS to trigger logical/physical entity table maintenance polls.	Entity table configuration changed
coldStart	1.3.6.1.6.3.1.1.5.1	N/A	N/A	A coldStart trap signifies that the SNMP entity, supporting a notification originator application, is reinitializing itself and that its configuration may have been altered.	Cold start trap
warmStart	1.3.6.1.6.3.1.1.5.2	N/A	N/A	A warmStart trap signifies that the SNMP entity, supporting a notification originator application, is reinitializing itself such that its configurationis unaltered	Warm start trap
authenticationFailure	1.3.6.1.6.3.1.1.5.5	N/A	N/A	An authenticationFailure trap signifies that the SNMP entity has received a protocol message that is not properly authenticated. While all implementations of SNMP entities MAY be capable of generating this trap, the snmpEnableAuthenTraps object indicates whether this trap will be generated.	SNMP authentication failure
linkDown	1.3.6.1.6.3.1.1.5.3	N/A	N/A	A linkDown trap signifies that the SNMP entity, acting in an agent role, has detected that the ifOperStatus object for one of its communication links is about to enter the down state from some other state (but not from the notPresent state). This other state is indicated by the included value of ifOperStatus.	SNMP Link down
linkUp	1.3.6.1.6.3.1.1.5.4	N/A	N/A	A linkUp trap signifies that the SNMP entity, acting in an agent role, has detected that the ifOperStatus object for one of its communication links left the down state and transitioned into some other state (but not into the notPresent state). This other state is indicated by the included value of ifOperStatus.	SNMP Link up

Table 16-8 Cisco MIB2 V2/V3 Traps (continued)

Trap Name	Trap OID	Subtype Varbind OID	Subtype Varbind Value	Description	Short Description
ipv6IfStateChange	1.3.6.1.2.1.55.2.0.1	N/A	N/A	An ipv6IfStateChange notification signifies that there has been a change in the state of an ipv6 interface. This notification should be generated when the interface's operational status transitions to or from the up(1) state.	ipv6 interface state changed
ospfIfStateChange	1.3.6.1.2.1.14.16.2.16	1.3.6.1.2.1.14.7.1.12	= 1	An ospfIfStateChange trap signifies that there has been a change in the state of a non virtualOSPF interface. This trap should be generated when the interface state regresses (e.g., goes from Dr to Down) or progresses to a terminal state (i.e., Point-to-Point, DR Other, Dr, or Backup).	OSPF interface state changed to Down
ospfIfStateChange	1.3.6.1.2.1.14.16.2.16	1.3.6.1.2.1.14.7.1.12	!= 1	An ospfIfStateChange trap signifies that there has been a change in the state of a non virtualOSPF interface. This trap should be generated when the interface state regresses (e.g., goes from Dr to Down) or progresses to a terminal state (i.e., Point-to-Point, DR Other, Dr, or Backup).	OSPF interface state changed to Up
ospfVirtIfStateChange	1.3.6.1.2.1.14.16.2.1	N/A	N/A	An ospfIfStateChange trap signifies that there has been a change in the state of an OSPF virtual interface. This trap should be generated when the interface state regresses (e.g., goes from Point-to-Point to Down) or progresses to a terminal state (i.e., Point-to-Point).	OSPF virtual interface state changed to Down
ospfNbrStateChange	1.3.6.1.2.1.14.16.2.2	1.3.6.1.2.1.14.10.1.6	!= 8	An ospfNbrStateChange trap signifies that there has been a change in the state of a non virtual OSPF neighbor. This trap should be generated when the neighbor state regresses (e.g., goes from Attempt or Full to 1-Way or Down) or progresses to a terminal state (e.g., 2-Way or Full).	OSPF neighbor state down

Table 16-8 Cisco MIB2 V2/V3 Traps (continued)

Trap Name	Trap OID	Subtype Varbind OID	Subtype Varbind Value	Description	Short Description
ospfNbrStateChange	1.3.6.1.2.1.14.16.2.2	1.3.6.1.2.1.14.10.1.6	= 8	An ospfNbrStateChange trap signifies that there has been a change in the state of a non virtual OSPF neighbor. This trap should be generated when the neighbor state regresses (e.g., goes from Attempt or Full to 1-Way or Down) or progresses to a terminal state (e.g., 2-Way or Full).	OSPF neighbor state up
ospfVirtNbrStateChange	1.3.6.1.2.1.14.16.2.3	1.3.6.1.2.1.14.11.1.5	!= 8	An ospfIfStateChange trap signifies that there has been a change in the state of an OSPF virtual neighbor. This trap should be generated when the neighbor state regresses (e.g., goes from Attempt or Full to 1-Way or Down) or progresses to a terminal state (e.g., Full).	OSPF virtual neighbor state down
ospfVirtNbrStateChange	1.3.6.1.2.1.14.16.2.3	1.3.6.1.2.1.14.11.1.5	= 8	An ospfIfStateChange trap signifies that there has been a change in the state of an OSPF virtual neighbor. This trap should be generated when the neighbor state regresses (e.g., goes from Attempt or Full to 1-Way or Down) or progresses to a terminal state (e.g., Full).	OSPF virtual neighbor state up
ospfIfConfigError	1.3.6.1.2.1.14.16.2.4	N/A	N/A	An ospfIfConfigError trap signifies that a packet has been received on a non virtual interface from a router whose configuration parameters conflict with this router's configuration parameters.	OSPF interface configuration error
ospfVirtIfConfigError	1.3.6.1.2.1.14.16.2.5	N/A	N/A	An ospfConfigError trap signifies that a packet has been received on a virtual interface from a router whose configuration parameters conflict with this router's configuration parameters.	OSPF virtual interface configuration error
ospfIfAuthFailure	1.3.6.1.2.1.14.16.2.6	N/A	N/A	An ospfIfAuthFailure trap signifies that a packet has been received on a non virtual interface from a router whose authentication key or authentication type conflicts with this router's authentication key or authentication type.	OSPF interface authentication failure

Table 16-8 Cisco MIB2 V2/V3 Traps (continued)

Trap Name	Trap OID	Subtype Varbind OID	Subtype Varbind Value	Description	Short Description
ospfVirtIfAuthFailure	1.3.6.1.2.1.14.16.2.7	N/A	N/A	An ospfVirtIfAuthFailure trap signifies that a packet has been received on a virtual interface from a router whose authentication key or authentication type conflicts with this router's authentication key or authentication type.	OSPF virtual interface authentication failure
ospfIfRxBadPacket	1.3.6.1.2.1.14.16.2.8	N/A	N/A	An ospfIfRxBadPacket trap signifies that an OSPF packet has been received on a non virtual interface that cannot be parsed.	OSPF bad packet received
ospfVirtIfRxBadPacket	1.3.6.1.2.1.14.16.2.9	N/A	N/A	An ospfRxBadPacket trap signifies that an OSPF packet has been received on a virtual interface that cannot be parsed.	OSPF bad packet received on virtual interface
ospfTxRetransmit	1.3.6.1.2.1.14.16.2.10	N/A	N/A	An ospfTxRetransmit trap signifies than an OSPF packet has been retransmitted on a non virtual interface.	OSPF packet retransmitted
ospfVirtIfTxRetransmit	1.3.6.1.2.1.14.16.2.11	N/A	N/A	An ospfTxRetransmit trap signifies than an OSPF packet has been retransmitted on a virtual interface.	OSPF packet retransmitted on virtual interface
ospfOriginateLsa	1.3.6.1.2.1.14.16.2.12	N/A	N/A	An ospfOriginateLsa trap signifies that a new LSA has been originated by this router. This trap should not be invoked for simple refreshes of LSAs (which happens every 30 minutes), but instead will only be invoked when an LSA is (re)originated due to a topology change.	OSPF new LSA originated
ospfMaxAgeLsa	1.3.6.1.2.1.14.16.2.13	N/A	N/A	An ospfMaxAgeLsa trap signifies that one of the LSA in the link-state database of the router has aged to MaxAge.	OSPF LSA aged to MaxAge
mplsL3VpnNumVrfRouteMaxThreshCleared	1.3.6.1.2.1.10.166.11.0.6	N/A	N/A	This notification is generated only after the number of routes contained by the specified VRF exceeds or attempts to exceed the maximum allowed value as indicated by mplsVrfMaxRouteThreshold, and then falls below this value.	mpls l3 vpn numvrf routemax thresh cleared Trap

Table 16-8 Cisco MIB2 V2/V3 Traps (continued)

Trap Name	Trap OID	Subtype Varbind OID	Subtype Varbind Value	Description	Short Description
mplsL3VpnVrfDown	1.3.6.1.2.1.10.166.11.0.2	N/A	N/A	This notification is generated when: a. One interface is associated with this VRF, and the ifOperStatus of this interface changes from up(1) to down(2). b. Multiple interfaces are associated with this VRF, and the ifOperStatus of all except one of these interfaces is equal to up(1), and the ifOperStatus of that interface changes from up(1) to down(2).c. The last interface with ifOperStatus equal to up(1) is disassociated from a VRF	mpls l3 vpn vrf Down Trap
mplsL3VpnVrfNumVrfRouteMaxThreshExceeded	1.3.6.1.2.1.10.166.11.0.4	N/A	N/A	This notification is generated when the number of routes contained by the specified VRF exceeds or attempts to exceed the maximum allowed value as indicated by mplsL3VpnVrfMaxRouteThreshold.	mpls l3 vpn vrf numvrf routemax thresh exceeded Trap
mplsL3VpnVrfRouteMidThreshExceeded	1.3.6.1.2.1.10.166.11.0.3	N/A	N/A	This notification is generated when the number of routes contained by the specified VRF exceeds the value indicated by mplsL3VpnVrfMidRouteThreshold.	mpls l3 vpn vrf routemid thresh exceeded Trap
mplsL3VpnVrfUp	1.3.6.1.2.1.10.166.11.0.1	N/A	N/A	This notification is generated when: a. No interface is associated with this VRF, and the first (and only first) interface associated with it has its ifOperStatus change to up(1). b. One interface is associated with this VRF, and the ifOperStatus of this interface changes to up(1). c. Multiple interfaces are associated with this VRF, and the ifOperStatus of all interfaces is down(2), and the first of those interfaces has its ifOperStatus change to up(1).	mpls l3 vpn vrf Up Trap
mplsLdpInitSessionThresholdExceeded	1.3.6.1.2.1.10.166.4.0.1	N/A	N/A	generated when the value of the 'mplsLdpEntityInitSessionThreshold' object is not zero, and the number of Session Initialization messages exceeds the value of the 'mplsLdpEntityInitSessionThreshold' object	MPLS LDP init session threshold exceeded Trap

Table 16-8 Cisco MIB2 V2/V3 Traps (continued)

Trap Name	Trap OID	Subtype Varbind OID	Subtype Varbind Value	Description	Short Description
mplsLdpSessionDown	1.3.6.1.2.1.10.166.4.0.4	N/A	N/A	sent when the value of 'mplsLdpSessionState' leaves the 'operational(5)' state	MPLS LDP session down Trap
mplsLdpSessionUp	1.3.6.1.2.1.10.166.4.0.3	N/A	N/A	sent when the value of 'mplsLdpSessionState' enters the 'operational(5)' state	MPLS LDP session up Trap
mplsTunnelRerouted	1.3.6.1.2.1.10.166.3.0.3	N/A	N/A	generated when a tunnel is rerouted. If the mplsTunnelARHopTable is used, then this tunnel instance's entry in the mplsTunnelARHopTable MAY contain the new path for this tunnel some time after this trap is issued by the agent	MPLS TE tunnel rerouted trap
mplsTunnelReoptimized	1.3.6.1.2.1.10.166.3.0.4	N/A	N/A	generated when a tunnel is reoptimized. If the mplsTunnelARHopTable is used, then this tunnel instance's entry in the mplsTunnelARHopTable MAY contain the new path for this tunnel some time after this trap is issued by the agent	MPLS TE tunnel reoptimized trap
mplsTunnelDown	1.3.6.1.2.1.10.166.3.0.2	N/A	N/A	generated when a mplsTunnelOperStatus object for one of the configured tunnels is about to enter the down state from some other state (but not from the notPresen state). This other state is indicated by the included value of mplsTunnelOperStatus	MPLS TE tunnel down
mplsTunnelUp	1.3.6.1.2.1.10.166.3.0.1	N/A	N/A	generated when a mplsTunnelOperStatus object for one of the configured tunnels is about to leave the down state and transition into some other state (but not into the notPresent state). This other state is indicated by the included value of mplsTunnelOperStatus	MPLS TE tunnel up
DSX1 V1 Line Status Change	1.3.6.1.2.1.10.18.15.0.1	1.3.6.1.2.1.10.18.6.1.10.17	2	Indicates the line status of dsx1 interface	DSX1 Far end LOF
DSX1 V1 Line Status Change	1.3.6.1.2.1.10.18.15.0.1	1.3.6.1.2.1.10.18.6.1.10.17	4	Indicates the line status of dsx1 interface	DSX1 Near end sending LOF Indication

Table 16-8 Cisco MIB2 V2/V3 Traps (continued)

Trap Name	Trap OID	Subtype Varbind OID	Subtype Varbind Value	Description	Short Description
DSX1 V1 Line Status Change	1.3.6.1.2.1.10.18.15.0.1	1.3.6.1.2.1.10.18.6.1.10.17	8	Indicates the line status of dsx1 interface	DSX1 Far end sending AIS
DSX1 V1 Line Status Change	1.3.6.1.2.1.10.18.15.0.1	1.3.6.1.2.1.10.18.6.1.10.17	16	Indicates the line status of dsx1 interface	DSX1 Near end sending AIS
DSX1 V1 Line Status Change	1.3.6.1.2.1.10.18.15.0.1	1.3.6.1.2.1.10.18.6.1.10.17	32	Indicates the line status of dsx1 interface	DSX1 Near end LOF
DSX1 V1 Line Status Change	1.3.6.1.2.1.10.18.15.0.1	1.3.6.1.2.1.10.18.6.1.10.17	64	Indicates the line status of dsx1 interface	DSX1 Near end Loss of Signal
DSX1 V1 Line Status Change	1.3.6.1.2.1.10.18.15.0.1	1.3.6.1.2.1.10.18.6.1.10.17	128	Indicates the line status of dsx1 interface	DSX1 Near end is looped
DSX1 V1 Line Status Change	1.3.6.1.2.1.10.18.15.0.1	1.3.6.1.2.1.10.18.6.1.10.17	256	Indicates the line status of dsx1 interface	DSX1 E1 TS16 AIS
DSX1 V1 Line Status Change	1.3.6.1.2.1.10.18.15.0.1	1.3.6.1.2.1.10.18.6.1.10.17	512	Indicates the line status of dsx1 interface	DSX1 Far End Sending TS16 LOMF
DSX1 V1 Line Status Change	1.3.6.1.2.1.10.18.15.0.1	1.3.6.1.2.1.10.18.6.1.10.17	1024	Indicates the line status of dsx1 interface	DSX1 Near End Sending TS16 LOMF
DSX1 V1 Line Status Change	1.3.6.1.2.1.10.18.15.0.1	1.3.6.1.2.1.10.18.6.1.10.17	2048	Indicates the line status of dsx1 interface	DSX1 Near End detects a test code
DSX1 V1 Line Status Change	1.3.6.1.2.1.10.18.15.0.1	1.3.6.1.2.1.10.18.6.1.10.17	4096	Indicates the line status of dsx1 interface	DSX1 any line status not defined here
DSX1 V1 Line Status Change	1.3.6.1.2.1.10.18.15.0.1	1.3.6.1.2.1.10.18.6.1.10.17	8192	Indicates the line status of dsx1 interface	DSX1 Near End in Unavailable Signal State
DSX1 V1 Line Status Change	1.3.6.1.2.1.10.18.15.0.1	1.3.6.1.2.1.10.18.6.1.10.17	16384	Indicates the line status of dsx1 interface	DSX1 Carrier Equipment Out of Service
DSX1 V1 Line Status Change	1.3.6.1.2.1.10.18.15.0.1	1.3.6.1.2.1.10.18.6.1.10.17	32768	Indicates the line status of dsx1 interface	DSX1 DS2 Payload AIS
DSX1 V1 Line Status Change	1.3.6.1.2.1.10.18.15.0.1	1.3.6.1.2.1.10.18.6.1.10.17	65536	Indicates the line status of dsx1 interface	DSX1 DS2 Performance Threshold Exceeded

Table 16-8 Cisco MIB2 V2/V3 Traps (continued)

Trap Name	Trap OID	Subtype Varbind OID	Subtype Varbind Value	Description	Short Description
DSX1 V1 Line Status Change	1.3.6.1.2.1.10.18.15.0.1	1.3.6.1.2.1.10.18.6.1.10.17	!=(2 or 4 or 8 or 16 or 32 or 64 or 128 or 256 or 512 or 1024 or 2048 or 4096 or 8192 or 16384 or 32768 or 65536 or 1)	Indicates the line status of dsx1 interface	DSX1 combination of bitmaps due to multiple failures
DSX1 V1 Line Status Change	1.3.6.1.2.1.10.18.15.0.1	1.3.6.1.2.1.10.18.6.1.10.17	1	Indicates the line status of dsx1 interface	DSX1 No alarm present
DSX3 V1 Line Status Change	1.3.6.1.2.1.10.30.15.0.1	1.3.6.1.2.1.10.30.5.1.10.17	2	Indicates the line status of dsx3 interface	DSX3 Receiving Yellow/Remote Alarm Indication
DSX3 V1 Line Status Change	1.3.6.1.2.1.10.30.15.0.1	1.3.6.1.2.1.10.30.5.1.10.17	4	Indicates the line status of dsx3 interface	DSX3 Transmitting Yellow/Remote Alarm Indication
DSX3 V1 Line Status Change	1.3.6.1.2.1.10.30.15.0.1	1.3.6.1.2.1.10.30.5.1.10.17	8	Indicates the line status of dsx3 interface	DSX3 Receiving AIS failure state
DSX3 V1 Line Status Change	1.3.6.1.2.1.10.30.15.0.1	1.3.6.1.2.1.10.30.5.1.10.17	16	Indicates the line status of dsx3 interface	DSX3 Transmitting AIS
DSX3 V1 Line Status Change	1.3.6.1.2.1.10.30.15.0.1	1.3.6.1.2.1.10.30.5.1.10.17	32	Indicates the line status of dsx3 interface	DSX3 Receiving LOF failure state
DSX3 V1 Line Status Change	1.3.6.1.2.1.10.30.15.0.1	1.3.6.1.2.1.10.30.5.1.10.17	64	Indicates the line status of dsx3 interface	DSX3 Receiving LOS failure state
DSX3 V1 Line Status Change	1.3.6.1.2.1.10.30.15.0.1	1.3.6.1.2.1.10.30.5.1.10.17	128	Indicates the line status of dsx3 interface	DSX3 Looping the received signal
DSX3 V1 Line Status Change	1.3.6.1.2.1.10.30.15.0.1	1.3.6.1.2.1.10.30.5.1.10.17	256	Indicates the line status of dsx3 interface	DSX3 Receiving a Test Pattern
DSX3 V1 Line Status Change	1.3.6.1.2.1.10.30.15.0.1	1.3.6.1.2.1.10.30.5.1.10.17	512	Indicates the line status of dsx3 interface	DSX3 any line status not defined here
DSX3 V1 Line Status Change	1.3.6.1.2.1.10.30.15.0.1	1.3.6.1.2.1.10.30.5.1.10.17	1024	Indicates the line status of dsx3 interface	DSX3 Near End in Unavailable Signal State

Table 16-8 Cisco MIB2 V2/V3 Traps (continued)

Trap Name	Trap OID	Subtype Varbind OID	Subtype Varbind Value	Description	Short Description
DSX3 V1 Line Status Change	1.3.6.1.2.1.10.30.15.0.1	1.3.6.1.2.1.10.30.5.1.10.17	2048	Indicates the line status of dsx3 interface	DSX3 Carrier Equipment Out of Service
DSX3 V1 Line Status Change	1.3.6.1.2.1.10.30.15.0.1	1.3.6.1.2.1.10.30.5.1.10.17	!=(2 or 4 or 8 or 16 or 32 or 64 or 128 or 256 or 512 or 1024 or 2048 or 1)	Indicates the line status of dsx3 interface	DSX3 combination of bitmaps due to multiple failures
DSX3 V1 Line Status Change	1.3.6.1.2.1.10.30.15.0.1	1.3.6.1.2.1.10.30.5.1.10.17	1	Indicates the line status of dsx3 interface	DSX3 No alarm present
Frame-Relay dlci status change trap v1	1.3.6.1.2.1.10.32.0.1	1.3.6.1.2.1.10.32.2.1.3	1	This trap indicates that the indicated Virtual Circuit has changed state. It has either been created or invalidated, or has toggled between the active and inactive states.	FR DLCI status invalid trap
Frame-Relay dlci status change trap v1	1.3.6.1.2.1.10.32.0.1	1.3.6.1.2.1.10.32.2.1.3	3	This trap indicates that the indicated Virtual Circuit has changed state. It has either been created or invalidated, or has toggled between the active and inactive states.	FR DLCI status inactive trap
Frame-Relay dlci status change trap v1	1.3.6.1.2.1.10.32.0.1	1.3.6.1.2.1.10.32.2.1.3	2	This trap indicates that the indicated Virtual Circuit has changed state. It has either been created or invalidated, or has toggled between the active and inactive states.	FR DLCI status active trap

Cisco ACE V1 Traps

Table 16-9 lists the Cisco ACE SNMP V1 traps supported in Prime Network. For associated event types, event subtypes, and Prime Network registry parameters, use the link under Short Description or Table 16-25.

Table 16-9 CIsco ACE V1 Traps

Trap Name	Generic Type	Specific Type	Enterprise OID	Subtype Varbind OID	Subtype Varbind Value	Description	Short Description
cesRealServerStateUp	6	1	1.3.6.1.4.1.9.9.470	N/A	N/A	ces real server state up trap	ces real server state up trap
cesRealServerStateDown	6	2	1.3.6.1.4.1.9.9.470	N/A	N/A	ces real server state down trap	ces real server state down trap

Table 16-9 Cisco ACE V1 Traps (continued)

Trap Name	Generic Type	Specific Type	Enterprise OID	Subtype Varbind OID	Subtype Varbind Value	Description	Short Description
cesRealServerStateChange	6	3	1.3.6.1.4.1.9.9.470	N/A	N/A	ces real server state change trap	ces real server state change trap
cesRserverStateUp	6	4	1.3.6.1.4.1.9.9.470	N/A	N/A	ces R server state up trap	ces R server state up trap
cesRserverStateDown	6	5	1.3.6.1.4.1.9.9.470	N/A	N/A	ces R server state down trap	ces R server state down trap
cesRserverStateChange	6	6	1.3.6.1.4.1.9.9.470	N/A	N/A	ces R server state change trap	ces R server state change trap
ciscoSlbVServerVIPStateChange	6	6	1.3.6.1.4.1.9.9.161.2	N/A	N/A	Cisco sib V server VIP state change trap	cisco sib V server VIP state change trap
ciscoSlbVServerStateChange	6	5	1.3.6.1.4.1.9.9.161.2	N/A	N/A	Cisco sib V server state change trap	cisco sib V server state change trap
clmLicenseExpiryNotify	6	1	1.3.6.1.4.1.9.9.369.3	N/A	N/A	clm license expiry notify trap	clm license expiry notify trap
clmLicenseFileMissingNotify	6	3	1.3.6.1.4.1.9.9.369.3	N/A	N/A	clm license file missing notify trap	clm license file missing notify trap
clmLicenseExpiryWarningNotify	6	4	1.3.6.1.4.1.9.9.369.3	N/A	N/A	clm license expiry warning notify trap	clm license expiry warning notify trap

Cisco ACE V2/V3 Traps

Table 16-10 lists the Cisco ACE SNMP V2/V3 traps supported in Prime Network. For associated event types, event subtypes, and Prime Network registry parameters, use the link in the Short Description column or see Table 16-26.

Table 16-10 Cisco ACE V2/V3 Traps

Trap Name	Trap OID	Subtype Varbind OID	Subtype Varbind Value	Description	Short Description
linkDown	1.3.6.1.6.3.1.1.5.3	N/A	N/A	SNMP Link down	SNMP Link down
linkUp	1.3.6.1.6.3.1.1.5.4	N/A	N/A	SNMP Link up	SNMP Link up
cesRealServerStateUp	1.3.6.1.4.1.9.9.470.0.1	N/A	N/A	ces real server state up trap	ces real server state up trap
cesRealServerStateDown	1.3.6.1.4.1.9.9.470.0.2	N/A	N/A	ces real server state down trap	ces real server state down trap
cesRealServerStateChange	1.3.6.1.4.1.9.9.470.0.3	N/A	N/A	ces real server state change trap	ces real server state change trap
cesRserverStateUp	1.3.6.1.4.1.9.9.470.0.4	N/A	N/A	ces R server state up trap	ces R server state up trap
cesRserverStateDown	1.3.6.1.4.1.9.9.470.0.5	N/A	N/A	ces R server state down trap	ces R server state down trap
cesRserverStateChange	1.3.6.1.4.1.9.9.470.0.6	N/A	N/A	ces R server state change trap	ces R server state change trap
ciscoSlbVServerVIPStateChange	1.3.6.1.4.1.9.9.161.2.0.6	N/A	N/A	Cisco sib V server VIP state change trap	cisco sib V server VIP state change trap
ciscoSlbVServerStateChange	1.3.6.1.4.1.9.9.161.2.0.5	N/A	N/A	Cisco sib V server state change trap	cisco sib V server state change trap
clmLicenseExpiryNotify	1.3.6.1.4.1.9.9.369.3.0.1	N/A	N/A	clm license expiry notify trap	clm license expiry notify trap
clmLicenseFileMissingNotify	1.3.6.1.4.1.9.9.369.3.0.3	N/A	N/A	clm license file missing notify trap	clm license file missing notify trap
clmLicenseExpiryWarningNotify	1.3.6.1.4.1.9.9.369.3.0.4	N/A	N/A	clm license expiry warning notify trap	clm license expiry warning notify trap

Cisco Nexus V1 Traps

Table 16-11 lists the Cisco NEXUS SNMP V1 traps supported in Prime Network. For associated event types, event subtypes, and Prime Network registry parameters, use the link under Short Description or Table 16-27.

Table 16-11 Cisco Nexus V1 Traps

Trap Name	Generic Type	Specific Type	Enterprise OID	Subtype Varbind OID	Subtype Varbind Value	Description	Short Description
bgpEstablished	6	1	1.3.6.1.2.1.15.7	1.3.6.1.2.1 .15.3.1.2	= 6	The BGP Established event is generated when the BGP FSM enters the ESTABLISHED state.	BGP established trap
bgpBackwardTransition	6	2	1.3.6.1.2.1.15.7	N/A	N/A	The BGP Established event is generated when the BGP FSM enters the ESTABLISHED state.	BGP down trap
newRoot	6	1	1.3.6.1.2.1.17	N/A	N/A	The newRoot trap indicates that the sending agent has become the new root of the Spanning Tree; the trap is sent by a bridge soon after its election as the new root,e.g., upon expiration of the Topology Change Timer, immediately subsequent to its election. Implementation of this trap is optional.	new root trap
topologyChange	6	2	1.3.6.1.2.1.17	N/A	N/A	This Notification is sent by a bridge when any of its configured ports transitions from the Learning state to the Forwarding state, or from the Forwarding state to the Blocking state.	Spanning Tree Topology Changed
cefcModuleStatusChange	6	1	1.3.6.1.4.1.9.9.117.2	1.3.6.1.4.1 .9.9.117.1.2.1.1.2	!=2	This notification is generated when the value of cefcModuleOperStatus changes. It can be utilized by an NMS to update the status of the module it is managing.	cefc module oper status down

Table 16-11 Cisco Nexus V1 Traps (continued)

Trap Name	Generic Type	Specific Type	Enterprise OID	Subtype Varbind OID	Subtype Varbind Value	Description	Short Description
cefcModuleStatusChange	6	1	1.3.6.1.4.1.9.9.117.2	1.3.6.1.4.1.9.9.117.1.2.1.1.2	=2	This notification is generated when the value of cefcModuleOperStatus changes. It can be utilized by an NMS to update the status of the module it is managing.	cefc module oper status up
cefcPowerStatusChange	6	2	1.3.6.1.4.1.9.9.117.2	1.3.6.1.4.1.9.9.117.1.1.2.1.2	!=2	The cefcFRUPowerStatusChange notification indicates that the power status of a FRU has changed. The varbind for this notification indicates the entPhysicalIndex of the FRU, and the new operational-status of the FRU.	cefc power status down
cefcPowerStatusChange	6	2	1.3.6.1.4.1.9.9.117.2	1.3.6.1.4.1.9.9.117.1.1.2.1.2	=2	The cefcFRUPowerStatusChange notification indicates that the power status of a FRU has changed. The varbind for this notification indicates the entPhysicalIndex of the FRU, and the new operational-status of the FRU.	cefc power status up
cefcFRUInserted	6	3	1.3.6.1.4.1.9.9.117.2	N/A	N/A	The cecfFRUInserted notification indicates that a FRU was inserted. The varbind for this notification indicates the entPhysicalIndex of the inserted FRU, and the entPhysicalIndex of the FRU's container.	cefc FRU inserted

Table 16-11 Cisco Nexus V1 Traps (continued)

Trap Name	Generic Type	Specific Type	Enterprise OID	Subtype Varbind OID	Subtype Varbind Value	Description	Short Description
cefcFRURemoved	6	4	1.3.6.1.4.1.9.9.117.2	N/A	N/A	The cefcFRURemoved notification indicates that a FRU was removed. The varbind for this notification indicates the entPhysicalIndex of the removed FRU, and the entPhysicalIndex of the FRU's container.	cefc FRU removed
entSensorThresholdNotification	6	1	1.3.6.1.4.1.9.9.91.2.0	N/A	N/A	The sensor value crossed the threshold listed in entSensorThresholdTable. This notification is generated once each time the sensor value crosses the threshold	sensor value crossed threshold in entSensorThresholdTable
cpsIfVlanSecureMacAddrViolation	6	3	1.3.6.1.4.1.9.9.315	N/A	N/A	The address violation notification is generated when port security address violation is detected on a multi-vlan interface and the cpsIfViolationAction is set to 'dropNotify'.	cps IfVlan Secure MacAddr Violation Trap
cpsSecureMacAddrViolation	6	1	1.3.6.1.4.1.9.9.315	N/A	N/A	The address violation notification is generated when port security address violation is detected on a secure non-trunk, access interface (that carries a single vlan) and the cpsIfViolationAction is set to 'dropNotify'.	cps Secure MacAddr Violation Trap

Table 16-11 Cisco Nexus V1 Traps (continued)

Trap Name	Generic Type	Specific Type	Enterprise OID	Subtype Varbind OID	Subtype Varbind Value	Description	Short Description
stpxInconsistencyUpdate	6	1	1.3.6.1.4.1.9.9.82.2	1.3.6.1.4.1.9.9.82.1.3.1.1.3	=1	A stpxPortInconsistencyUpdate notification is sent by abridge when an instance of stpxInconsistentState is created or destroyed. That is, when an inconsistency is discovered in the VLAN's Spanning Tree for a particular port, or when such an inconsistency disappears. Note that the trap is not sent if the port transitions between different types of inconsistency. The stpxInconsistentState value indicates the type of inconsistency which now exists/no longer exists for the relevant VLAN on the relevant port.	Stpx Pvid Inconsistency Trap
stpxInconsistencyUpdate	6	1	1.3.6.1.4.1.9.9.82.2	1.3.6.1.4.1.9.9.82.1.3.1.1.3	=0	A stpxPortInconsistencyUpdate notification is sent by a bridge when an instance of stpxInconsistentState is created or destroyed. That is, when an inconsistency is discovered in the VLAN's Spanning Tree for a particular port, or when such an inconsistency disappears. Note that the trap is not sent if the port transitions between different types of inconsistency.The stpxInconsistentState value indicates the type of inconsistency which now exists/no longer exists for the relevant VLAN on the relevant port.	Stpx Type Inconsistency Trap

Table 16-11 Cisco Nexus V1 Traps (continued)

Trap Name	Generic Type	Specific Type	Enterprise OID	Subtype Varbind OID	Subtype Varbind Value	Description	Short Description
stpxLoopInconsistencyUpdate	6	3	1.3.6.1.4.1.9.9.82.2	1.3.6.1.4.1.9.9.82.1.8.2.1.3	= 1	A stpxLoopInconsistencyUpdate notification is sent by a bridge when an instance of stpxLoopInconsistencyState is created or destroyed. That is, when an loop-inconsistency is discovered in the VLAN's or instance's Spanning Tree for a particular port, or when such a loop-inconsistency disappears. For creation, the value of stpxLoopInconsistencyState in the notification is true(1); for deletion, the value is false(2).The object value of stpxSpanningTreeType indicates which Spanning Tree protocol is running when an instance of stpxLoopInconsistencyState is created or destroyed.	stpx loop inconsistency discovered

Table 16-11 Cisco Nexus V1 Traps (continued)

Trap Name	Generic Type	Specific Type	Enterprise OID	Subtype Varbind OID	Subtype Varbind Value	Description	Short Description
stpxLoopInconsistencyUpdate	6	3	1.3.6.1.4.1.9.9.82.2	1.3.6.1.4.1.9.9.82.1.8.2.1.3	= 2	A stpxLoopInconsistencyUpdate notification is sent by a bridge when an instance of stpxLoopInconsistencyState is created or destroyed. That is, when an loop-inconsistency is discovered in the VLAN's or instance's Spanning Tree for a particular port, or when such a loop-inconsistency disappears. For creation, the value of stpxLoopInconsistencyState in the notification is true(1); for deletion, the value is false(2).The object value of stpxSpanningTreeType indicateswhich Spanning Tree protocol is running when an instance of stpxLoopInconsistencyState is created or destroyed.	stpx loop inconsistency resolved

Table 16-11 Cisco Nexus V1 Traps (continued)

Trap Name	Generic Type	Specific Type	Enterprise OID	Subtype Varbind OID	Subtype Varbind Value	Description	Short Description
stpxRootInconsistencyUpdate	6	2	1.3.6.1.4.1.9.9.82.2	1.3.6.1.4.1.9.9.82.1.5.2.1.3	= 1	A stpxRootInconsistencyUpdate notification is sent by a bridge when an instance of stpxRootInconsistencyState is created or destroyed. That is, when an root-inconsistency is discovered in the VLAN's or instance's Spanning Tree for a particular port, or when such an root-inconsistency disappears. For creation, the value of stpxRootInconsistencyState in the notification is true(1); for deletion, the value is false(2).The object value of stpxSpanningTreeType indicates which Spanning Tree protocol is running when an instance of stpxRootInconsistencyState is created or destroyed.	stpx root inconsistency discovered

Table 16-11 Cisco Nexus V1 Traps (continued)

Trap Name	Generic Type	Specific Type	Enterprise OID	Subtype Varbind OID	Subtype Varbind Value	Description	Short Description
stpxRootInconsistencyUpdate	6	2	1.3.6.1.4.1.9.9.82.2	1.3.6.1.4.1.9.9.82.1.5.2.1.3	= 2	A stpxRootInconsistencyUpdate notification is sent by a bridge when an instance of stpxRootInconsistencyState is created or destroyed. That is, when an root-inconsistency is discovered in the VLAN's or instance's Spanning Tree for a particular port, or when such an root-inconsistency disappears. For creation, the value of stpxRootInconsistencyState in the notification is true(1); for deletion, the value is false(2).The object value of stpxSpanningTreeType indicates which Spanning Tree protocol is running when an instance of stpxRootInconsistencyState is created or destroyed.	stpx root inconsistency resolved
linkDown	2	0	1.3.6.1.6.3.1.1.5	N/A	N/A	A linkDown trap signifies that the sending protocol entity recognizes a failure in one of the communication links represented in the agent's configuration. The Trap-PDU of type linkDown contains as the first element of its variable-bindings, the name and value of the ifIndex instance for the affected interface.	SNMP Link down

Table 16-11 Cisco Nexus V1 Traps (continued)

Trap Name	Generic Type	Specific Type	Enterprise OID	Subtype Varbind OID	Subtype Varbind Value	Description	Short Description
linkUp	3	0	1.3.6.1.6.3.1.1.5	N/A	N/A	A linkUp trap signifies that the sending protocol entity recognizes that one of the communication links represented in the agent's configuration has come up. The Trap-PDU of type linkUp contains as the first element of its variable-bindings, the name and value of the ifIndex instance for the affected interface.	SNMP Link up
risingAlarm	6	1	1.3.6.1.2.1.16	N/A	N/A	RMON Rising Alarm	RMON Rising Alarm
fallingAlarm	6	2	1.3.6.1.2.1.16	N/A	N/A	RMON Falling Alarm	RMON Falling Alarm
coldStart	6	1	1.3.6.1.6.3.1.1.5	N/A	N/A	A coldStart trap signifies that the SNMP entity, supporting a notification originator application, is reinitializing itself and that its configuration may have been altered.	Cold start trap
ospfVirtIfStateChange	6	1	1.3.6.1.2.1.14.16.2	N/A	N/A	An ospfIfStateChange trap signifies that there has been a change in the state of an OSPF virtual interface. This trap should be generated when the interface state regresses (e.g., goes from Point-to-Point to Down) or progresses to a terminal state (i.e., Point-to-Point).	OSPF virtual interface state changed to Down

Table 16-11 Cisco Nexus V1 Traps (continued)

Trap Name	Generic Type	Specific Type	Enterprise OID	Subtype Varbind OID	Subtype Varbind Value	Description	Short Description
ospfNbrStateChange	6	2	1.3.6.1.2.1.14.16.2	1.3.6.1.2.1.14.10.1.6	!= 8	An ospfNbrStateChange trap signifies that there has been a change in the state of a non-virtual OSPF neighbor. This trap should be generated when the neighbor state regresses (e.g., goes from Attempt or Full to 1-Way or Down) or progresses to a terminal state (e.g., 2-Way or Full).	OSPF neighbor state down
ospfNbrStateChange	6	2	1.3.6.1.2.1.14.16.2	1.3.6.1.2.1.14.10.1.6	= 8	An ospfNbrStateChange trap signifies that there has been a change in the state of a non-virtual OSPF neighbor. This trap should be generated when the neighbor state regresses (e.g., goes from Attempt or Full to 1-Way or Down) or progresses to a terminal state (e.g., 2-Way or Full).	OSPF neighbor state up
ospfVirtNbrStateChange	6	3	1.3.6.1.2.1.14.16.2	1.3.6.1.2.1.14.11.1.5	!= 8	An ospfIfStateChange trap signifies that there has been a change in the state of an OSPF virtual neighbor. This trap should be generated when the neighbor state regresses (e.g., goes from Attempt or Full to 1-Way or Down) or progresses to a terminal state (e.g., Full).	OSPF virtual neighbor state down
ospfVirtNbrStateChange	6	3	1.3.6.1.2.1.14.16.2	1.3.6.1.2.1.14.11.1.5	= 8	An ospfIfStateChange trap signifies that there has been a change in the state of an OSPF virtual neighbor. This trap should be generated when the neighbor state regresses (e.g., goes from Attempt or Full to 1-Way or Down) or progresses to a terminal state (e.g., Full).	OSPF virtual neighbor state up

Table 16-11 Cisco Nexus V1 Traps (continued)

Trap Name	Generic Type	Specific Type	Enterprise OID	Subtype Varbind OID	Subtype Varbind Value	Description	Short Description
ospfIfConfigError	6	4	1.3.6.1.2.1.14.16.2	N/A	N/A	An ospfIfConfigError trap signifies that a packet has been received on a non-virtual interface from a router whose configuration parameters conflict with this router's configuration parameters.	OSPF interface configuration error
ospfVirtIfConfigError	6	5	1.3.6.1.2.1.14.16.2	N/A	N/A	An ospfConfigError trap signifies that a packet has been received on a virtual interface from a router whose configuration parameters conflict with this router's configuration parameters.	OSPF virtual interface configuration error
ospfIfAuthFailure	6	6	1.3.6.1.2.1.14.16.2	N/A	N/A	An ospfIfAuthFailure trap signifies that a packet has been received on a non-virtual interface from a router whose authentication key or authentication type conflicts with this router's authentication key or authentication type.	OSPF interface authentication failure
ospfVirtIfAuthFailure	6	7	1.3.6.1.2.1.14.16.2	N/A	N/A	An ospfVirtIfAuthFailure trap signifies that a packet has been received on a virtual interface from a router whose authentication key or authentication type conflicts with this router's authentication key or authentication type.	OSPF virtual interface authentication failure
ospfIfRxBadPacket	6	8	1.3.6.1.2.1.14.16.2	N/A	N/A	An ospfIfRxBadPacket trap signifies that an OSPF packet has been received on a non-virtual interface that cannot be parsed.	OSPF bad packet received

Table 16-11 Cisco Nexus V1 Traps (continued)

Trap Name	Generic Type	Specific Type	Enterprise OID	Subtype Varbind OID	Subtype Varbind Value	Description	Short Description
ospfVirtIfRxBadPacket	6	9	1.3.6.1.2.1.14.16.2	N/A	N/A	An ospfRxBadPacket trap signifies that an OSPF packet has been received on a virtual interface that cannot be parsed.	OSPF bad packet received on virtual interface
ospfTxRetransmit	6	10	1.3.6.1.2.1.14.16.2	N/A	N/A	An ospfTxRetransmit trap signifies than an OSPF packet has been retransmitted on a non-virtual interface.	OSPF packet retransmitted
ospfVirtIfTxRetransmit	6	11	1.3.6.1.2.1.14.16.2	N/A	N/A	An ospfTxRetransmit trap signifies than an OSPF packet has been retransmitted on a virtual interface.	OSPF packet retransmitted on virtual interface
ospfOriginateLsa	6	12	1.3.6.1.2.1.14.16.2	N/A	N/A	An ospfOriginateLsa trap signifies that a new LSA has been originated by this router. This trap should not be invoked for simple refreshes of LSAs (which happens every 30 minutes), but instead will only be invoked when an LSA is (re)originated due to a topology change.	OSPF new LSA originated
ospfMaxAgeLsa	6	13	1.3.6.1.2.1.14.16.2	N/A	N/A	An ospfMaxAgeLsa trap signifies that one of the LSA in the router's link-state database has aged to MaxAge.	OSPF LSA aged to MaxAge
ospfLsdbOverflow	6	14	1.3.6.1.2.1.14.16.2	N/A	N/A	OSPF lsdb overflow trap	OSPF lsdb overflow trap
ospfLsdbApproachingOverflow	6	15	1.3.6.1.2.1.14.16.2	N/A	N/A	OSPF lsdb approaching overflow trap	OSPF lsdb approaching overflow trap

Table 16-11 Cisco Nexus V1 Traps (continued)

Trap Name	Generic Type	Specific Type	Enterprise OID	Subtype Varbind OID	Subtype Varbind Value	Description	Short Description
ospfIfStateChange	6	16	1.3.6.1.2.1.14.16.2	1.3.6.1.2.1.14.7.1.12	= 1	An ospfIfStateChange trap signifies that there has been a change in the state of a non-virtualOSPF interface. This trap should be generated when the interface state regresses (e.g., goes from Dr to Down) or progresses to a terminal state (i.e., Point-to-Point, DR Other, Dr, or Backup)	OSPF interface state changed to Down
ospfIfStateChange	6	16	1.3.6.1.2.1.14.16.2	1.3.6.1.2.1.14.7.1.12	!= 1	An ospfIfStateChange trap signifies that there has been a change in the state of a non-virtualOSPF interface. This trap should be generated when the interface state regresses (e.g., goes from Dr to Down) or progresses to a terminal state (i.e., Point-to-Point, DR Other, Dr, or Backup)	OSPF interface state changed to Up
ospfNssaTranslatorStatusChange	6	17	1.3.6.1.2.1.14.16.2	N/A	N/A	OSPF NSSA translator status change trap	OSPF NSSA translator status change trap
ospfRestartStatusChange	6	18	1.3.6.1.2.1.14.16.2	N/A	N/A	OSPF restart status change trap	OSPF restart status change trap
ospfNbrRestartHelperStatusChange	6	19	1.3.6.1.2.1.14.16.2	N/A	N/A	OSPF neighbor restart helper status change trap	OSPF neighbor restart helper status change trap
ospfVirtNbrRestartHelperStatusChange	6	20	1.3.6.1.2.1.14.16.2	N/A	N/A	OSPF virtual neighbor restart helper status change trap	OSPF virtual neighbor restart helper status change trap

Cisco Nexus V2/V3 Traps

Table 16-12 lists the Cisco Nexus SNMP V2/V3 traps supported in Prime Network. For associated event types, event subtypes, and Prime Network registry parameters, use the link in the Short Description column or see Table 16-28.

Table 16-12 Cisco Nexus V2/V3 Traps

Trap Name	Trap OID	Subtype Varbind OID	Subtype Varbind Value	Description	Short Description
bgpEstablished	1.3.6.1.2.1.15.7.1	1.3.6.1.2.1.15.3.1.2	N/A	The BGP Established event is generated when the BGP FSM enters the ESTABLISHED state.	BGP established trap
bgpBackwardTransition	1.3.6.1.2.1.15.7.2	N/A	N/A	The BGP Established event is generated when the BGP FSM enters the ESTABLISHED state.	BGP down trap
newRoot	1.3.6.1.2.1.17.1	N/A	N/A	The newRoot trap indicates that the sending agent has become the new root of the Spanning Tree; the trap is sent by a bridge soon after its election as the new root, e.g., upon expiration of the Topology Change Timer, immediately subsequent to its election. Implementation of this trap is optional.	new root trap
topologyChange	1.3.6.1.2.1.17.2	N/A	N/A	This Notification is sent by a bridge when any of its configured ports transitions from the Learning state to the Forwarding state, or from the Forwarding state to the Blocking state.	Spanning Tree Topology Changed
cefcModuleStatusChange	1.3.6.1.4.1.9.9.117.2.1	1.3.6.1.4.1.9.9.117.1.2.1.1.2	N/A	This notification is generated when the value of cefcModuleOperStatus changes. It can be utilized by an NMS to update the status of the module it is managing.	cefc module oper status down
cefcModuleStatusChange	1.3.6.1.4.1.9.9.117.2.1	1.3.6.1.4.1.9.9.117.1.2.1.1.2	N/A	This notification is generated when the value of cefcModuleOperStatus changes. It can be utilized by an NMS to update the status of the module it is managing.	cefc module oper status up
cefcPowerStatusChange	1.3.6.1.4.1.9.9.117.2.2	1.3.6.1.4.1.9.9.117.1.1.2.1.2	N/A	The cefcFRUPowerStatusChange notification indicates that the power status of a FRU has changed. The varbind for this notification indicates the entPhysicalIndex of the FRU, and the new operational-status of the FRU.	cefc power status down

Table 16-12 Cisco Nexus V2/V3 Traps (continued)

Trap Name	Trap OID	Subtype Varbind OID	Subtype Varbind Value	Description	Short Description
cefcPowerStatusChange	1.3.6.1.4.1.9.9.117.2.2	1.3.6.1.4.1.9.9.117.1.1.2.1.2	N/A	The cefcFRUPowerStatusChange notification indicates that the power status of a FRU has changed. The varbind for this notification indicates the entPhysicalIndex of the FRU, and the new operational-status of the FRU.	cefc power status up
cefcFRUInserted	1.3.6.1.4.1.9.9.117.2.3	N/A	N/A	The cecfFRUInserted notification indicates that a FRU was inserted. The varbind for this notification indicates the entPhysicalIndex of the inserted FRU, and the entPhysicalIndex of the FRU's container.	cefc FRU inserted
cefcFRURemoved	1.3.6.1.4.1.9.9.117.2.4	N/A	N/A	The cefcFRURemoved notification indicates that a FRU was removed. The varbind for this notification indicates the entPhysicalIndex of the removed FRU, and the entPhysicalIndex of the FRU's container.	cefc FRU removed
entSensorThresholdNotification	1.3.6.1.4.1.9.9.91.2.0.1	N/A	N/A	The sensor value crossed the threshold listed in entSensorThresholdTable. This notification is generated once each time the sensor value crosses the threshold.	sensor value crossed threshold in entSensorThresholdTable
cpsIfVlanSecureMacAddrViolation	1.3.6.1.4.1.9.9.315.3	N/A	N/A	The address violation notification is generated when port security address violation is detected on a multi-vlan interface and the cpsIfViolationAction is set to 'dropNotify'.	cps IfVlan Secure MacAddr Violation Trap
cpsSecureMacAddrViolation	1.3.6.1.4.1.9.9.315.1	N/A	N/A	The address violation notification is generated when port security address violation is detected on a secure non-trunk, access interface (that carries a single vlan) and the cpsIfViolationAction is set to 'dropNotify'.	cps Secure MacAddr Violation Trap
stpxInconsistencyUpdate	1.3.6.1.4.1.9.9.82.2.1	1.3.6.1.4.1.9.9.82.1.3.1.1.3	N/A	A stpxPortInconsistencyUpdate notification is sent by a bridge when an instance of stpxInconsistentState is created or destroyed. That is, when an inconsistency is discovered in the VLAN's Spanning Tree for a particular port, or when such an inconsistency disappears. Note that the trap is not sent if the port transitions between different types of inconsistency. The stpxInconsistentState value indicates the type of inconsistency which now exists/no longer exists for the relevant VLAN on the relevant port.	Stpx Pvid Inconsistency Trap

Table 16-12 Cisco Nexus V2/V3 Traps (continued)

Trap Name	Trap OID	Subtype Varbind OID	Subtype Varbind Value	Description	Short Description
stpxInconsistencyUpdate	1.3.6.1.4.1.9.9.82.2.2.1	1.3.6.1.4.1.9.9.82.1.3.1.1.3	N/A	A stpxPortInconsistencyUpdate notification is sent by a bridge when an instance of stpxInconsistentState is created or destroyed. That is, when an inconsistency is discovered in the VLAN's Spanning Tree for a particular port, or when such an inconsistency disappears. Note that the trap is not sent if the port transitions between different types of inconsistency. The stpxInconsistentState value indicates the type of inconsistency which now exists/no longer exists for the relevant VLAN on the relevant port.	Stpx Type Inconsistency Trap
stpxLoopInconsistencyUpdate	1.3.6.1.4.1.9.9.82.2.2.3	1.3.6.1.4.1.9.9.82.1.8.2.1.3	N/A	A stpxLoopInconsistencyUpdate notification is sent by a bridge when an instance of stpxLoopInconsistencyStateis created or destroyed. That is, when an loop-inconsistency is discovered in the VLAN's or instance's Spanning Tree for a particular port, or when such a loop-inconsistency disappears. For creation, the value of stpxLoopInconsistencyState in the notification is true(1); for deletion, the value is false(2). The object value of stpxSpanningTreeType indicates which Spanning Tree protocol is running when an instance of stpxLoopInconsistencyState is created or destroyed.	stpx loop inconsistency discovered
stpxLoopInconsistencyUpdate	1.3.6.1.4.1.9.9.82.2.2.3	1.3.6.1.4.1.9.9.82.1.8.2.1.3	N/A	A stpxLoopInconsistencyUpdate notification is sent by a bridge when an instance of stpxLoopInconsistencyState is created or destroyed. That is, when an loop-inconsistency is discovered in the VLAN's or instance's Spanning Tree for a particular port, or when such a loop-inconsistency disappears. For creation, the value of stpxLoopInconsistencyState in the notification is true(1); for deletion, the value is false(2). The object value of stpxSpanningTreeType indicates which Spanning Tree protocol is running when an instance of stpxLoopInconsistencyState is created or destroyed.	stpx loop inconsistency resolved

Table 16-12 Cisco Nexus V2/V3 Traps (continued)

Trap Name	Trap OID	Subtype Varbind OID	Subtype Varbind Value	Description	Short Description
stpxRootInconsistencyUpdate	1.3.6.1.4.1.9.9.82.2.2	1.3.6.1.4.1.9.9.82.1.5.2.1.3	N/A	A stpxRootInconsistencyUpdate notification is sent by a bridge when an instance of stpxRootInconsistencyState is created or destroyed. That is, when an root-inconsistency is discovered in the VLAN's or instance's Spanning Tree for a particular port, or when such an root-inconsistency disappears. For creation, the value of stpxRootInconsistencyState in the notification istrue(1); for deletion, the value is false(2).The object value of stpxSpanningTreeType indicates which Spanning Tree protocol is running when an instance of stpxRootInconsistencyState is created or destroyed.	stpx root inconsistency discovered
stpxRootInconsistencyUpdate	1.3.6.1.4.1.9.9.82.2.2	1.3.6.1.4.1.9.9.82.1.5.2.1.3	N/A	A stpxRootInconsistencyUpdate notification is sent by a bridge when an instance of stpxRootInconsistencyState is created or destroyed. That is, when an root-inconsistency is discovered in the VLAN's or instance's Spanning Tree for a particular port, or when such an root-inconsistency disappears. For creation, the value of stpxRootInconsistencyState in the notification is true(1); for deletion, the value is false(2).The object value of stpxSpanningTreeType indicates which Spanning Tree protocol is running when an instance of stpxRootInconsistencyState is created or destroyed.	stpx root inconsistency resolved
linkDown	1.3.6.1.6.3.1.1.5.3	N/A	N/A	A linkDown trap signifies that the sending protocol entity recognizes a failure in one of the communication links represented in the agent's configuration. The Trap-PDU of type linkDown contains as the first element of its variable-bindings, the name and value of the ifIndex instance for the affected interface.	SNMP Link down
linkUp	1.3.6.1.6.3.1.1.5.4	N/A	N/A	A linkUp trap signifies that the sending protocol entity recognizes that one of the communication links represented in the agent's configuration has come up. The Trap-PDU of type linkUp contains as the first element of its variable-bindings, the name and value of the ifIndex instance for the affected interface.	SNMP Link up

Table 16-12 Cisco Nexus V2/V3 Traps (continued)

Trap Name	Trap OID	Subtype Varbind OID	Subtype Varbind Value	Description	Short Description
risingAlarm	1.3.6.1.2.1.16.0.1	N/A	N/A	RMON Rising Alarm	RMON Rising Alarm
fallingAlarm	1.3.6.1.2.1.16.0.2	N/A	N/A	RMON Falling Alarm	RMON Falling Alarm
coldStart	1.3.6.1.6.3.1.1.5.1	N/A	N/A	A coldStart trap signifies that the SNMP entity, supporting a notification originator application, is reinitializing itself and that its configuration may have been altered.	Cold start trap
ospfVirtIfStateChange	1.3.6.1.2.1.14.16.2.1	N/A	N/A	An ospfIfStateChange trap signifies that there has been a change in the state of an OSPF virtual interface. This trap should be generated when the interface state regresses (e.g., goes from Point-to-Point to Down) or progresses to a terminal state (i.e., Point-to-Point).	OSPF virtual interface state changed to Down
ospfNbrStateChange	1.3.6.1.2.1.14.16.2.2	1.3.6.1.2.1.14.10.1.6	N/A	N/A	OSPF neighbor state down
ospfNbrStateChange	1.3.6.1.2.1.14.16.2.2	1.3.6.1.2.1.14.10.1.6	N/A	An ospfNbrStateChange trap signifies that there has been a change in the state of a non-virtual OSPF neighbor. This trap should be generated when the neighbor state regresses (e.g., goes from Attempt or Full to 1-Way or Down) or progresses to a terminal state (e.g., 2-Way or Full).	OSPF neighbor state up
ospfVirtNbrStateChange	1.3.6.1.2.1.14.16.2.3	1.3.6.1.2.1.14.11.1.5	N/A	An ospfIfStateChange trap signifies that there has been a change in the state of an OSPF virtual neighbor. This trap should be generated when the neighbor state regresses (e.g., goes from Attempt or Full to 1-Way or Down) or progresses to a terminal state (e.g., Full).	OSPF virtual neighbor state down
ospfVirtNbrStateChange	1.3.6.1.2.1.14.16.2.3	1.3.6.1.2.1.14.11.1.5	N/A	An ospfIfStateChange trap signifies that there has been a change in the state of an OSPF virtual neighbor. This trap should be generated when the neighbor state regresses (e.g., goes from Attempt or Full to 1-Way or Down) or progresses to a terminal state (e.g., Full).	OSPF virtual neighbor state up
ospfIfConfigError	1.3.6.1.2.1.14.16.2.4	N/A	N/A	An ospfIfConfigError trap signifies that a packet has been received on a non-virtual interface from a router whose configuration parameters conflict with this router's configuration parameters.	OSPF interface configuration error

Table 16-12 Cisco Nexus V2/V3 Traps (continued)

Trap Name	Trap OID	Subtype Varbind OID	Subtype Varbind Value	Description	Short Description
ospfVirtIfConfigError	1.3.6.1.2.1.14.16.2.5	N/A	N/A	An ospfConfigError trap signifies that a packet has been received on a virtual interface from a router whose configuration parameters conflict with this router's configuration parameters.	OSPF virtual interface configuration error
ospfIfAuthFailure	1.3.6.1.2.1.14.16.2.6	N/A	N/A	An ospfIfAuthFailure trap signifies that a packet has been received on a non-virtual interface from a router whose authentication key or authentication type conflicts with this router's authentication key or authentication type.	OSPF interface authentication failure
ospfVirtIfAuthFailure	1.3.6.1.2.1.14.16.2.7	N/A	N/A	An ospfVirtIfAuthFailure trap signifies that a packet has been received on a virtual interface from a router whose authentication key or authentication type conflicts with this router's authentication key or authentication type.	OSPF virtual interface authentication failure
ospfIfRxBadPacket	1.3.6.1.2.1.14.16.2.8	N/A	N/A	An ospfIfRxBadPacket trap signifies that an OSPF packet has been received on a non-virtual interface that cannot be parsed.	OSPF bad packet received
ospfVirtIfRxBadPacket	1.3.6.1.2.1.14.16.2.9	N/A	N/A	An ospfRxBadPacket trap signifies that an OSPF packet has been received on a virtual interface that cannot be parsed.	OSPF bad packet received on virtual interface
ospfTxRetransmit	1.3.6.1.2.1.14.16.2.10	N/A	N/A	An ospfTxRetransmit trap signifies than an OSPF packet has been retransmitted on a non-virtual interface.	OSPF packet retransmitted
ospfVirtIfTxRetransmit	1.3.6.1.2.1.14.16.2.11	N/A	N/A	An ospfTxRetransmit trap signifies than an OSPF packet has been retransmitted on a virtual interface.	OSPF packet retransmitted on virtual interface
ospfOriginateLsa	1.3.6.1.2.1.14.16.2.12	N/A	N/A	An ospfOriginateLsa trap signifies that a new LSA has been originated by this router. This trap should not be invoked for simple refreshes of LSAs (which happens every 30 minutes), but instead will only be invoked when an LSA is (re)originated due to a topology change.	OSPF new LSA originated
ospfMaxAgeLsa	1.3.6.1.2.1.14.16.2.13	N/A	N/A	An ospfMaxAgeLsa trap signifies that one of the LSA in the router's link-state database has aged to MaxAge.	OSPF LSA aged to MaxAge
ospfLsdbOverflow	1.3.6.1.2.1.14.16.2.14	N/A	N/A	OSPF lsdb overflow trap	OSPF lsdb overflow trap
ospfLsdbApproachingOverflow	1.3.6.1.2.1.14.16.2.15	N/A	N/A	OSPF lsdb approaching overflow trap	OSPF lsdb approaching overflow trap

Table 16-12 Cisco Nexus V2/V3 Traps (continued)

Trap Name	Trap OID	Subtype Varbind OID	Subtype Varbind Value	Description	Short Description
ospfIfStateChange	1.3.6.1.2.1.14.16.2.16	1.3.6.1.2.1.14.7.1.12	N/A	An ospfIfStateChange trap signifies that there has been a change in the state of a non-virtualOSPF interface. This trap should be generated when the interface state regresses (e.g., goes from Dr to Down) or progresses to a terminal state (i.e., Point-to-Point, DR Other, Dr, or Backup)	OSPF interface state changed to Down
ospfIfStateChange	1.3.6.1.2.1.14.16.2.16	1.3.6.1.2.1.14.7.1.12	N/A	An ospfIfStateChange trap signifies that there has been a change in the state of a non-virtualOSPF interface. This trap should be generated when the interface state regresses (e.g., goes from Dr to Down) or progresses to a terminal state (i.e., Point-to-Point, DR Other, Dr, or Backup)	OSPF interface state changed to Up
ospfNssaTranslatorStatusChange	1.3.6.1.2.1.14.16.2.17	N/A	N/A	OSPF NSSA translator status change trap	OSPF NSSA translator status change trap
ospfRestartStatusChange	1.3.6.1.2.1.14.16.2.18	N/A	N/A	OSPF restart status change trap	OSPF restart status change trap
ospfNbrRestartHelperStatusChange	1.3.6.1.2.1.14.16.2.19	N/A	N/A	OSPF neighbor restart helper status change trap	OSPF neighbor restart helper status change trap
ospfVirtNbrRestartHelperStatusChange	1.3.6.1.2.1.14.16.2.20	N/A	N/A	OSPF virtual neighbor restart helper status change trap	OSPF virtual neighbor restart helper status change trap

Cisco CPT V2 Traps

Table 16-13 lists the Cisco CPT V2 traps supported in Prime Network. For associated event types, event subtypes, and Prime Network registry parameters, use the link in the Short Description column or see Table 16-29.

Table 16-13 Cisco CPT V2 Traps

Trap Name	Trap OID	Subtype Varbind OID	Subtype Varbind Value	Description	Short Description
Improper Removal	1.3.6.1.4.1.3607.6.10.30.0.2070	1.3.6.1.4.1.3607.6.10.20.30.20.1.130	10	Improper Removal.	Improper Removal
Improper Removal Cleared	1.3.6.1.4.1.3607.6.10.30.0.2070	1.3.6.1.4.1.3607.6.10.20.30.20.1.130	20	Improper Removal.	Improper Removal Cleared

Table 16-13 Cisco CPT V2 Traps (continued)

Trap Name	Trap OID	Subtype Varbind OID	Subtype Varbind Value	Description	Short Description
Cold Restart	1.3.6.1.4.1.3607.6.10.30.0.2220	1.3.6.1.4.1.3607.6.10.20.30.20.1.130	10	Cold Restart.	Cold Restart
Cold Restart Cleared	1.3.6.1.4.1.3607.6.10.30.0.2220	1.3.6.1.4.1.3607.6.10.20.30.20.1.130	20	Cold Restart.	Cold Restart Cleared

Cisco ASR 5000 Series V2 Traps

Table 16-14 lists the Cisco ASR 5000 Series V2 traps supported in Prime Network. For associated event types, event subtypes, and Prime Network registry parameters, use the link in the Short Description column or see Table 16-30.

Table 16-14 Cisco ASR 5000 Series V2 Traps

Trap Name	Trap OID	Subtype Varbind OID	Subtype Varbind Value	Description	Short Description
starCardRemoved	.1.3.6.1.4.1.8164.2.7	.1.3.6.1.4.1.8164.2.7	7	A card has been removed from the chassis.	Card Removed
starCardInserted	.1.3.6.1.4.1.8164.2.8	.1.3.6.1.4.1.8164.2.8	8	A card has been inserted into the chassis	Card Inserted
starCardRebootRequest	.1.3.6.1.4.1.8164.2.4	.1.3.6.1.4.1.8164.2.4	4	A Reboot operation has been invoked on this card by an administrator	Card Reboot Request
starCardVoltageFailure	.1.3.6.1.4.1.8164.2.6	.1.3.6.1.4.1.8164.2.6	6	A voltage regulation failure has been detected this card.	Card Voltage Failure
starCardMismatch	.1.3.6.1.4.1.8164.2.13	.1.3.6.1.4.1.8164.2.13	13	The card does not match its configuration, or the card does not match the slot it was inserted into, or the card is of an unsupported type	Card Mismatch
starRaidFailed	.1.3.6.1.4.1.8164.2.1077	.1.3.6.1.4.1.8164.2.1077	1077	The specified raid array has failed. The raid array can no longer be used to store data.	Raid Fail
starRaidStarted	.1.3.6.1.4.1.8164.2.1078	.1.3.6.1.4.1.8164.2.1078	1078	The specific raid array has resumed operation.	Raid Start
starGGSNServiceStop	.1.3.6.1.4.1.8164.2.64	.1.3.6.1.4.1.8164.2.64	64	A GGSN Service has stopped	GGSN Service Stop

Table 16-14 Cisco ASR 5000 Series V2 Traps (continued)

Trap Name	Trap OID	Subtype Varbind OID	Subtype Varbind Value	Description	Short Description
starStorageServerClusterStateChange	.1.3.6.1.4.1.8164.2.171	.1.3.6.1.4.1.8164.2.171	171	GTPP Storage Server cluster state has been changed.	Server Cluster State Change
starStorageServerClusSwitchOver	.1.3.6.1.4.1.8164.2.172	.1.3.6.1.4.1.8164.2.172	172	GTPP Storage Server switchover from current online node to next available node in cluster.	Server Cluster SwitchOver
starThreshClearCDRFlowControl	.1.3.6.1.4.1.8164.2.347	.1.3.6.1.4.1.8164.2.347	347	The threshold condition is now clear	The threshold condition is now clear
starRaidRecovered	.1.3.6.1.4.1.8164.2.1080	.1.3.6.1.4.1.8164.2.1080	1080	A Packet Data Network Gateway (PGW) Service has started.	Raid Recovered
starRaidDegraded	.1.3.6.1.4.1.8164.2.1079	.1.3.6.1.4.1.8164.2.1079	1079	The specified raid array is running in a degraded state.	Raid Degraded
starStorageServerUnackedGcdrFileGen	.1.3.6.1.4.1.8164.2.104	.1.3.6.1.4.1.8164.2.104	104	GTPP storage server has exported the unacked GCDRs to file from backup db.	Export Unacknowledged GCDRs from Backup DB
starStorageServerUnackedGcdrVolPurge	.1.3.6.1.4.1.8164.2.103	.1.3.6.1.4.1.8164.2.103	103	GTPP storage server has performed unacked GCDRs volume purge.	Unacknowledged GCDRs Volume Purge
starOSPFv3NeighborFull	.1.3.6.1.4.1.8164.2.1117	.1.3.6.1.4.1.8164.2.1117	1117	An OSPFv3 neighbor is full. A starOSPFv3NeighborFull notification is only sent for neighbors which had previous been declared down via a starOSPFv3NeighborDown notification	OSPF v3 Neighbour Full
starThreshClearLMASessions	.1.3.6.1.4.1.8164.2.413	.1.3.6.1.4.1.8164.2.413	413	The threshold condition is now clear.	The threshold condition is now clear
starCardRemoved	.1.3.6.1.4.1.8164.2.7	.1.3.6.1.4.1.8164.2.7	7	A card has been removed from the chassis.	Card Removed
starThreshLMASessions	.1.3.6.1.4.1.8164.2.412	.1.3.6.1.4.1.8164.2.412	412	The total number of LMA sessions is above the configured threshold value	The total number of LMA sessions is above the configured threshold value
starOSPFNeighborFull	.1.3.6.1.4.1.8164.2.1002	.1.3.6.1.4.1.8164.2.1002	1002	An OSPF neighbor is full.	OSPF Neighbour Full
starOSPFNeighborDown	.1.3.6.1.4.1.8164.2.1001	.1.3.6.1.4.1.8164.2.1001	1001	An OSPF neighbor is down.	OSPF Neighbour Down

Table 16-14 Cisco ASR 5000 Series V2 Traps (continued)

Trap Name	Trap OID	Subtype Varbind OID	Subtype Varbind Value	Description	Short Description
starThreshClearGPRSSessions	.1.3.6.1.4.1.8164.2.433	.1.3.6.1.4.1.8164.2.433	433	he threshold condition is now clear.	GPRS Sessions Threshold Cleared
starThreshClearMAGSessions	.1.3.6.1.4.1.8164.2.415	.1.3.6.1.4.1.8164.2.415	415	The threshold condition is now clear.	The threshold condition is now clear
starThreshGPRSSessions	.1.3.6.1.4.1.8164.2.432	.1.3.6.1.4.1.8164.2.432	432	The total number of GPRS sessions is above the configured threshold value	GPRS Sessions Threshold
starThreshMAGSessions	.1.3.6.1.4.1.8164.2.414	.1.3.6.1.4.1.8164.2.414	414	The total number of MAG sessions is above the configured threshold value.	The total number of MAG sessions is above the configured threshold value
starCertShortLifetime	.1.3.6.1.4.1.8164.2.1043	.1.3.6.1.4.1.8164.2.1043	1043	A certificate is approaching its expiration	Certificate is approaching its expiration
starThreshClearIPPoolAvail	.1.3.6.1.4.1.8164.2.239	.1.3.6.1.4.1.8164.2.239	239	The threshold condition is now clear.	Cleared IP Pool Threshold Available
starThreshNAPTPortChunks	.1.3.6.1.4.1.8164.2.430	.1.3.6.1.4.1.8164.2.430	430	The NAT port chunks utilization of NAT pool is above the configured threshold value.	The NAT port chunks utilization of NAT pool is above the configured
starThreshIPPoolAvail	.1.3.6.1.4.1.8164.2.238	.1.3.6.1.4.1.8164.2.238	238	The available IP pool addresses in a context has fallen below the configured threshold.	IP Pool Threshold Available
starThreshClearStorageUtilization	.1.3.6.1.4.1.8164.2.311	.1.3.6.1.4.1.8164.2.311	311	The threshold condition is now clear.	Storage Utilization Threshold is now clear
starThreshStorageUtilization	.1.3.6.1.4.1.8164.2.310	.1.3.6.1.4.1.8164.2.310	310	The utilization of a mass storage device has exeeded the configured threshold.	Storage Utilization Reached Threshold
starThreshPerServiceGPRSSessions	.1.3.6.1.4.1.8164.2.434	.1.3.6.1.4.1.8164.2.434	434	The total number of GPRS sessions in a service is above the configured threshold value.	Number of GPRS sessions in a service is above the threshold

Table 16-14 Cisco ASR 5000 Series V2 Traps (continued)

Trap Name	Trap OID	Subtype Varbind OID	Subtype Varbind Value	Description	Short Description
starThreshClearGPRSPdpSessions	.1.3.6.1.4.1.8164.2.437	.1.3.6.1.4.1.8164.2.437	437	The threshold condition is now clear.	GPRS Pdp Sessions Threshold Cleared
starThreshGPRSPdpSessions	.1.3.6.1.4.1.8164.2.436	.1.3.6.1.4.1.8164.2.436	436	The total number of GPRS PDP sessions is above the configured threshold value.	GPRS Pdp Sessions Threshold
starThreshPerServiceGPRSPdpSessions	.1.3.6.1.4.1.8164.2.438	.1.3.6.1.4.1.8164.2.438	438	The total number of GPRS PDP sessions in a service is above the configured threshold value.	Number of GPRS PDP sessions in a service is above the threshold value
starThreshClearCPULoad	.1.3.6.1.4.1.8164.2.243	.1.3.6.1.4.1.8164.2.243	243	The threshold condition is now clear.	CPU Load Threshold Cleared
starThreshClearPerServiceGPRSSessions	.1.3.6.1.4.1.8164.2.435	.1.3.6.1.4.1.8164.2.435	435	The threshold condition is now clear.	The threshold condition cleared
starThreshCPULoad	.1.3.6.1.4.1.8164.2.242	.1.3.6.1.4.1.8164.2.242	242	The CPU load for the identified processor has exceeded for configured threshold value for the current monitoring period.	CPU Load Threshold
star5kThreshPCCQuotaSessions	.1.3.6.1.4.1.8164.2.470	.1.3.6.1.4.1.8164.2.470	470	Number of PCC-Quota sessions is above the threshold value.	Number of PCC-Quota sessions is above the threshold value
starThreshClearPerServicePCCPolicySessions	.1.3.6.1.4.1.8164.2.469	.1.3.6.1.4.1.8164.2.469	469	The threshold condition cleared.	The threshold condition cleared
starSystemStartup	.1.3.6.1.4.1.8164.2.1028	.1.3.6.1.4.1.8164.2.1028	1028	The system has completed a reboot/startup.	System Startup
starThreshClearPCCQuotaSessions	.1.3.6.1.4.1.8164.2.471	.1.3.6.1.4.1.8164.2.471	471	The threshold condition cleared.	The threshold condition cleared
starLicenseExpired	.1.3.6.1.4.1.8164.2.1126	.1.3.6.1.4.1.8164.2.1126	1126	A license is in the grace period and should be updated with a new license.	Licence Expired

Table 16-14 Cisco ASR 5000 Series V2 Traps (continued)

Trap Name	Trap OID	Subtype Varbind OID	Subtype Varbind Value	Description	Short Description
starThreshPCCPolicySessions	.1.3.6.1.4.1.8164.2.466	.1.3.6.1.4.1.8164.2.466	466	Number of PCC-Policy sessions is above the threshold value.	Number of PCC-Policy sessions is above the threshold value
starThreshClearPPPSetupFailRate	.1.3.6.1.4.1.8164.2.309	.1.3.6.1.4.1.8164.2.309	309	The threshold condition is now clear.	PPP Setup FailRate Threshold Cleared
starThreshClearPerServiceGPRSPdpSessions	.1.3.6.1.4.1.8164.2.439	.1.3.6.1.4.1.8164.2.439	439	The threshold condition is now clear.	The threshold condition cleared
starThreshPPPSetupFailRate	.1.3.6.1.4.1.8164.2.308	.1.3.6.1.4.1.8164.2.308	308	The threshold condition is now clear.	PPP Setup FailRate Threshold
starThreshLMASessions	.1.3.6.1.4.1.8164.2.412	.1.3.6.1.4.1.8164.2.412	412	The total number of LMA sessions is above the configured threshold value	The total number of LMA sessions is above the configured threshold value
starThreshPerServicePCCPolicySessions	.1.3.6.1.4.1.8164.2.468	.1.3.6.1.4.1.8164.2.468	468	Number of PCC-Policy sessions in a service is above the threshold value.	Number of PCC-Policy sessions in a service is above the threshold value
starThreshClearCPUMemUsage	.1.3.6.1.4.1.8164.2.245	.1.3.6.1.4.1.8164.2.245	245	The threshold condition is now clear.	CPU Memory Usage Threhold cleared
starThreshClearPCCPolicySessions	.1.3.6.1.4.1.8164.2.467	.1.3.6.1.4.1.8164.2.467	467	The threshold condition cleared.	The threshold condition cleared
starThreshCPUMemUsage	.1.3.6.1.4.1.8164.2.244	.1.3.6.1.4.1.8164.2.244	244	The CPU mem usage for the identified processor has exceeded for configured threshold value for the current monitoring period.	CPU Memory Usage Threhold reached
starThreshClearPacketsFilteredDropped	.1.3.6.1.4.1.8164.2.233	.1.3.6.1.4.1.8164.2.233	233	The threshold condition is now clear.	The threshold condition is now clear
starThreshClearCallRejectNoResource	.1.3.6.1.4.1.8164.2.231	.1.3.6.1.4.1.8164.2.231	231	The threshold condition is now clear.	The threshold condition is now clear

Table 16-14 Cisco ASR 5000 Series V2 Traps (continued)

Trap Name	Trap OID	Subtype Varbind OID	Subtype Varbind Value	Description	Short Description
starThreshPacketsFilteredDropped	.1.3.6.1.4.1.8164.2.232	.1.3.6.1.4.1.8164.2.232	232	The number of user data packets filtered has exceeded the configured threshold for the current monitoring period.	User data packets filtered has exceeded the configured threshold
starSystemReboot	.1.3.6.1.4.1.8164.2.1124	.1.3.6.1.4.1.8164.2.1124	1124	The system has rebooted by the operator.	System Reboot
starThreshClearCardTemperatureNearPowerOffLimit	.1.3.6.1.4.1.8164.2.504	.1.3.6.1.4.1.8164.2.504	504	Card Temperature Threshold NearPowerOffLimit Cleared.	Card Temperature Threshold NearPowerOffLimit Cleared
starThreshCardTemperatureNearPowerOffLimit	.1.3.6.1.4.1.8164.2.503	.1.3.6.1.4.1.8164.2.503	503	Card Temperature Threshold NearPowerOffLimit.	Card Temperature Threshold NearPowerOffLimit
starThreshClearSystemCapacity	.1.3.6.1.4.1.8164.2.494	.1.3.6.1.4.1.8164.2.494	494	System Capacity Threshold Cleared.	System Capacity Threshold Cleared
starThreshSystemCapacity	.1.3.6.1.4.1.8164.2.493	.1.3.6.1.4.1.8164.2.493	493	System Capacity Reached Threshold.	System Capacity Reached Threshold
starThreshClearAAAAcctArchive	.1.3.6.1.4.1.8164.2.271	.1.3.6.1.4.1.8164.2.271	271	The threshold condition is now clear.	The threshold condition is now clear.
starThreshAAAAcctArchive	.1.3.6.1.4.1.8164.2.270	.1.3.6.1.4.1.8164.2.270	270	The AAA accounting archive size has gone above the configured threshold.	The AAA accounting archive size has gone above the configured
starThreshClearPerServiceHASessions	.1.3.6.1.4.1.8164.2.259	.1.3.6.1.4.1.8164.2.259	259	The threshold condition is now clear.	The threshold condition is now clear.
starThreshPerServiceHASessions	.1.3.6.1.4.1.8164.2.258	.1.3.6.1.4.1.8164.2.258	258	The total number of HA sessions in a service is above the configured threshold value.	Number of HA sessions in a service is above the configured threshold
starThreshClearDCCAProtocolErrors	.1.3.6.1.4.1.8164.2.313	.1.3.6.1.4.1.8164.2.313	313	The threshold condition is now clear.	The threshold condition is now clear

Table 16-14 Cisco ASR 5000 Series V2 Traps (continued)

Trap Name	Trap OID	Subtype Varbind OID	Subtype Varbind Value	Description	Short Description
starThreshDCCAProtocolErrors	.1.3.6.1.4.1.8164.2.312	.1.3.6.1.4.1.8164.2.312	312	The number of DCCA Protocol Errors has exceeded the configured threshold.	The number of DCCA Protocol Errors has exceeded the configured threshold
starThreshClearAAAMgrQueue	.1.3.6.1.4.1.8164.2.301	.1.3.6.1.4.1.8164.2.301	301	The threshold condition is now clear.	The threshold condition is now clear
starThreshAAAMgrQueue	.1.3.6.1.4.1.8164.2.300	.1.3.6.1.4.1.8164.2.300	300	The Per-AAA Manager internal request queue usage has gone above the configured threshold.	The Per-AAA Manager internal request queue usage has gone above the configured threshold
starThreshDCCABadAnswers	.1.3.6.1.4.1.8164.2.314	.1.3.6.1.4.1.8164.2.314	314	The number of DCCA BadAnswers has exceeded the configured threshold.	The number of DCCA BadAnswers has exceeded the configured threshold
starPowerFilterUnitUnavail	.1.3.6.1.4.1.8164.2.33	.1.3.6.1.4.1.8164.2.33	33	Power Filter Unit (PFU) is unavailable.	Power Filter Unit Unavailable
starThreshClearDCCABadAnswers	.1.3.6.1.4.1.8164.2.315	.1.3.6.1.4.1.8164.2.315	315	The threshold condition is now clear.	The threshold condition is now clear
starPowerFilterUnitAvail	.1.3.6.1.4.1.8164.2.34	.1.3.6.1.4.1.8164.2.34	34	A Power Filter Unit (PFU) is available.	Power Filter Unit Available
starNPUARPPoolExhausted	.1.3.6.1.4.1.8164.2.31	.1.3.6.1.4.1.8164.2.31	31	The ARP pool on this NPU manager is exhausted.	NPU ARP Pool Exhausted
starPowerFilterUnitFailed	.1.3.6.1.4.1.8164.2.32	.1.3.6.1.4.1.8164.2.32	32	A Power Filter Unit (PFU) failed.	Power Filter Unit Failed
starGGSNServiceStart	.1.3.6.1.4.1.8164.2.63	.1.3.6.1.4.1.8164.2.63	63	A GGSN Service has started.	GGSN Service Start
starThreshDCCAUnknownRatingGroup	.1.3.6.1.4.1.8164.2.316	.1.3.6.1.4.1.8164.2.316	316	The number of DCCA UnknownRatingGroup has exceeded the configured threshold.	The number of DCCA UnknownRatingGroup has exceeded the configured threshold

Table 16-14 Cisco ASR 5000 Series V2 Traps (continued)

Trap Name	Trap OID	Subtype Varbind OID	Subtype Varbind Value	Description	Short Description
starThreshDCCARatingFailed	.1.3.6.1.4.1.8164.2.318	.1.3.6.1.4.1.8164.2.318	318	The number of DCCA RatingFailed has exceeded the configured threshold.	The number of DCCA RatingFailed has exceeded the configured threshold
starThreshClearDCCAUnknownRatingGroup	.1.3.6.1.4.1.8164.2.317	.1.3.6.1.4.1.8164.2.317	317	The threshold condition is now clear.	The threshold condition is now clear
starThreshCDRFileSpace	.1.3.6.1.4.1.8164.2.338	.1.3.6.1.4.1.8164.2.338	338	The CDR file space usage is above the configured threshold percentage.	The CDR file space usage is above the configured threshold percentage
starThreshClearDCCARatingFailed	.1.3.6.1.4.1.8164.2.319	.1.3.6.1.4.1.8164.2.319	319	The threshold condition is now clear.	The threshold condition is now clear
starThreshEDRFileSpace	.1.3.6.1.4.1.8164.2.340	.1.3.6.1.4.1.8164.2.340	340	The EDR file space usage is above the configured threshold percentage	The EDR file space usage is above the configured threshold percentage
starThreshClearCDRFileSpace	.1.3.6.1.4.1.8164.2.339	.1.3.6.1.4.1.8164.2.339	339	The threshold condition is now clear.	The threshold condition is now clear
starThreshCDRFlowControl	.1.3.6.1.4.1.8164.2.346	.1.3.6.1.4.1.8164.2.346	346	The number of Charging Data Record (CDR) records which have been discarded at an ACSMGR due to flow control has gone above the configured threshold	The number of CDR records which have been discarded at an ACSMGR
starThreshClearEDRFileSpace	.1.3.6.1.4.1.8164.2.341	.1.3.6.1.4.1.8164.2.341	341	The threshold condition is now clear.	The threshold condition is now clear
starThreshAAAAuthFailRate	.1.3.6.1.4.1.8164.2.218	.1.3.6.1.4.1.8164.2.218	218	The percentage of AAA authentication requests which failed has exceeded the configured threshold during the current monitoring period.	AAA auth requests exceeded threshold

Table 16-14 Cisco ASR 5000 Series V2 Traps (continued)

Trap Name	Trap OID	Subtype Varbind OID	Subtype Varbind Value	Description	Short Description
starThreshClearAAAAuthFailRate	.1.3.6.1.4.1.8164.2.219	.1.3.6.1.4.1.8164.2.219	219	The threshold condition is now clear.	The threshold condition is cleared
starThreshAAAAuthFail	.1.3.6.1.4.1.8164.2.216	.1.3.6.1.4.1.8164.2.216	216	The number of AAA authentication failures has exceeded the configured threshold during the current monitoring period	Number of AAA authentication failures exceeded
starThreshClearAAAAuthFail	.1.3.6.1.4.1.8164.2.217	.1.3.6.1.4.1.8164.2.217	217	The threshold condition is now clear	The threshold condition is cleared
starThreshSubscriberTotal	.1.3.6.1.4.1.8164.2.206	.1.3.6.1.4.1.8164.2.206	206	The total number of subscribers is above the configured threshold value	Number of subscribers above configured threshold value
starThreshClearSubscriberTotal	.1.3.6.1.4.1.8164.2.207	.1.3.6.1.4.1.8164.2.207	207	The threshold condition is now clear.	The threshold condition is cleared
starPCCNtfyIntfPeerUnreachable	.1.3.6.1.4.1.8164.2.1173	.1.3.6.1.4.1.8164.2.1173	1173	The IPCF Event Notification Interface peer cannot be reached	The IPCF Event Notification Interface peer cannot be reached
starLawfulInterceptChanged	.1.3.6.1.4.1.8164.2.1188	.1.3.6.1.4.1.8164.2.1188	1188	Original Lawful Intercept configured by Admin	Original Lawful Intercept configured by Admin
starThreshTpoLowCompressionGain	.1.3.6.1.4.1.8164.2.499	.1.3.6.1.4.1.8164.2.499	499	Number of TPO low compression gain is above the configured	Number of TPO low compression gain is above the configured
starPCCNtfyIntfPeerReachable	.1.3.6.1.4.1.8164.2.1174	.1.3.6.1.4.1.8164.2.1174	1174	The Notification Interface peer can be reached	The Notification Interface peer can be reached
starCdrPurged	.1.3.6.1.4.1.8164.2.1178	.1.3.6.1.4.1.8164.2.1178	1178	CDRs purged	CDRs purged
starDiameterCapabilitiesExchangeFailure	.1.3.6.1.4.1.8164.2.1035	.1.3.6.1.4.1.8164.2.1035	1035	A GS Service has started	Capability negotiations has failed and connections are down

Table 16-14 Cisco ASR 5000 Series V2 Traps (continued)

Trap Name	Trap OID	Subtype Varbind OID	Subtype Varbind Value	Description	Short Description
starThreshClearTpoLowCompressionGain	.1.3.6.1.4.1.8164.2.500	.1.3.6.1.4.1.8164.2.500	500	The threshold condition cleared	The threshold condition cleared
starDiameterIpv6PeerDown	.1.3.6.1.4.1.8164.2.1039	.1.3.6.1.4.1.8164.2.1039	1039	An IUPS Service has started	A diameter peer is down
starDiameterCapabilitiesExchangeSuccess	.1.3.6.1.4.1.8164.2.1036	.1.3.6.1.4.1.8164.2.1036	1036	A GS Service has stopped	A diameter server is up
starDiameterIpv6PeerUp	.1.3.6.1.4.1.8164.2.1040	.1.3.6.1.4.1.8164.2.1040	1040	An IUPS Service has stopped	A diameter peer is up
starThreshClearAAAAcctFail	.1.3.6.1.4.1.8164.2.221	.1.3.6.1.4.1.8164.2.221	221	The threshold condition is now clear	The threshold condition is cleared.
starThreshAAAAcctFail	.1.3.6.1.4.1.8164.2.220	.1.3.6.1.4.1.8164.2.220	220	The number of AAA accounting failures has exceeded the configured threshold during the current monitoring period	AAA accounting exceeded threshold
starThreshClearAAAAcctFailRate	.1.3.6.1.4.1.8164.2.223	.1.3.6.1.4.1.8164.2.223	223	The threshold condition is now clear.	The threshold condition is now clear
starThreshAAAAcctFailRate	.1.3.6.1.4.1.8164.2.222	.1.3.6.1.4.1.8164.2.222	222	The percentage of AAA accounting requests which failed has exceeded the configured threshold during the current monitoring period.	AAA accounting requests exceeded threshold
starThreshClearCallSetup	.1.3.6.1.4.1.8164.2.227	.1.3.6.1.4.1.8164.2.227	227	The threshold condition is now clear	The threshold condition is now clear
starThreshCallSetupFailure	.1.3.6.1.4.1.8164.2.228	.1.3.6.1.4.1.8164.2.228	228	The number of call setup operations which failed has exceeded the configured threshold during the current monitoring period.	Number of call setup operations exceeded threshold
starThreshClearCallSetupFailure	.1.3.6.1.4.1.8164.2.229	.1.3.6.1.4.1.8164.2.229	229	The threshold condition is now clear	The threshold condition is now clear

Table 16-14 Cisco ASR 5000 Series V2 Traps (continued)

Trap Name	Trap OID	Subtype Varbind OID	Subtype Varbind Value	Description	Short Description
starThreshCallRejectNoResource	.1.3.6.1.4.1.8164.2.230	.1.3.6.1.4.1.8164.2.230	230	The number of call setup operations which were rejected due to a no resource condition has exceeded the configured threshold during the current monitoring period	Number of call setup operations rejected due to a no resource condition exceeded threshold
starThreshAAARetryRate	.1.3.6.1.4.1.8164.2.224	.1.3.6.1.4.1.8164.2.224	224	The percentage of AAA requests which has to be retried has exceeded the configured threshold during the current monitoring period	AAA requests exceeded threshold
starThreshClearAAARetryRate	.1.3.6.1.4.1.8164.2.225	.1.3.6.1.4.1.8164.2.225	225	The threshold condition is now clear	The threshold condition is now clear.
starDiameterServerReachable	.1.3.6.1.4.1.8164.2.187	.1.3.6.1.4.1.8164.2.187	187	A diameter server is up.	A diameter server is up
starThreshCallSetup	.1.3.6.1.4.1.8164.2.226	.1.3.6.1.4.1.8164.2.226	226	The number of call setup operations has exceeded the configured threshold during the current monitoring period.	number of call setup operations has exceeded threshold
starCDRFileRemoved	.1.3.6.1.4.1.8164.2.188	.1.3.6.1.4.1.8164.2.188	188	A Charging Data Record (CDR) file has been deleted from the system due to a lack of available storage space.	CDR file has been deleted from the system
starDiameterPeerUp	.1.3.6.1.4.1.8164.2.185	.1.3.6.1.4.1.8164.2.185	185	A diameter peer is up.	A diameter peer is up
starDiameterServerUnreachable	.1.3.6.1.4.1.8164.2.186	.1.3.6.1.4.1.8164.2.186	186	A diameter server is down.	A diameter server is down
starThreshAAAAcctArchiveQueue-1	.1.3.6.1.4.1.8164.2.505	.1.3.6.1.4.1.8164.2.505	505	The Per-Sessmgr Archive queue usage is above the configured threshold percentage	The Per-Sessmgr Archive queue usage is above the configured threshold percentage
starThreshClearAAAAcctArchiveQueue-1	.1.3.6.1.4.1.8164.2.506	.1.3.6.1.4.1.8164.2.506	506	The threshold condition cleared	The threshold condition cleared
starDiameterPeerDown	.1.3.6.1.4.1.8164.2.184	.1.3.6.1.4.1.8164.2.184	184	A diameter peer is down.	A diameter peer is down

Table 16-14 Cisco ASR 5000 Series V2 Traps (continued)

Trap Name	Trap OID	Subtype Varbind OID	Subtype Varbind Value	Description	Short Description
starThreshAAAAcctArchiveQueue-2	.1.3.6.1.4.1.8164.2.507	.1.3.6.1.4.1.8164.2.507	507	The Sessmgr Archive queue usage is above the configured threshold percentage	The Sessmgr Archive queue usage is above the configured threshold percentage
starCgfDead	.1.3.6.1.4.1.8164.2.77	.1.3.6.1.4.1.8164.2.77	77	GTPP CGF Server Dead.	GTPP CGF Server Dead
starThreshClearAAAAcctArchiveQueue-2	.1.3.6.1.4.1.8164.2.508	.1.3.6.1.4.1.8164.2.508	508	The threshold condition cleared	The threshold condition cleared
starGtpcPathFailure	.1.3.6.1.4.1.8164.2.71	.1.3.6.1.4.1.8164.2.71	71	GTP Control Path Failure.	GTPC Path Failure
starThreshAAAAcctArchiveQueue-3	.1.3.6.1.4.1.8164.2.509	.1.3.6.1.4.1.8164.2.509	509	The Sessmgr Archive queue usage is above the configured threshold percentage	The Sessmgr Archive queue usage is above the configured threshold percentage
starThreshClearAAAAcctArchiveQueue-3	.1.3.6.1.4.1.8164.2.510	.1.3.6.1.4.1.8164.2.510	510	The Sessmgr Archive queue usage is above the configured threshold percentage	The threshold condition cleared
starCgfAlive	.1.3.6.1.4.1.8164.2.76	.1.3.6.1.4.1.8164.2.76	76	GTPP CGF Server Alive.	GTPP CGF Server Alive
starHeartbeat	.1.3.6.1.4.1.8164.2.166	.1.3.6.1.4.1.8164.2.166	166	Periodic SNMP heartbeat. A starHeartbeat notification can be generated periodically if the system is configured to do so. These notifications serve only to validate that there is communication to external entities which sink SNMP notifications	Periodic SNMP heartbeat
starAAAAccServerMisconfigured	.1.3.6.1.4.1.8164.2.44	.1.3.6.1.4.1.8164.2.44	44	The Authentication, Authorization and Accounting (AAA) server has been misconfigured.	The AAA server has been misconfigured
starGtpuPathFailure	.1.3.6.1.4.1.8164.2.72	.1.3.6.1.4.1.8164.2.72	72	GTP Data Path Failure.	GTP Data Path Failure
starAAAArchiveStarted	.1.3.6.1.4.1.8164.2.1191	.1.3.6.1.4.1.8164.2.1191	1191	Archive started	Archive started

Table 16-14 Cisco ASR 5000 Series V2 Traps (continued)

Trap Name	Trap OID	Subtype Varbind OID	Subtype Varbind Value	Description	Short Description
starThreshGGSNSessions	.1.3.6.1.4.1.8164.2.248	.1.3.6.1.4.1.8164.2.248	248	The total number of GGSN sessions is above the configured threshold value	Threshold GGSN sessions
starStorageServerCPUNormal	.1.3.6.1.4.1.8164.2.136	.1.3.6.1.4.1.8164.2.136	136	GTPP Storage Server CPU usage has returned to a normal range.	Storage Server CPU Normal
starGgsnInitiatedUpdtFailed	.1.3.6.1.4.1.8164.2.80	.1.3.6.1.4.1.8164.2.80	80	GGSN Initiated Update PDP Context Response Failed.	GGSN initiate update failed
starThreshSGWSessions	.1.3.6.1.4.1.8164.2.408	.1.3.6.1.4.1.8164.2.408	408	The total number of SGW sessions is above the configured threshold value.	SGW sessions is above the configured threshold value.
starPGWServiceStop	.1.3.6.1.4.1.8164.2.1082	.1.3.6.1.4.1.8164.2.1082	1082	PGW Service stopped	PGW Service stopped
starPGWServiceStart	.1.3.6.1.4.1.8164.2.1081	.1.3.6.1.4.1.8164.2.1081	1081	PGW Service started	PGW Service started
starThreshClearPGWSessions	.1.3.6.1.4.1.8164.2.411	.1.3.6.1.4.1.8164.2.411	411	The threshold condition is now clear.	PGW sessions threshold condition cleared
starThreshPGWSessions	.1.3.6.1.4.1.8164.2.410	.1.3.6.1.4.1.8164.2.410	410	The total number of PGW sessions is above the configured threshold value	PGW sessions are above the configured threshold value
starThreshClearPerServiceGGSNSessions	.1.3.6.1.4.1.8164.2.257	.1.3.6.1.4.1.8164.2.257	257	The threshold condition is now clear	Threshold Per Service GGSN Sessions Cleared
starThreshPerServiceGGSNSessions	.1.3.6.1.4.1.8164.2.256	.1.3.6.1.4.1.8164.2.256	256	The total number of GGSN sessions in a service is above the configured threshold value	Threshold Per Service GGSN Sessions
starThreshClearGGSNSessions	.1.3.6.1.4.1.8164.2.249	.1.3.6.1.4.1.8164.2.249	249	The threshold condition is now clear	Threshold GGSN sessions cleared
starOverloadService	.1.3.6.1.4.1.8164.2.169	.1.3.6.1.4.1.8164.2.169	169	A service-specific congestion overload condition has occurred	Service Overload
starOverloadSystemClear	.1.3.6.1.4.1.8164.2.168	.1.3.6.1.4.1.8164.2.168	168	A system-wide congestion overload condition has cleared	System Overload Cleared
starStorageServerCPUBusy	.1.3.6.1.4.1.8164.2.135	.1.3.6.1.4.1.8164.2.135	135	GTPP Storage Server is experiencing high CPU usage.	Storage Server CPU Busy
starOverloadServiceClear	.1.3.6.1.4.1.8164.2.170	.1.3.6.1.4.1.8164.2.170	170	A service-specific congestion overload condition has cleared	Service Overload Cleared

Table 16-14 Cisco ASR 5000 Series V2 Traps (continued)

Trap Name	Trap OID	Subtype Varbind OID	Subtype Varbind Value	Description	Short Description
starOverloadSystem	.1.3.6.1.4.1.8164.2.167	.1.3.6.1.4.1.8164.2.167	167	A system-wide congestion overload condition has occurred.	System Overload
starMVGPeerUp	.1.3.6.1.4.1.8164.2.1170	.1.3.6.1.4.1.8164.2.1170	1170	A MVG peer is up	A MVG peer is up
starStorageServerDiskSpaceLow	.1.3.6.1.4.1.8164.2.137	.1.3.6.1.4.1.8164.2.137	137	GTPP Storage Server is experiencing low available disk space.	Storage Server DiskSpace Low
starStorageServerDiskSpaceOk	.1.3.6.1.4.1.8164.2.138	.1.3.6.1.4.1.8164.2.138	138	GTPP Storage Server available disk space to a normal range.	Storage Server Low DiskSpace Cleared
starSGTPServiceStart	.1.3.6.1.4.1.8164.2.1141	.1.3.6.1.4.1.8164.2.1141	1141	A SGTP Service has started	A SGTP Service has started
starTaskFailed	.1.3.6.1.4.1.8164.2.150	.1.3.6.1.4.1.8164.2.150	150	A non-critical task has failed and the appropriate recovery steps begun.	Task Failed
starMVGPeerDown	.1.3.6.1.4.1.8164.2.1169	.1.3.6.1.4.1.8164.2.1169	1169	A MVG peer is down	A MVG peer is down
starTaskRestart	.1.3.6.1.4.1.8164.2.151	.1.3.6.1.4.1.8164.2.151	151	A non-critical task has restarted after an earlier failure	Task Restarted
starAAAAuthServerUnreachable	.1.3.6.1.4.1.8164.2.39	.1.3.6.1.4.1.8164.2.39	39	The Authentication, Authorization and Accouting (AAA) server cannot be reached	AAA AuthServer Unreachable
starAAAAuthServerReachable	.1.3.6.1.4.1.8164.2.40	.1.3.6.1.4.1.8164.2.40	40	The Authentication, Authorization and Accouting (AAA) server is now reachable.	AAA AuthServer Reachable
starAAAAccServerUnreachable	.1.3.6.1.4.1.8164.2.42	.1.3.6.1.4.1.8164.2.42	42	The Authentication, Authorization and Accouting (AAA) server cannot be reached	AAA AccServer Unreachable
starAAAAuthServerReachable	.1.3.6.1.4.1.8164.2.40	.1.3.6.1.4.1.8164.2.40	40	The Authentication, Authorization and Accouting (AAA) server is now reachable.	AAA AccServer Reachable
starAAAAccServerUnreachable	.1.3.6.1.4.1.8164.2.42	.1.3.6.1.4.1.8164.2.42	42	The Authentication, Authorization and Accouting (AAA) server cannot be reached	AAA AccServer Unreachable

Table 16-14 Cisco ASR 5000 Series V2 Traps (continued)

Trap Name	Trap OID	Subtype Varbind OID	Subtype Varbind Value	Description	Short Description
starAAAAccServerReachable	.1.3.6.1.4.1.8164.2.43	.1.3.6.1.4.1.8164.2.43	43	The Authentication, Authorization and Accouting (AAA) server is now reachable.	AAA AccServer Reachable
starPCCPolicyServiceStart	.1.3.6.1.4.1.8164.2.1127	.1.3.6.1.4.1.8164.2.1127	1127	A PCC-Policy Service has started	A PCC-Policy Service has started
starPCCQuotaServiceStop	.1.3.6.1.4.1.8164.2.1130	.1.3.6.1.4.1.8164.2.1130	1130	A PCC-Quota Service has stopped	A PCC-Quota Service has stopped
starPCCPolicyServiceStop	.1.3.6.1.4.1.8164.2.1128	.1.3.6.1.4.1.8164.2.1128	1128	A PCC-Policy Service has stopped	A PCC-Policy Service has stopped
starPCCAFServiceStart	.1.3.6.1.4.1.8164.2.1131	.1.3.6.1.4.1.8164.2.1131	1131	A PCC-AF Service has started	A PCC-AF Service has started
starSGTPServiceStop	.1.3.6.1.4.1.8164.2.1142	.1.3.6.1.4.1.8164.2.1142	1142	A SGTP Service has stopped.	A SGTP Service has stopped
starPCCQuotaServiceStart	.1.3.6.1.4.1.8164.2.1129	.1.3.6.1.4.1.8164.2.1129	1129	A PCC-Quota Service has started	A PCC-Quota Service has started
starPCCAFServiceStop	.1.3.6.1.4.1.8164.2.1132	.1.3.6.1.4.1.8164.2.1132	1132	A PCC-AF Service has stopped	A PCC-AF Service has stopped
starStrgSrvrClusMemLow	.1.3.6.1.4.1.8164.2.179	.1.3.6.1.4.1.8164.2.179	179	GTPP Storage Server is experiencing a low memory condition.	GTPP Storage Server Memory Low
starCertValid	.1.3.6.1.4.1.8164.2.1045	.1.3.6.1.4.1.8164.2.1045	1045	Valid Certificate Configured	Valid Certificate Configured
starStrgSrvrClusMemOK	.1.3.6.1.4.1.8164.2.180	.1.3.6.1.4.1.8164.2.180	180	GTPP Storage Server Memory usage has returned to a normal range.	GTPP Storage Server Memory Normal
starStrgSrvrClusPathOK	.1.3.6.1.4.1.8164.2.174	.1.3.6.1.4.1.8164.2.174	174	GTPP Storage Server cluster disk path failure has been restored to ok state	GTPP Storage Server Cluster Disk Path Failure Restored to OK
starEgtpcPathFailureClear	.1.3.6.1.4.1.8164.2.1113	.1.3.6.1.4.1.8164.2.1113	1113	EGTP Control Path Failure condition is no longer valid	EGTP Control Path Failure condition is no longer valid.
starEgtpuPathFailure	.1.3.6.1.4.1.8164.2.1119	.1.3.6.1.4.1.8164.2.1119	1119	No response received for GTP-U ECHO requests. Data path failure detected towards peer EPC Node.	No response received for GTP-U ECHO requests

Table 16-14 Cisco ASR 5000 Series V2 Traps (continued)

Trap Name	Trap OID	Subtype Varbind OID	Subtype Varbind Value	Description	Short Description
starStrgSrvrClusIntercFail	.1.3.6.1.4.1.8164.2.175	.1.3.6.1.4.1.8164.2.175	175	GTPP Storage Server cluster transport path (Interconnect) failure has been occurred	GTPP Storage Server Cluster Transport Path Failure
starEgtpuPathFailureClear	.1.3.6.1.4.1.8164.2.1120	.1.3.6.1.4.1.8164.2.1120	1120	M3UA Stream Control Transmission Protocol(SCTP) association establishment failure.	The data path to the peer EPC node which was down is now available
starStorageServerCDRLoss	.1.3.6.1.4.1.8164.2.1121	.1.3.6.1.4.1.8164.2.1121	1121	M3UA Stream Control Transmission Protocol (SCTP) association establishment ok	GTPP Storage Server is experiencing CDR Loss greater than the configured threshold value at the GSS
starStrgSrvrClusPathFail	.1.3.6.1.4.1.8164.2.173	.1.3.6.1.4.1.8164.2.173	173	GTPP Storage Server cluster disk path failure has been occured.	GTPP Storage Server Cluster Disk Path Failure
starStrgSrvrClusIfOK	.1.3.6.1.4.1.8164.2.178	.1.3.6.1.4.1.8164.2.178	178	GTPP Storage Server cluster GE Interface failure failure has been restored to ok state.	GTPP Storage Server Cluster GE Interface Failure Restored to OK
starCertExpired	.1.3.6.1.4.1.8164.2.1044	.1.3.6.1.4.1.8164.2.1044	1044	Certificate Expired	Certificate Expired
starStrgSrvrClusIntercOK	.1.3.6.1.4.1.8164.2.176	.1.3.6.1.4.1.8164.2.176	176	GTPP Storage Server cluster transport path (Interconnect) failure has been restored to an operational state.	GTPP Storage Server Cluster Transport Path Failure Restored to OK
starStrgSrvrClusIfFail	.1.3.6.1.4.1.8164.2.177	.1.3.6.1.4.1.8164.2.177	177	GTPP Storage Server cluster GE Interface failure has been occured.	GTPP Storage Server Cluster GE Interface Failure
starEGTPServiceStart	.1.3.6.1.4.1.8164.2.1085	.1.3.6.1.4.1.8164.2.1085	1085	An Evolved GPRS Tunneling Protocol (EGTP) Service has started	An Evolved GPRS Tunneling Protocol (EGTP) Service has started
starLMAServiceStop	.1.3.6.1.4.1.8164.2.1088	.1.3.6.1.4.1.8164.2.1088	1088	A Local Mobility Anchor (LMA) Service has stopped	A Local Mobility Anchor (LMA) Service has stopped
starLMAServiceStart	.1.3.6.1.4.1.8164.2.1087	.1.3.6.1.4.1.8164.2.1087	1087	A Local Mobility Anchor (LMA) Service has started	A Local Mobility Anchor (LMA) Service has started

Table 16-14 Cisco ASR 5000 Series V2 Traps (continued)

Trap Name	Trap OID	Subtype Varbind OID	Subtype Varbind Value	Description	Short Description
starMAGServiceStop	.1.3.6.1.4.1.8164.2.1090	.1.3.6.1.4.1.8164.2.1090	1090	A MAG Service has stopped	A MAG Service has stopped
starNTPSyncEstablished	.1.3.6.1.4.1.8164.2.106	.1.3.6.1.4.1.8164.2.106	106	NTP Synchronization Established.	NTP Sync Established
starPCCPolicyServiceStart	.1.3.6.1.4.1.8164.2.1127	.1.3.6.1.4.1.8164.2.1127	1127	A PCC-Policy Service has started	A PCC-Policy Service has started
starPCCQuotaServiceStop	.1.3.6.1.4.1.8164.2.1130	.1.3.6.1.4.1.8164.2.1130	1130	A PCC-Quota Service has stopped	A PCC-Quota Service has stopped
starPCCPolicyServiceStop	.1.3.6.1.4.1.8164.2.1128	.1.3.6.1.4.1.8164.2.1128	1128	A PCC-Policy Service has stopped	A PCC-Policy Service has stopped
starPCCAFServiceStart	.1.3.6.1.4.1.8164.2.1131	.1.3.6.1.4.1.8164.2.1131	1131	A PCC-AF Service has started	A PCC-AF Service has started
starSGTPServiceStop	.1.3.6.1.4.1.8164.2.1142	.1.3.6.1.4.1.8164.2.1142	1142	A SGTP Service has stopped.	A SGTP Service has stopped
starPCCQuotaServiceStart	.1.3.6.1.4.1.8164.2.1129	.1.3.6.1.4.1.8164.2.1129	1129	A PCC-Quota Service has started	A PCC-Quota Service has started
starPCCAFServiceStop	.1.3.6.1.4.1.8164.2.1132	.1.3.6.1.4.1.8164.2.1132	1132	A PCC-AF Service has stopped	A PCC-AF Service has stopped
starStrgSrvrClusMemLow	.1.3.6.1.4.1.8164.2.179	.1.3.6.1.4.1.8164.2.179	179	GTPP Storage Server is experiencing a low memory condition.	GTPP Storage Server Memory Low
starCertValid	.1.3.6.1.4.1.8164.2.1045	.1.3.6.1.4.1.8164.2.1045	1045	Valid Certificate Configured	Valid Certificate Configured
starStrgSrvrClusMemOK	.1.3.6.1.4.1.8164.2.180	.1.3.6.1.4.1.8164.2.180	180	GTPP Storage Server Memory usage has returned to a normal range.	GTPP Storage Server Memory Normal
starStrgSrvrClusPathOK	.1.3.6.1.4.1.8164.2.174	.1.3.6.1.4.1.8164.2.174	174	GTPP Storage Server cluster disk path failure has been restored to ok state	GTPP Storage Server Cluster Disk Path Failure Restored to OK
starEgtpcPathFailureClear	.1.3.6.1.4.1.8164.2.1113	.1.3.6.1.4.1.8164.2.1113	1113	EGTP Control Path Failure condition is no longer valid	EGTP Control Path Failure condition is no longer valid.
starEgtpuPathFailure	.1.3.6.1.4.1.8164.2.1119	.1.3.6.1.4.1.8164.2.1119	1119	No response received for GTP-U ECHO requests. Data path failure detected towards peer EPC Node.	No response received for GTP-U ECHO requests

Table 16-14 Cisco ASR 5000 Series V2 Traps (continued)

Trap Name	Trap OID	Subtype Varbind OID	Subtype Varbind Value	Description	Short Description
starStrgSrvrClusIntercFail	.1.3.6.1.4.1.8164.2.175	.1.3.6.1.4.1.8164.2.175	175	GTPP Storage Server cluster transport path (Interconnect) failure has been occurred	GTPP Storage Server Cluster Transport Path Failure
starEgtpuPathFailureClear	.1.3.6.1.4.1.8164.2.1120	.1.3.6.1.4.1.8164.2.1120	1120	M3UA Stream Control Transmission Protocol(SCTP) association establishment failure.	The data path to the peer EPC node which was down is now available
starStorageServerCDRLoss	.1.3.6.1.4.1.8164.2.1121	.1.3.6.1.4.1.8164.2.1121	1121	M3UA Stream Control Transmission Protocol (SCTP) association establishment ok	GTPP Storage Server is experiencing CDR Loss greater than the configured threshold value at the GSS
starStrgSrvrClusPathFail	.1.3.6.1.4.1.8164.2.173	.1.3.6.1.4.1.8164.2.173	173	GTPP Storage Server cluster disk path failure has been occured.	GTPP Storage Server Cluster Disk Path Failure
starStrgSrvrClusIfOK	.1.3.6.1.4.1.8164.2.178	.1.3.6.1.4.1.8164.2.178	178	GTPP Storage Server cluster GE Interface failure failure has been restored to ok state.	GTPP Storage Server Cluster GE Interface Failure Restored to OK
starCertExpired	.1.3.6.1.4.1.8164.2.1044	.1.3.6.1.4.1.8164.2.1044	1044	Certificate Expired	Certificate Expired
starStrgSrvrClusIntercOK	.1.3.6.1.4.1.8164.2.176	.1.3.6.1.4.1.8164.2.176	176	GTPP Storage Server cluster transport path (Interconnect) failure has been restored to an operational state.	GTPP Storage Server Cluster Transport Path Failure Restored to OK
starStrgSrvrClusIfFail	.1.3.6.1.4.1.8164.2.177	.1.3.6.1.4.1.8164.2.177	177	GTPP Storage Server cluster GE Interface failure has been occured.	GTPP Storage Server Cluster GE Interface Failure
starEGTPServiceStart	.1.3.6.1.4.1.8164.2.1085	.1.3.6.1.4.1.8164.2.1085	1085	An Evolved GPRS Tunneling Protocol (EGTP) Service has started	An Evolved GPRS Tunneling Protocol (EGTP) Service has started
starLMAServiceStop	.1.3.6.1.4.1.8164.2.1088	.1.3.6.1.4.1.8164.2.1088	1088	A Local Mobility Anchor (LMA) Service has stopped	A Local Mobility Anchor (LMA) Service has stopped
starLMAServiceStart	.1.3.6.1.4.1.8164.2.1087	.1.3.6.1.4.1.8164.2.1087	1087	A Local Mobility Anchor (LMA) Service has started	A Local Mobility Anchor (LMA) Service has started

Table 16-14 Cisco ASR 5000 Series V2 Traps (continued)

Trap Name	Trap OID	Subtype Varbind OID	Subtype Varbind Value	Description	Short Description
starMAGServiceStop	.1.3.6.1.4.1.8164.2.1090	.1.3.6.1.4.1.8164.2.1090	1090	A MAG Service has stopped	A MAG Service has stopped
starNTPSyncEstablished	.1.3.6.1.4.1.8164.2.106	.1.3.6.1.4.1.8164.2.106	106	NTP Synchronization Established.	NTP Sync Established
starNTPSyncLost	.1.3.6.1.4.1.8164.2.91	.1.3.6.1.4.1.8164.2.91	91	NTP Synchronization Lost.	NTP Sync lost
starNTPPeerReachable	.1.3.6.1.4.1.8164.2.105	.1.3.6.1.4.1.8164.2.105	105	NTP Peer Reachable.	NTP Peer Reachable
starNTPPeerUnreachable	.1.3.6.1.4.1.8164.2.90	.1.3.6.1.4.1.8164.2.90	90	NTP Peer Unreachable.	NTP Peer UnReachable
starConfigurationUpdate	.1.3.6.1.4.1.8164.2.1100	.1.3.6.1.4.1.8164.2.1100	1100	The configuration of the chassis has been changed.	Config change
SNMPLinkUp	.1.3.6.1.6.3.1.1.5.4	.1.3.6.1.6.3.1.1.5.4	4	The Interface Index for this trap is the IfIndex for the physical port, not the logical interface.	Link Up
SNMPLinkDown	.1.3.6.1.6.3.1.1.5.3	.1.3.6.1.6.3.1.1.5.3	3	The Interface Index for this trap is the IfIndex for the physical port, not the logical interface.	Link Down
starSGWServiceStop	.1.3.6.1.4.1.8164.2.1084	.1.3.6.1.4.1.8164.2.1084	1084	A Serving Gateway (SGW) Service has stopped.an indication of the failure.	SGW Service stopped
starBGPPeerSessionUp	.1.3.6.1.4.1.8164.2.118	.1.3.6.1.4.1.8164.2.118	118	The BGP peer session to the specified IP address is operational.	NTP Sync lost
starBGPPeerSessionDown	.1.3.6.1.4.1.8164.2.119	.1.3.6.1.4.1.8164.2.119	119	The BGP peer session to the specified IP address is no longer operational.	BGP Peer Session Down
starThreshClearPCCAFSessions	.1.3.6.1.4.1.8164.2.475	.1.3.6.1.4.1.8164.2.475	475	PCCAFSessions threshold condition is now clear.	PCCA threshold condition cleared
starThreshPCCAFSessions	.1.3.6.1.4.1.8164.2.474	.1.3.6.1.4.1.8164.2.474	474	The total number of PCC-AF sessions is above the configured threshold value.	Number of PCC-AF sessions is above the threshold value
starThreshClearSGWSessions	.1.3.6.1.4.1.8164.2.409	.1.3.6.1.4.1.8164.2.409	409	SGWSessions threshold condition is now clear.	SGW Sessions threshold condition cleared
starDhcpServiceStarted	.1.3.6.1.4.1.8164.2.154	.1.3.6.1.4.1.8164.2.154	154	A DHCP Service has started	Dhcp Service Started

Table 16-14 Cisco ASR 5000 Series V2 Traps (continued)

Trap Name	Trap OID	Subtype Varbind OID	Subtype Varbind Value	Description	Short Description
starThreshClearPerServicePCCQuotaSessions	.1.3.6.1.4.1.8164.2.473	.1.3.6.1.4.1.8164.2.473	473	ServicePCCQuotaSessions threshold condition is now clear.	Number of PCC-Quota sessions threshold condition cleared
starSGWServiceStart	.1.3.6.1.4.1.8164.2.1083	.1.3.6.1.4.1.8164.2.1083	1083	A Serving Gateway (SGW) Service has started.	SGW Service started
starThreshPerServicePCCQuotaSessions	.1.3.6.1.4.1.8164.2.472	.1.3.6.1.4.1.8164.2.472	472	The total number of PCC-Quota sessions in a service is above the configured threshold	Number of PCC-Quota sessions threshold condition cleared
starThreshClearDiameterRetryRate	.1.3.6.1.4.1.8164.2.483	.1.3.6.1.4.1.8164.2.483	483	DiameterRetryRate threshold condition is now clear	The threshold condition cleared
starDhcpAlive	.1.3.6.1.4.1.8164.2.88	.1.3.6.1.4.1.8164.2.88	88	DHCP Server Alive.	DHCP Alive
starStrgSrvrClusPathOK	.1.3.6.1.4.1.8164.2.174	.1.3.6.1.4.1.8164.2.174	174	GTPP Storage Server cluster disk path failure has been restored to ok state	GTPP Storage Server Cluster Transport Path Failure Restored to OK
starThreshDiameterRetryRate	.1.3.6.1.4.1.8164.2.482	.1.3.6.1.4.1.8164.2.482	482	The percentage of Diameter requests which has to be retried has exceeded the configured threshold during the current monitoring period.	The percentage of Diameter requests which has to be retried has exceeded the configured threshold
starDhcpServiceStopped	.1.3.6.1.4.1.8164.2.155	.1.3.6.1.4.1.8164.2.155	155	A DHCP Service has stopped.	Dhcp Service Stopped
starThreshClearPerServicePCCAFSessions	.1.3.6.1.4.1.8164.2.477	.1.3.6.1.4.1.8164.2.477	477	starThreshClearPerServicePCCAFSessions	The threshold condition cleared
starStorageServerAlive	.1.3.6.1.4.1.8164.2.78	.1.3.6.1.4.1.8164.2.78	78	GTPP Storage Server is Alive.	Storage Server Alive
starThreshPerServicePCCAFSessions	.1.3.6.1.4.1.8164.2.476	.1.3.6.1.4.1.8164.2.476	476	The total number of PCC-AF sessions in a service is above the configured threshold value.	The threshold condition cleared
starDhcpDead	.1.3.6.1.4.1.8164.2.89	.1.3.6.1.4.1.8164.2.89	89	DHCP Server Dead.	DHCP Dead

Table 16-14 Cisco ASR 5000 Series V2 Traps (continued)

Trap Name	Trap OID	Subtype Varbind OID	Subtype Varbind Value	Description	Short Description
starServiceLossLC	.1.3.6.1.4.1.8164.2.84	.1.3.6.1.4.1.8164.2.84	84	A service loss condition has occurred due to LC failure or removal.	Service Loss LC
starStorageServerDead	.1.3.6.1.4.1.8164.2.79	.1.3.6.1.4.1.8164.2.79	79	GTPP Storage Server is Dead.	Storage Server Dead
starThreshTpoRtoTimeout	.1.3.6.1.4.1.8164.2.495	.1.3.6.1.4.1.8164.2.495	495	The total number of TPO RTO timeouts is above the configured.	Number of TPO RTO timeouts is above the configured
starThreshClearNPUUtilization	.1.3.6.1.4.1.8164.2.479	.1.3.6.1.4.1.8164.2.479	479	NPU Utilization threshold condition is now clear.	NPU Utilization Threshold reached
starThreshHNBGWIuSess	.1.3.6.1.4.1.8164.2.488	.1.3.6.1.4.1.8164.2.488	488	The chassis-wide count of current HNBGW IU sessions has gone above the configured threshold	The chassis-wide count of current HNBGW IU sessions has gone above the configured threshold
starServiceLossPTACs	.1.3.6.1.4.1.8164.2.83	.1.3.6.1.4.1.8164.2.83	83	A service loss condition has occurred due to PAC/PSC/TAC failure or removal.	Service Loss PTACs
starThreshNPUUtilization	.1.3.6.1.4.1.8164.2.478	.1.3.6.1.4.1.8164.2.478	478	The overall NPU utilization for the identified processor has exceeded for configured threshold value for the current monitoring period.	NPU Utilization Threshold reached
starCLISessionEnd	.1.3.6.1.4.1.8164.2.53	.1.3.6.1.4.1.8164.2.53	53	An interactive CLI session has ended.	CLISession End
starCLISessionStart	.1.3.6.1.4.1.8164.2.52	.1.3.6.1.4.1.8164.2.52	52	An interactive CLI session has started.	CLISession start
starThreshClearTpoRtoTimeout	.1.3.6.1.4.1.8164.2.496	.1.3.6.1.4.1.8164.2.496	496	TpoRtoTimeout threshold condition is now clear.	Number of TPO RTO timeouts is above the configured
starThreshClearCPUOrbsCritical	.1.3.6.1.4.1.8164.2.305	.1.3.6.1.4.1.8164.2.305	305	CPU Orbs threshold condition is now clear	Thresh CPU Orbs Critical Cleared
starThreshClearTpoDnsFailure	.1.3.6.1.4.1.8164.2.498	.1.3.6.1.4.1.8164.2.498	498	Tpo DNS Failure threshold condition is now clear.	The threshold condition cleared

Table 16-14 Cisco ASR 5000 Series V2 Traps (continued)

Trap Name	Trap OID	Subtype Varbind OID	Subtype Varbind Value	Description	Short Description
starThreshCPUOrbsCritical	.1.3.6.1.4.1.8164.2.304	.1.3.6.1.4.1.8164.2.304	304	The ORBs task has exceeded the CPU usage configured as a critical error	Thresh CPU Orbs Critical
starThreshTpoDnsFailure	.1.3.6.1.4.1.8164.2.497	.1.3.6.1.4.1.8164.2.497	497	The total number of TPO DNS query failure is above the configured threshold value.	Number of TPO DNS query failure is above the configured threshold value
starIPMSServerReachable	.1.3.6.1.4.1.8164.2.1042	.1.3.6.1.4.1.8164.2.1042	1042	An IPMS server is reachable. A starIPMSServerReachable notification is only generated for servers which had previously been declared unreachable.	An IPMS server is reachable
starIPMSServerUnreachable	.1.3.6.1.4.1.8164.2.1041	.1.3.6.1.4.1.8164.2.1041	1041	An IPMS server is unreachable.	An IPMS server is unreachable
starLicenseExceeded	.1.3.6.1.4.1.8164.2.65	.1.3.6.1.4.1.8164.2.65	65	The licenses session limit has been exceeded; note that a small number of sessions are permitted beyond the licensed limit.	License Exceeded
starSS7PCCongestionCleared	.1.3.6.1.4.1.8164.2.1057	.1.3.6.1.4.1.8164.2.1057	1057	SS7 Point code Congestion gets cleared, one of the routes to this point-code is cleared from congestion.	SS7 Point code Congestion gets cleared
starCardSPOFClear	.1.3.6.1.4.1.8164.2.140	.1.3.6.1.4.1.8164.2.140	140	The identified card is no longer a Single Point of Failure (SPOF)	Card SPOF Alarm Cleared
starSS7PCCongested	.1.3.6.1.4.1.8164.2.1056	.1.3.6.1.4.1.8164.2.1056	1056	SS7 Point code is congested, all the routes to this point-code is congested.	SS7 Point code Congestion gets cleared
starCardSPOFAlarm	.1.3.6.1.4.1.8164.2.139	.1.3.6.1.4.1.8164.2.139	139	The identified card is a Single Point of Failure (SPOF). There is no redundant card available to take over in the event of a failure.	Card SPOF Alarm
starGPRSServiceStart	.1.3.6.1.4.1.8164.2.1060	.1.3.6.1.4.1.8164.2.1060	1060	A GPRS Service has started.	A GPRS Service has started
starGPRSServiceStop	.1.3.6.1.4.1.8164.2.1061	.1.3.6.1.4.1.8164.2.1061	1061	A GPRS Service has stopped.	A GPRS Service has stopped

Table 16-14 Cisco ASR 5000 Series V2 Traps (continued)

Trap Name	Trap OID	Subtype Varbind OID	Subtype Varbind Value	Description	Short Description
starStorageFailed	.1.3.6.1.4.1.8164.2.1076	.1.3.6.1.4.1.8164.2.1076	1076	The specified storage device has failed. This storage device is now out of service and cannot be used to store additional data.	Storage Failed
starOSPFv3NeighbourDown	.1.3.6.1.4.1.8164.2.1116	.1.3.6.1.4.1.8164.2.1116	1116	An OSPFv3 neighbor is down.	OSPF v3 Neighbour Down
starEGTPServiceStop	.1.3.6.1.4.1.8164.2.1086	.1.3.6.1.4.1.8164.2.1086	1086	An Evolved GPRS Tunneling Protocol (EGTP) Service has stopped.	An Evolved GPRS Tunneling Protocol (EGTP) Service has started
starSRPConnUp	.1.3.6.1.4.1.8164.2.1038	.1.3.6.1.4.1.8164.2.1038	1038	The connection to the standby SRP system is now up. This notification is only generated if a starSRPConnDown had previously been generated.	SRP Connection Up
starSRPConnDown	.1.3.6.1.4.1.8164.2.1037	.1.3.6.1.4.1.8164.2.1037	1037	The connection to the standby SRP system is down. While this connection is down, the active system is operating without a standby and would be unable to perform an SRP switchover.	SRP Connection Down
starkLicenseUnderLimit	.1.3.6.1.4.1.8164.2.94	.1.3.6.1.4.1.8164.2.94	94	Usage is now under the licensed session limit.	License UnderLimit
starFanInserted	.1.3.6.1.4.1.8164.2.24	.1.3.6.1.4.1.8164.2.24	24	A fan tray has been inserted	Fan Inserted
starFanFailed	.1.3.6.1.4.1.8164.2.22	.1.3.6.1.4.1.8164.2.22	22	One of more fans have failed on the indicated fan controller.	Fan Failed
starFanRemoved	.1.3.6.1.4.1.8164.2.23	.1.3.6.1.4.1.8164.2.23	23	A fan tray has been removed.	Fan Removed
starPortUp	.1.3.6.1.4.1.8164.2.1025	.1.3.6.1.4.1.8164.2.1025	1025	Port status is up. This notification is only generated for physical port and a 'starPortDown' notification was previously generated.	Port Up
starPortDown	.1.3.6.1.4.1.8164.2.1024	.1.3.6.1.4.1.8164.2.1024	1024	Port status is Down. This notification is only generated for physical port.	Port Down
starAlertsEnabled	.1.3.6.1.4.1.8164.2.38	.1.3.6.1.4.1.8164.2.38	38	The sending of SNMP Traps has been reenabled	Alerts Enabled

Table 16-14 Cisco ASR 5000 Series V2 Traps (continued)

Trap Name	Trap OID	Subtype Varbind OID	Subtype Varbind Value	Description	Short Description
starThreshDiameterRetryRate	.1.3.6.1.4.1.8164.2.482	.1.3.6.1.4.1.8164.2.482	482	The percentage of Diameter requests which has to be retried has exceeded the configured threshold during the current monitoring period.	The percentage of Diameter requests which has to be retried has exceeded the configured threshold
starAlertsDisabled	.1.3.6.1.4.1.8164.2.37	.1.3.6.1.4.1.8164.2.37	37	The sending of SNMP Traps has been disabled because too many alerts were generated within the defined window type.	Alerts Disabled
starasr5kLogMsg	.1.3.6.1.4.1.8164.2.45	.1.3.6.1.4.1.8164.2.45	45	A log message. This trap is used only for debugging.	Log Msg
starCardActive	.1.3.6.1.4.1.8164.2.55	.1.3.6.1.4.1.8164.2.55	55	The card is now active.	Card Active
starCardDown	.1.3.6.1.4.1.8164.2.60	.1.3.6.1.4.1.8164.2.60	60	The card is now down. generated when the card is restarted.	Card Up
starEgtpcPathFailure	.1.3.6.1.4.1.8164.2.1112	.1.3.6.1.4.1.8164.2.1112	1112	EGTP Control Path Failure. No response received for GTPV2 request sent from MME or SGW or PGW.	EGTP Control Path Failure
starMAGServiceStart	.1.3.6.1.4.1.8164.2.1089	.1.3.6.1.4.1.8164.2.1089	1089	A Mobile Access Gateway (MAG) Service has started.	A Mobile Access Gateway (MAG) Service has started
starCardPACMigrateStart	.1.3.6.1.4.1.8164.2.16	.1.3.6.1.4.1.8164.2.16	16	A PAC/PSC Migration operation has begun.	PAC Card Migration Started
starCardTempOverheat	.1.3.6.1.4.1.8164.2.1	.1.3.6.1.4.1.8164.2.1	1	The card has reached a temperature beyond its safe operating range	Card Temperature Over Heat
starCardTempOK	.1.3.6.1.4.1.8164.2.2	.1.3.6.1.4.1.8164.2.2	2	The temperature of the card is now within its safe operating range	Card Temperature OK
starCardUp	.1.3.6.1.4.1.8164.2.5	.1.3.6.1.4.1.8164.2.5	5	The card is up (operational)	Card Up
starCpuMemoryLowClear	.1.3.6.1.4.1.8164.2.1096	.1.3.6.1.4.1.8164.2.1096	1096	CPU Memory Low Clear	CPU Memory Low Clear
starCpuBusyClear	.1.3.6.1.4.1.8164.2.1095	.1.3.6.1.4.1.8164.2.1095	1095	CPU Busy Clear	CPU Busy Clear
starCritTaskFailed	.1.3.6.1.4.1.8164.2.54	.1.3.6.1.4.1.8164.2.54	54	A critical task has failed and the appropriate recovery steps begun	Critical Task Failed

Table 16-14 Cisco ASR 5000 Series V2 Traps (continued)

Trap Name	Trap OID	Subtype Varbind OID	Subtype Varbind Value	Description	Short Description
starCardBoot Failed	.1.3.6.1.4.1.8164 .2.9	.1.3.6.1.4.1.8164.2.9	9	A card has failed to startup properly. The card is not operational	Card Boot Failed
starCardSPCS witchoverFail ed	.1.3.6.1.4.1.8164 .2.21	.1.3.6.1.4.1.8164.2.21	21	An SPC switchover operation has failed.	SPC Card SwitchOver Failed
starCardSPCS witchoverCo mplete	.1.3.6.1.4.1.8164 .2.20	.1.3.6.1.4.1.8164.2.20	20	An SPC Switchover has completed successfully.	SPC Card Switchover Completed
starCardSPCS witchoverStar t	.1.3.6.1.4.1.8164 .2.19	.1.3.6.1.4.1.8164.2.19	19	An SPC switchover operation has begun.	SPC Card Switchover Started
starCardPAC MigrateFailed	.1.3.6.1.4.1.8164 .2.18	.1.3.6.1.4.1.8164.2.18	18	A PAC/PSC Migration operation has failed.	PAC Card Migration Failed
starCardPAC MigrateComp lete	.1.3.6.1.4.1.8164 .2.17	.1.3.6.1.4.1.8164.2.17	17	A PAC/PSC Migration operation has successfully completed	PAC Card Migration Completed
starCpuWatch DogExpired	.1.3.6.1.4.1.8164 .2.30	.1.3.6.1.4.1.8164.2.30	30	The watch dog timer has failed on this CPU	CPU WatchDog Expired
starCpuFailed	.1.3.6.1.4.1.8164 .2.29	.1.3.6.1.4.1.8164.2.29	29	The CPU has failed.	CPU Failed
starCpuMemo ryFailed	.1.3.6.1.4.1.8164 .2.28	.1.3.6.1.4.1.8164.2.28	28	The memory on this CPU has failed	CPU Memory Failed
starCpuMemo ryLow	.1.3.6.1.4.1.8164 .2.27	.1.3.6.1.4.1.8164.2.27	27	The CPU is experiencing a low memory condition.	CPU Memory Low
star5kCpuBus y	.1.3.6.1.4.1.8164 .2.26	.1.3.6.1.4.1.8164.2.26	26	The CPU is experiencing very high usage.	CPU Busy

Cisco Unified Computing System V2 Traps

Table 16-15 lists the Cisco Unified Computing System V2 traps supported in Prime Network. For associated event types, event subtypes, and Prime Network registry parameters, use the link in the Short Description column or see Table 16-29.

Table 16-15 Cisco Unified Computing System V2 Traps

Trap Name	Trap OID	Subtype Varbind OID	Subtype Varbind Value	Description	Short Description
fltEquipment PsuInoperable	1.3.6.1.4.1.9.9.719.0.1	1.3.6.1.4.1.9.9.719.1.1.1.9	374	This fault typically occurs when the Cisco UCS Manager detects a problem with a power supply unit in a chassis, fabric interconnect or a fex. For example, the PSU is not functional.	fltEquipmentPsuInoperable
fltEquipment PsuInoperable	1.3.6.1.4.1.9.9.719.0.2	1.3.6.1.4.1.9.9.719.1.1.1.9	374		fltEquipmentPsuInoperable-cleared
fltPortPIoFailed	1.3.6.1.4.1.9.9.719.0.1	1.3.6.1.4.1.9.9.719.1.1.1.9	277	This fault is raised on the fabric interconnect port, the server facing ports on the IOM or the FEX module when the system detects an indeterminate fault.	fltPortPIoFailed
fltPortPIoFailed	1.3.6.1.4.1.9.9.719.0.2	1.3.6.1.4.1.9.9.719.1.1.1.9	277		fltPortPIoFailed-cleared
fltPortPIoHardware-failure	1.3.6.1.4.1.9.9.719.0.1	1.3.6.1.4.1.9.9.719.1.1.1.9	278	This fault is raised on the fabric interconnect port, ports on the IOM or the FEX module when the system detects a hardware failure.	fltPortPIoHardware-failure
fltPortPIoHardware-failure	1.3.6.1.4.1.9.9.719.0.2	1.3.6.1.4.1.9.9.719.1.1.1.9	278		fltPortPIoHardware-failure-cleared
fltPortPIoInvalid-sfp	1.3.6.1.4.1.9.9.719.0.1	1.3.6.1.4.1.9.9.719.1.1.1.9	713	This fault is raised against a Fabric Interconnect port,network facing IOM port or a FEX module port if an unsupported transceiver type is inserted in it.The port cannot be used when it has an unsupported transceiver.	fltPortPIoInvalid-sfp
fltPortPIoInvalid-sfp	1.3.6.1.4.1.9.9.719.0.2	1.3.6.1.4.1.9.9.719.1.1.1.9	713		fltPortPIoInvalid-sfp-cleared
fltPortPIoLink-down	1.3.6.1.4.1.9.9.719.0.1	1.3.6.1.4.1.9.9.719.1.1.1.9	276		fltPortPIoLink-down

Table 16-15 Cisco Unified Computing System V2 Traps (continued)

Trap Name	Trap OID	Subtype Varbind OID	Subtype Varbind Value	Description	Short Description
fltPortPIoLink-down	1.3.6.1.4.1.9.9.719.0.2	1.3.6.1.4.1.9.9.719.1.1.1.9	276		fltPortPIoLink-down-cleared
fltPortPIoSfp-not-present	1.3.6.1.4.1.9.9.719.0.1	1.3.6.1.4.1.9.9.719.1.1.1.9	279	When a fabric interconnect port is not in an unconfigured state, an SFP is required for its operation. This fault is raised to indicate that the SFP is missing.	fltPortPIoSfp-not-present
fltPortPIoSfp-not-present	1.3.6.1.4.1.9.9.719.0.2	1.3.6.1.4.1.9.9.719.1.1.1.9	279		fltPortPIoSfp-not-present-cleared
fltEquipmentPsuIdentity	1.3.6.1.4.1.9.9.719.0.1	1.3.6.1.4.1.9.9.719.1.1.1.9	407	This fault typically occurs when a power supply unit has corrupted or has malformed FRU information.	fltEquipmentPsuIdentity
fltEquipmentPsuIdentity	1.3.6.1.4.1.9.9.719.0.2	1.3.6.1.4.1.9.9.719.1.1.1.9	407		fltEquipmentPsuIdentity-cleared
fltEquipmentPsuMissing	1.3.6.1.4.1.9.9.719.0.1	1.3.6.1.4.1.9.9.719.1.1.1.9	378	This fault typically occurs when the Cisco UCS Manager detects a problem with a power supply unit in a chassis, fabric interconnect or a fex. For example, the PSU is missing.	fltEquipmentPsuMissing
fltEquipmentPsuMissing	1.3.6.1.4.1.9.9.719.0.2	1.3.6.1.4.1.9.9.719.1.1.1.9	378		fltEquipmentPsuMissing-cleared
fltEquipmentPsuOffline	1.3.6.1.4.1.9.9.719.0.1	1.3.6.1.4.1.9.9.719.1.1.1.9	528	This fault typically occurs when Cisco UCS Manager detects that a power supply unit in a chassis, fabric interconnect or a fex is offline.	fltEquipmentPsuOffline
fltEquipmentPsuOffline	1.3.6.1.4.1.9.9.719.0.2	1.3.6.1.4.1.9.9.719.1.1.1.9	528		fltEquipmentPsuOffline-cleared
fltEquipmentPsuPerfThresholdCritical	1.3.6.1.4.1.9.9.719.0.1	1.3.6.1.4.1.9.9.719.1.1.1.9	393		fltEquipmentPsuPerfThresholdCritical
fltEquipmentPsuPerfThresholdCritical	1.3.6.1.4.1.9.9.719.0.2	1.3.6.1.4.1.9.9.719.1.1.1.9	393		fltEquipmentPsuPerfThresholdCritical-cleared
fltEquipmentPsuPerfThresholdNonCritical	1.3.6.1.4.1.9.9.719.0.1	1.3.6.1.4.1.9.9.719.1.1.1.9	392		fltEquipmentPsuPerfThresholdNonCritical

Table 16-15 Cisco Unified Computing System V2 Traps (continued)

Trap Name	Trap OID	Subtype Varbind OID	Subtype Varbind Value	Description	Short Description
fltEquipmentPsuPerfThresholdNonCritical	1.3.6.1.4.1.9.9.719.0.2	1.3.6.1.4.1.9.9.719.1.1.1.1.9	392		fltEquipmentPsuPerfThresholdNonCritical-cleared
fltEquipmentPsuPerfThresholdNonRecoverable	1.3.6.1.4.1.9.9.719.0.1	1.3.6.1.4.1.9.9.719.1.1.1.1.9	394		fltEquipmentPsuInoperable
fltEquipmentPsuPerfThresholdNonRecoverable	1.3.6.1.4.1.9.9.719.0.2	1.3.6.1.4.1.9.9.719.1.1.1.1.9	394		fltEquipmentPsuPerfThresholdNonRecoverable
fltEquipmentPsuPowerSupplyProblem	1.3.6.1.4.1.9.9.719.0.1	1.3.6.1.4.1.9.9.719.1.1.1.1.9	369	This fault typically occurs when the Cisco UCS Manager detects a problem with a power supply unit in a chassis, fabric interconnect or a fex. For example, the PSU is not functional.	fltEquipmentPsuPowerSupplyProblem
fltEquipmentPsuPowerSupplyProblem	1.3.6.1.4.1.9.9.719.0.2	1.3.6.1.4.1.9.9.719.1.1.1.1.9	369		fltEquipmentPsuPowerSupplyProblem-cleared
fltEquipmentPsuThermalThresholdCritical	1.3.6.1.4.1.9.9.719.0.1	1.3.6.1.4.1.9.9.719.1.1.1.1.9	383		fltEquipmentPsuThermalThresholdCritical
fltEquipmentPsuThermalThresholdCritical	1.3.6.1.4.1.9.9.719.0.2	1.3.6.1.4.1.9.9.719.1.1.1.1.9	383		fltEquipmentPsuThermalThresholdCritical-cleared
fltEquipmentPsuThermalThresholdNonCritical	1.3.6.1.4.1.9.9.719.0.1	1.3.6.1.4.1.9.9.719.1.1.1.1.9	381		fltEquipmentPsuThermalThresholdNonCritical
fltEquipmentPsuThermalThresholdNonCritical	1.3.6.1.4.1.9.9.719.0.2	1.3.6.1.4.1.9.9.719.1.1.1.1.9	381		fltEquipmentPsuThermalThresholdNonCritical-cleared
fltEquipmentPsuThermalThresholdNonRecoverable	1.3.6.1.4.1.9.9.719.0.1	1.3.6.1.4.1.9.9.719.1.1.1.1.9	385		fltEquipmentPsuThermalThresholdNonRecoverable

Table 16-15 Cisco Unified Computing System V2 Traps (continued)

Trap Name	Trap OID	Subtype Varbind OID	Subtype Varbind Value	Description	Short Description
fltEquipmentPsuThermalThresholdNonRecoverable	1.3.6.1.4.1.9.9.719.0.2	1.3.6.1.4.1.9.9.719.1.1.1.9	385		fltEquipmentPsuThermalThresholdNonRecoverable-cleared
fltEquipmentPsuVoltageThresholdCritical	1.3.6.1.4.1.9.9.719.0.1	1.3.6.1.4.1.9.9.719.1.1.1.9	389		fltEquipmentPsuVoltageThresholdCritical
fltEquipmentPsuVoltageThresholdCritical	1.3.6.1.4.1.9.9.719.0.2	1.3.6.1.4.1.9.9.719.1.1.1.9	389		fltEquipmentPsuVoltageThresholdCritical-cleared
fltEquipmentPsuVoltageThresholdNonCritical	1.3.6.1.4.1.9.9.719.0.1	1.3.6.1.4.1.9.9.719.1.1.1.9	387		fltEquipmentPsuVoltageThresholdNonCritical
fltEquipmentPsuVoltageThresholdNonCritical	1.3.6.1.4.1.9.9.719.0.2	1.3.6.1.4.1.9.9.719.1.1.1.9	387		fltEquipmentPsuVoltageThresholdNonCritical-cleared
fltEquipmentPsuVoltageThresholdNonRecoverable	1.3.6.1.4.1.9.9.719.0.1	1.3.6.1.4.1.9.9.719.1.1.1.9	391		fltEquipmentPsuVoltageThresholdNonRecoverable
fltEquipmentPsuVoltageThresholdNonRecoverable	1.3.6.1.4.1.9.9.719.0.2	1.3.6.1.4.1.9.9.719.1.1.1.9	391		fltEquipmentPsuVoltageThresholdNonRecoverable-cleared
fltEquipmentIOCardIdentity	1.3.6.1.4.1.9.9.719.0.1	1.3.6.1.4.1.9.9.719.1.1.1.9	405		fltEquipmentIOCardIdentity
fltEquipmentIOCardIdentity	1.3.6.1.4.1.9.9.719.0.2	1.3.6.1.4.1.9.9.719.1.1.1.9	405		fltEquipmentIOCardIdentity-cleared
fltEquipmentIOCardInaccessible	1.3.6.1.4.1.9.9.719.0.1	1.3.6.1.4.1.9.9.719.1.1.1.9	478		fltEquipmentIOCardInaccessible
fltEquipmentIOCardInaccessible	1.3.6.1.4.1.9.9.719.0.2	1.3.6.1.4.1.9.9.719.1.1.1.9	478		fltEquipmentIOCardInaccessible-cleared
fltEquipmentIOCardPeerDisconnected	1.3.6.1.4.1.9.9.719.0.1	1.3.6.1.4.1.9.9.719.1.1.1.9	403		fltEquipmentIOCardPeerDisconnected

Table 16-15 Cisco Unified Computing System V2 Traps (continued)

Trap Name	Trap OID	Subtype Varbind OID	Subtype Varbind Value	Description	Short Description
fltEquipmentIOCardPeerDisconnected	1.3.6.1.4.1.9.9.719.0.2	1.3.6.1.4.1.9.9.719.1.1.1.9	403		fltEquipmentIOCardPeerDisconnected-cleared
fltEquipmentIOCardPost-failure	1.3.6.1.4.1.9.9.719.0.1	1.3.6.1.4.1.9.9.719.1.1.1.9	481		fltEquipmentIOCardPost-failure
fltEquipmentIOCardPost-failure	1.3.6.1.4.1.9.9.719.0.2	1.3.6.1.4.1.9.9.719.1.1.1.9	481		fltEquipmentIOCardPost-failure-cleared
fltEquipmentIOCardRemoved	1.3.6.1.4.1.9.9.719.0.1	1.3.6.1.4.1.9.9.719.1.1.1.9	376		fltEquipmentIOCardRemoved
fltEquipmentIOCardRemoved	1.3.6.1.4.1.9.9.719.0.2	1.3.6.1.4.1.9.9.719.1.1.1.9	376		fltEquipmentIOCardRemoved-cleared
fltEquipmentIOCardThermalProblem	1.3.6.1.4.1.9.9.719.0.1	1.3.6.1.4.1.9.9.719.1.1.1.9	379		fltEquipmentIOCardThermalProblem
fltEquipmentIOCardThermalProblem	1.3.6.1.4.1.9.9.719.0.2	1.3.6.1.4.1.9.9.719.1.1.1.9	379		fltEquipmentIOCardThermalProblem-cleared
fltEquipmentIOCardThermalThresholdCritical	1.3.6.1.4.1.9.9.719.0.1	1.3.6.1.4.1.9.9.719.1.1.1.9	730		fltEquipmentIOCardThermalThresholdCritical
fltEquipmentIOCardThermalThresholdCritical	1.3.6.1.4.1.9.9.719.0.2	1.3.6.1.4.1.9.9.719.1.1.1.9	730		fltEquipmentIOCardThermalThresholdCritical-cleared
fltEquipmentIOCardThermalThresholdNonCritical	1.3.6.1.4.1.9.9.719.0.1	1.3.6.1.4.1.9.9.719.1.1.1.9	729		fltEquipmentIOCardThermalThresholdNonCritical
fltEquipmentIOCardThermalThresholdNonCritical	1.3.6.1.4.1.9.9.719.0.2	1.3.6.1.4.1.9.9.719.1.1.1.9	729		fltEquipmentIOCardThermalThresholdNonCritical-cleared
fltEquipmentIOCardThermalThresholdNonRecoverable	1.3.6.1.4.1.9.9.719.0.1	1.3.6.1.4.1.9.9.719.1.1.1.9	731		fltEquipmentIOCardThermalThresholdNonRecoverable

Table 16-15 Cisco Unified Computing System V2 Traps (continued)

Trap Name	Trap OID	Subtype Varbind OID	Subtype Varbind Value	Description	Short Description
fltEquipmentIOCardThermalThresholdNonRecoverable	1.3.6.1.4.1.9.9.719.1.19.0.2	1.3.6.1.4.1.9.9.719.1.1.1.1.9	731		fltEquipmentIOCardThermalThresholdNonRecoverable-cleared
fltEquipmentIOCardUnsupportedConnectivity	1.3.6.1.4.1.9.9.719.1.19.0.1	1.3.6.1.4.1.9.9.719.1.1.1.1.9	401		fltEquipmentIOCardUnsupportedConnectivity
fltEquipmentIOCardUnsupportedConnectivity	1.3.6.1.4.1.9.9.719.1.19.0.2	1.3.6.1.4.1.9.9.719.1.1.1.1.9	401		fltEquipmentIOCardUnsupportedConnectivity-cleared
fltEquipmentFanDegraded	1.3.6.1.4.1.9.9.719.1.19.0.1	1.3.6.1.4.1.9.9.719.1.1.1.1.9	371		fltEquipmentFanDegraded
fltEquipmentFanDegraded	1.3.6.1.4.1.9.9.719.1.19.0.2	1.3.6.1.4.1.9.9.719.1.1.1.1.9	371		fltEquipmentFanDegraded-cleared
fltEquipmentFanInoperable	1.3.6.1.4.1.9.9.719.1.19.0.1	1.3.6.1.4.1.9.9.719.1.1.1.1.9	373		fltEquipmentFanInoperable
fltEquipmentFanInoperable	1.3.6.1.4.1.9.9.719.1.19.0.2	1.3.6.1.4.1.9.9.719.1.1.1.1.9	373		fltEquipmentFanInoperable-cleared
fltEquipmentFanMissing	1.3.6.1.4.1.9.9.719.1.19.0.1	1.3.6.1.4.1.9.9.719.1.1.1.1.9	434		fltEquipmentFanMissing
fltEquipmentFanMissing	1.3.6.1.4.1.9.9.719.1.19.0.2	1.3.6.1.4.1.9.9.719.1.1.1.1.9	434		fltEquipmentFanMissing-cleared
fltEquipmentFanModuleDegraded	1.3.6.1.4.1.9.9.719.1.19.0.1	1.3.6.1.4.1.9.9.719.1.1.1.1.9	480		fltEquipmentFanModuleDegradedd
fltEquipmentFanModuleDegraded	1.3.6.1.4.1.9.9.719.1.19.0.2	1.3.6.1.4.1.9.9.719.1.1.1.1.9	480		fltEquipmentFanModuleDegraded-cleared
fltEquipmentFanModuleIdentity	1.3.6.1.4.1.9.9.719.1.19.0.1	1.3.6.1.4.1.9.9.719.1.1.1.1.9	406	This fault typically occurs when fan module has corrupted or has malformed FRU information.	fltEquipmentFanModuleIdentity
fltEquipmentFanModuleIdentity	1.3.6.1.4.1.9.9.719.1.19.0.2	1.3.6.1.4.1.9.9.719.1.1.1.1.9	406		fltEquipmentFanModuleIdentity-cleared
fltEquipmentFanModuleInoperable	1.3.6.1.4.1.9.9.719.1.19.0.1	1.3.6.1.4.1.9.9.719.1.1.1.1.9	794		fltEquipmentFanModuleInoperable

Table 16-15 Cisco Unified Computing System V2 Traps (continued)

Trap Name	Trap OID	Subtype Varbind OID	Subtype Varbind Value	Description	Short Description
fltEquipmentFanModuleInoperable	1.3.6.1.4.1.9.9.719.0.2	1.3.6.1.4.1.9.9.719.1.1.1.9	794		fltEquipmentFanModuleInoperable-cleared
fltEquipmentFanModuleMissing	1.3.6.1.4.1.9.9.719.0.1	1.3.6.1.4.1.9.9.719.1.1.1.9	377		fltEquipmentFanModuleMissing
fltEquipmentFanModuleMissing	1.3.6.1.4.1.9.9.719.0.2	1.3.6.1.4.1.9.9.719.1.1.1.9	377		fltEquipmentFanModuleMissing-cleared
fltEquipmentFanModuleThermalThresholdCritical	1.3.6.1.4.1.9.9.719.0.1	1.3.6.1.4.1.9.9.719.1.1.1.9	382		fltEquipmentFanModuleThermalThresholdCritical
fltEquipmentFanModuleThermalThresholdCritical	1.3.6.1.4.1.9.9.719.0.2	1.3.6.1.4.1.9.9.719.1.1.1.9	382		fltEquipmentFanModuleThermalThresholdCritical-cleared
fltEquipmentFanModuleThermalThresholdNonCritical	1.3.6.1.4.1.9.9.719.0.1	1.3.6.1.4.1.9.9.719.1.1.1.9	380		fltEquipmentFanModuleThermalThresholdNonCritical
fltEquipmentFanModuleThermalThresholdNonCritical	1.3.6.1.4.1.9.9.719.0.2	1.3.6.1.4.1.9.9.719.1.1.1.9	380		fltEquipmentFanModuleThermalThresholdNonCritical-cleared
fltEquipmentFanModuleThermalThresholdNonRecoverable	1.3.6.1.4.1.9.9.719.0.1	1.3.6.1.4.1.9.9.719.1.1.1.9	384		fltEquipmentFanModuleThermalThresholdNonRecoverable
fltEquipmentFanModuleThermalThresholdNonRecoverable	1.3.6.1.4.1.9.9.719.0.2	1.3.6.1.4.1.9.9.719.1.1.1.9	384		fltEquipmentFanModuleThermalThresholdNonRecoverable-cleared
fltEquipmentFanPerfThresholdCritical	1.3.6.1.4.1.9.9.719.0.1	1.3.6.1.4.1.9.9.719.1.1.1.9	396		fltEquipmentFanPerfThresholdCritical
fltEquipmentFanPerfThresholdCritical	1.3.6.1.4.1.9.9.719.0.2	1.3.6.1.4.1.9.9.719.1.1.1.9	396		fltEquipmentFanPerfThresholdCritical-cleared

Table 16-15 Cisco Unified Computing System V2 Traps (continued)

Trap Name	Trap OID	Subtype Varbind OID	Subtype Varbind Value	Description	Short Description
fltEquipmentFanPerfThresholdLowerNonRecoverable	1.3.6.1.4.1.9.9.719.1.19.0.1	1.3.6.1.4.1.9.9.719.1.1.1.1.9	484		fltEquipmentFanPerfThresholdLowerNonRecoverable
fltEquipmentFanPerfThresholdLowerNonRecoverable	1.3.6.1.4.1.9.9.719.1.19.0.2	1.3.6.1.4.1.9.9.719.1.1.1.1.9	484		fltEquipmentFanPerfThresholdLowerNonRecoverable-cleared
fltEquipmentFanPerfThresholdNonCritical	1.3.6.1.4.1.9.9.719.1.19.0.1	1.3.6.1.4.1.9.9.719.1.1.1.1.9	277		fltEquipmentFanPerfThresholdNonCritical
fltEquipmentFanPerfThresholdNonCritical	1.3.6.1.4.1.9.9.719.1.19.0.2	1.3.6.1.4.1.9.9.719.1.1.1.1.9	277		fltEquipmentFanPerfThresholdNonCritical-cleared
fltEquipmentFanPerfThresholdNonRecoverable	1.3.6.1.4.1.9.9.719.1.19.0.1	1.3.6.1.4.1.9.9.719.1.1.1.1.9	397		fltEquipmentFanPerfThresholdNonRecoverable
fltEquipmentFanPerfThresholdNonRecoverable	1.3.6.1.4.1.9.9.719.1.19.0.2	1.3.6.1.4.1.9.9.719.1.1.1.1.9	397		fltEquipmentFanPerfThresholdNonRecoverable-cleared
fltExtmgmtIfMgmtifdown	1.3.6.1.4.1.9.9.719.1.19.0.1	1.3.6.1.4.1.9.9.719.1.1.1.1.9	736	External management interface on fabric interconnect is operationally down.The Cisco UCS Manager raises this fault when any of the following scenario occur: •Endpoint(switch/fabric interconnect) reports that operational state of external management interface is down.	fltExtmgmtIfMgmtifdown
fltExtmgmtIfMgmtifdown	1.3.6.1.4.1.9.9.719.1.19.0.2	1.3.6.1.4.1.9.9.719.1.1.1.1.9	736		fltExtmgmtIfMgmtifdown-cleared
fltMgmtEntityDegraded	1.3.6.1.4.1.9.9.719.1.19.0.1	1.3.6.1.4.1.9.9.719.1.1.1.1.9	293		fltMgmtEntityDegraded
fltMgmtEntityDegraded	1.3.6.1.4.1.9.9.719.1.19.0.2	1.3.6.1.4.1.9.9.719.1.1.1.1.9	293		fltMgmtEntityDegraded-cleared
fltMgmtEntityDown	1.3.6.1.4.1.9.9.719.1.19.0.1	1.3.6.1.4.1.9.9.719.1.1.1.1.9	294		fltMgmtEntityDown

Table 16-15 Cisco Unified Computing System V2 Traps (continued)

Trap Name	Trap OID	Subtype Varbind OID	Subtype Varbind Value	Description	Short Description
fltMgmtEntityDown	1.3.6.1.4.1.9.9.719.0.2	1.3.6.1.4.1.9.9.719.1.1.1.9	294		fltMgmtEntityDown-cleared
fltMgmtEntityElection-failure	1.3.6.1.4.1.9.9.719.0.1	1.3.6.1.4.1.9.9.719.1.1.1.9	428		fltMgmtEntityElection-failure
fltMgmtEntityElection-failure	1.3.6.1.4.1.9.9.719.0.2	1.3.6.1.4.1.9.9.719.1.1.1.9	428		fltMgmtEntityElection-failure-cleared
fltMgmtEntityVersion-incompatible	1.3.6.1.4.1.9.9.719.0.1	1.3.6.1.4.1.9.9.719.1.1.1.9	430		fltMgmtEntityVersion-incompatible
fltMgmtEntityVersion-incompatible	1.3.6.1.4.1.9.9.719.0.2	1.3.6.1.4.1.9.9.719.1.1.1.9	430		fltMgmtEntityVersion-incompatible-cleared
fltNetworkElementInoperable	1.3.6.1.4.1.9.9.719.0.1	1.3.6.1.4.1.9.9.719.1.1.1.9	291		fltNetworkElementInoperable
fltNetworkElementInoperable	1.3.6.1.4.1.9.9.719.0.2	1.3.6.1.4.1.9.9.719.1.1.1.9	291		fltNetworkElementInoperable-cleared
fltStorageItemCapacityExceeded	1.3.6.1.4.1.9.9.719.0.1	1.3.6.1.4.1.9.9.719.1.1.1.9	182		fltStorageItemCapacityExceeded
fltStorageItemCapacityExceeded	1.3.6.1.4.1.9.9.719.0.2	1.3.6.1.4.1.9.9.719.1.1.1.9	182		fltStorageItemCapacityExceeded-cleared
fltStorageItemCapacityWarning	1.3.6.1.4.1.9.9.719.0.1	1.3.6.1.4.1.9.9.719.1.1.1.9	183		fltStorageItemCapacityWarning
fltStorageItemCapacityWarning	1.3.6.1.4.1.9.9.719.0.2	1.3.6.1.4.1.9.9.719.1.1.1.9	183		fltStorageItemCapacityWarning-cleared
fltEquipmentFexIdentity	1.3.6.1.4.1.9.9.719.0.1	1.3.6.1.4.1.9.9.719.1.1.1.9	703	This fault typically occurs when an fex has corrupted or has malformed FRU information.	fltEquipmentFexIdentity
fltEquipmentFexIdentity	1.3.6.1.4.1.9.9.719.0.2	1.3.6.1.4.1.9.9.719.1.1.1.9	703		fltEquipmentFexIdentity-cleared
fltEquipmentFexIdentity-unestablishable	1.3.6.1.4.1.9.9.719.0.2	1.3.6.1.4.1.9.9.719.1.1.1.9	778		fltEquipmentFexIdentity-unestablishable

Table 16-15 Cisco Unified Computing System V2 Traps (continued)

Trap Name	Trap OID	Subtype Varbind OID	Subtype Varbind Value	Description	Short Description
fltEquipmentChassisIdentity	1.3.6.1.4.1.9.9.719.1.1.1.9.0.1	1.3.6.1.4.1.9.9.719.1.1.1.9	404	This fault typically occurs when an I/O module has corrupted or has malformed FRU information.	fltEquipmentChassisIdentity
fltEquipmentChassisIdentity	1.3.6.1.4.1.9.9.719.1.1.1.9.0.2	1.3.6.1.4.1.9.9.719.1.1.1.9	404		fltEquipmentChassisIdentity-cleared
fltEquipmentChassisIdentity-unestablishable	1.3.6.1.4.1.9.9.719.1.1.1.9.0.1	1.3.6.1.4.1.9.9.719.1.1.1.9	543	This fault typically occurs because the Cisco UCS Manager has detected an unsupported chassis. For example, the model, vendor, or revision is not recognized.	fltEquipmentChassisIdentity-unestablishable
fltEquipmentChassisIdentity-unestablishable	1.3.6.1.4.1.9.9.719.1.1.1.9.0.2	1.3.6.1.4.1.9.9.719.1.1.1.9	543		fltEquipmentChassisIdentity-unestablishable-cleared
fltEquipmentChassisInoperable	1.3.6.1.4.1.9.9.719.1.1.1.9.0.1	1.3.6.1.4.1.9.9.719.1.1.1.9	456	This fault typically occurs for one of the following reasons: •The fabric interconnect cannot communicate with a chassis. For a cluster configuration, this fault means that neither fabric interconnect can communicate with the chassis. •The chassis has an invalid FRU.	fltEquipmentChassisInoperable
fltEquipmentChassisInoperable	1.3.6.1.4.1.9.9.719.1.1.1.9.0.2	1.3.6.1.4.1.9.9.719.1.1.1.9	456		fltEquipmentChassisInoperable-cleared
fltEquipmentChassisPowerProblem	1.3.6.1.4.1.9.9.719.1.1.1.9.0.1	1.3.6.1.4.1.9.9.719.1.1.1.9	408	This fault typically occurs when the chassis fails to meet the minimal power requirements defined in the power policy or when one or more power supplies have failed.	fltEquipmentChassisPowerProblem
fltEquipmentChassisPowerProblem	1.3.6.1.4.1.9.9.719.1.1.1.9.0.2	1.3.6.1.4.1.9.9.719.1.1.1.9	408		fltEquipmentChassisPowerProblem-cleared

Table 16-15 Cisco Unified Computing System V2 Traps (continued)

Trap Name	Trap OID	Subtype Varbind OID	Subtype Varbind Value	Description	Short Description
fltEquipmentChassisThermalThresholdCritical	1.3.6.1.4.1.9.9.719.0.1	1.3.6.1.4.1.9.9.719.1.1.1.9	409		fltEquipmentChassisThermalThresholdCritical
fltEquipmentChassisThermalThresholdCritical	1.3.6.1.4.1.9.9.719.0.2	1.3.6.1.4.1.9.9.719.1.1.1.9	409		fltEquipmentChassisThermalThresholdCritical-cleared
fltEquipmentChassisThermalThresholdNonCritical	1.3.6.1.4.1.9.9.719.0.1	1.3.6.1.4.1.9.9.719.1.1.1.9	410		fltEquipmentChassisThermalThresholdNonCritical
fltEquipmentChassisThermalThresholdNonCritical	1.3.6.1.4.1.9.9.719.0.2	1.3.6.1.4.1.9.9.719.1.1.1.9	410		fltEquipmentChassisThermalThresholdNonCritical-cleared
fltEquipmentChassisThermalThresholdNonRecoverable	1.3.6.1.4.1.9.9.719.0.1	1.3.6.1.4.1.9.9.719.1.1.1.9	411		fltEquipmentChassisThermalThresholdNonRecoverable
fltEquipmentChassisThermalThresholdNonRecoverable	1.3.6.1.4.1.9.9.719.0.2	1.3.6.1.4.1.9.9.719.1.1.1.9	411		fltEquipmentChassisThermalThresholdNonRecoverable-cleared
fltEquipmentChassisUnacknowledged	1.3.6.1.4.1.9.9.719.0.1	1.3.6.1.4.1.9.9.719.1.1.1.9	400	This fault typically occurs when or more of the I/O module links from the chassis are unacknowledged.	fltEquipmentChassisUnacknowledged
fltEquipmentChassisUnacknowledged	1.3.6.1.4.1.9.9.719.0.2	1.3.6.1.4.1.9.9.719.1.1.1.9	400		fltEquipmentChassisUnacknowledged-cleared
fltEquipmentChassisUnsupportedConnectivity	1.3.6.1.4.1.9.9.719.0.1	1.3.6.1.4.1.9.9.719.1.1.1.9	399	This fault typically occurs when the current connectivity for a chassis does not match the configuration in the chassis discovery policy.	fltEquipmentChassisUnsupportedConnectivity
fltEquipmentChassisUnsupportedConnectivity	1.3.6.1.4.1.9.9.719.0.2	1.3.6.1.4.1.9.9.719.1.1.1.9	399		fltEquipmentChassisUnsupportedConnectivity-cleared

Table 16-15 Cisco Unified Computing System V2 Traps (continued)

Trap Name	Trap OID	Subtype Varbind OID	Subtype Varbind Value	Description	Short Description
fltFabricComputeSlotEpMisplacedInChassisSlot	1.3.6.1.4.1.9.9.719.1.1.1.9	1.3.6.1.4.1.9.9.719.1.1.1.9	156	This fault typically occurs when the Cisco UCS Manager detects a server in a chassis slot that does not match what was previously equipped in the slot.	fltFabricComputeSlotEpMisplacedInChassisSlot
fltFabricComputeSlotEpMisplacedInChassisSlot	1.3.6.1.4.1.9.9.719.0.2	1.3.6.1.4.1.9.9.719.1.1.1.9	156		fltFabricComputeSlotEpMisplacedInChassisSlot-cleared
fltFabricComputeSlotEpServerIdentificationProblem	1.3.6.1.4.1.9.9.719.0.1	1.3.6.1.4.1.9.9.719.1.1.1.9	157	This fault typically occurs when the Cisco UCS Manager encountered a problem identifying the server in a chassis slot.	fltFabricComputeSlotEpServerIdentificationProblem
fltFabricComputeSlotEpServerIdentificationProblem	1.3.6.1.4.1.9.9.719.0.2	1.3.6.1.4.1.9.9.719.1.1.1.9	157		fltFabricComputeSlotEpServerIdentificationProblem-cleared

Cisco ASR 1000 V2 Traps

Table 16-16 lists the Cisco ASR 1000 V2 traps supported in Prime Network. For associated event types, event subtypes, and Prime Network registry parameters, use the link in the Short Description column or see Table 16-32.

Table 16-16 Cisco ASR 1000 V2 Traps

Trap Name	Trap OID	Subtype Varbind OID	Subtype Varbind Value	Description	Short Description
cikeTunnelStart	1.3.6.1.4.1.9.9.171.2.0.1	N/A	N/A	cisco IPSec tunnel state change trap	IPsec Phase-1 IKE Tunnel active trap
cikeTunnelStop	1.3.6.1.4.1.9.9.171.2.0.2	N/A	N/A	cisco IPSec tunnel state change trap	IPsec Phase-1 IKE Tunnel inactive trap

Cisco ASR 9000 V1 Trap Registry Parameters

Table 16-17 lists the associated event types, event subtypes, and Prime Network registry parameters for the ASR 9000 SNMP V1 traps shown in Table 16-1.

Table 16-17 Cisco ASR 9000 V1 Trap Registry Parameters

Short Description	Event Type	Event Subtype	Expedites Polling	Event Source (IMO Name)	Activate Flow	Correlate	Is Correlation Allowed	Weight	Auto Clear	Severity	Is Ticketable	Auto Remove	Flapping
dot1ag CFM Fault Alarm	dot1ag cfm fault alarm trap	dot1ag cfm fault alarm trap	N	ICFMService	F	F	F	0	F	info	T	T	F
dot1ag CFM Fault Alarm	dot1ag cfm fault alarm trap	dot1ag cfm fault alarm restore trap	N	ICFMService	F	F	F	0	F	clr	F	T	F

Cisco ASR 9000 V2/V3 Registry Parameters

Table 16-18 lists the associated event types, event subtypes, and Prime Network registry parameters for the Cisco ASR 9000 SNMP V2/V3 traps shown in Table 16-2.

Table 16-18 Cisco ASR 9000 V2/V3 Trap Registry Parameters

Short Description	Event Type	Event Subtype	Expedites Polling	Event Source (IMO Name)	Activate Flow	Correlate	Is Correlation Allowed	Weight	Auto Clear	Severity	Is Ticketable	Auto Remove	Flapping
NTP Server Status Changes to Unknown	cisco ntp server notification	unknown	N	IManaged Element	F	F	F	0	F	info	F	T	F
NTP Server Status Changes to notRunning	cisco ntp server notification	notRunning	N	IManaged Element	F	F	F	0	F	info	F	T	F
NTP Server Status Changes to notSynchronized	cisco ntp server notification	notSynchronized	N	IManaged Element	F	F	F	0	F	info	F	T	F
NTP Server Status Changes to syncToLocal	cisco ntp server notification	syncToLocal	N	IManaged Element	F	F	F	0	F	info	F	T	F
NTP Server Status Changes to syncToRefclock	cisco ntp server notification	syncToRefclock	N	IManaged Element	F	F	F	0	F	info	F	T	F
NTP Server Status Changes to syncToRemoteServer	cisco ntp server notification	syncToRemoteServer	N	IManaged Element	F	F	F	0	F	info	F	T	F
Spanning Tree Topology Changed	Spanning-Tree-Topology-Change-Trap	Spanning-Tree-Topology-Change	N	IManaged Element	F	F	F	0	F	info	F	T	F
Warm start trap	warm start trap	warm start trap	N	IManaged Element	F	F	F	0	F	min	T	T	F

Table 16-18 Cisco ASR 9000 V2/V3 Trap Registry Parameters (continued)

Short Description	Event Type	Event Subtype	Expedites Polling	Event Source (IMO Name)	Activate Flow	Correlate	Is Correlation Allowed	Weight	Auto Clear	Severity	Is Ticketable	Auto Remove	Flapping
dot1ag CFM Fault Alarm	dot1ag cfm fault alarm trap	dot1ag cfm fault alarm trap	N	ICFMService	F	F	F	0	F	info	T	T	F
dot1ag CFM Fault Alarm	dot1ag cfm fault alarm trap	dot1ag cfm fault alarm restore trap	N	ICFMService	F	F	F	0	F	clr	F	T	F

Cisco IOS V1 Trap Registry Parameters

Table 16-19 lists the associated event types, event subtypes, and Prime Network registry parameters for the Cisco IOS SNMP V1 traps shown in Table 16-3.

Table 16-19 Cisco IOS V1 Trap Registry Parameters

Short Description	Event Type	Event Subtype	Expedites Polling	Event Source (IMO Name)	Activate Flow	Correlate	Is Correlation Allowed	Weight	Auto Clear	Severity	Is Ticketable	Auto Remove	Flapping
Critical Temprature	cisco-Environment-Monitoring-Temperature-Notification	critical	N	IManaged Element	F	F	F	0	T	cri	F	T	F
Normal Temprature	cisco-Environment-Monitoring-Temperature-Notification	normal	N	IManaged Element	F	F	F	0	F	clr	F	T	F
Not Functioning	cisco-Environment-Monitoring-Temperature-Notification	notFunctioning	N	IManaged Element	F	F	F	0	T	maj	F	T	F
Not Present	cisco-Environment-Monitoring-Temperature-Notification	notPresent	N	IManaged Element	F	F	F	0	T	maj	F	T	F
Critical Temprature - Device Shutdown	cisco-Environment-Monitoring-Temperature-Notification	shutdown	N	IManaged Element	F	F	F	0	T	cri	F	T	F
Temprature Rising	cisco-Environment-Monitoring-Temperature-Notification	warning	N	IManaged Element	F	F	F	0	T	wrn	F	T	F

Table 16-19 Cisco IOS V1 Trap Registry Parameters (continued)

Short Description	Event Type	Event Subtype	Expedites Polling	Event Source (IMO Name)	Activate Flow	Correlate	Is Correlation Allowed	Weight	Auto Clear	Severity	Is Ticketable	Auto Remove	Flapping
Power Supply - Critical	cisco-EnvMon-Supply-State-Notification-Trap	critical	N	IManaged Element	F	F	F	0	F	cri	T	T	F
Power Supply - Normal	cisco-EnvMon-Supply-State-Notification-Trap	normal	N	IManaged Element	F	F	F	0	F	clr	T	T	F
Power Supply - Not Functioning	cisco-EnvMon-Supply-State-Notification-Trap	notFunctioning	N	IManaged Element	F	F	F	0	F	maj	T	T	F
Power Supply - Not Present	cisco-EnvMon-Supply-State-Notification-Trap	notPresent	N	IManaged Element	T	F	F	0	F	maj	T	T	F
Power Supply - Shutdown	cisco-EnvMon-Supply-State-Notification-Trap	shutdown	N	IManaged Element	F	F	F	0	F	cri	T	T	F
Power Supply - Warning	cisco-EnvMon-Supply-State-Notification-Trap	warning	N	IManaged Element	F	F	F	0	F	wrn	T	T	F
Fan down trap	fan down trap	fan down trap	N	IManaged Element	F	T	F	0	T	maj	F	T	F
Fan up trap	fan down trap	fan up trap	N	IManaged Element	F	F	F	0	F	clr	F	T	F
RTT Operation Timeout	RTT Operation Timeout	RTT Operation Timeout	N	IManaged Element	F	F	F	0	F	info	T	T	F
RTT Operation Threshold Violation	RTT Operation Threshold Violation	RTT Operation Threshold Violation	N	IManaged Element	F	F	F	0	F	info	T	T	F
dot1qBridge trap	dot1qBridge trap	dot1qBridge trap	N	IManaged Element	F	T	F	0	F	info	F	T	F
Mep up trap	mep trap	mep up	N	IManaged Element	F	F	F	0	F	clr	F	T	F
Mep down trap	mep trap	mep down	N	IManaged Element	F	F	F	0	T	maj	F	T	F
Cold start trap	cold start trap	cold start trap	N	IManaged Element	F	F	T	190000	F	info	T	T	F

Table 16-19 Cisco IOS V1 Trap Registry Parameters (continued)

Short Description	Event Type	Event Subtype	Expedites Polling	Event Source (IMO Name)	Activate Flow	Correlate	Is Correlation Allowed	Weight	Auto Clear	Severity	Is Ticketable	Auto Remove	Flapping
SNMP Link down	snmp link down	snmp link down	ce-efp-status-telnet/mtop-mlpp pbundle-status-telnet/mtop-ima-group-state-telnet/mtop-cem-group-status/bundle-status/mpls traffic engineering tunnel information/basetech-lldp-neighbors-snmp/basetech-cdp-neighbors-snmp/port-status/ip interface oper status	IPhysical Layer	F	T	F	0	T	min	F	T	T

Table 16-19 Cisco IOS V1 Trap Registry Parameters (continued)

Short Description	Event Type	Event Subtype	Expedites Polling	Event Source (IMO Name)	Activate Flow	Correlate	Is Correlation Allowed	Weight	Auto Clear	Severity	Is Ticketable	Auto Remove	Flapping
SNMP Link up	snmp link down	snmp link up	ce-efp-status-telnet/mtop-mlpppbundle-status-telnet/mtop-ima-group-state-telnet/mtop-cem-group-status/bundle-status/mpls traffic engineering tunnel information/basetech-lldp-neighbors-snmp/basetech-cdp-neighbors-snmp/port-status/ip interface oper status	IPhysical Layer	F	T	F	0	F	clr	F	T	T
IMA Group Remote Failure	IMA Group Failure trap	IMA Group Remote Failure	mtop-ima-group-state,port-status	ImaGroup Oid	F	F	F	0	T	MINOR	F	T	T
IMA Group Remote insufficient links trap	IMA Group Failure trap	IMA Group Remote insufficient links trap	mtop-ima-group-state,port-status	ImaGroup Oid	F	F	F	0	T	MAJOR	F	T	T

Table 16-19 Cisco IOS V1 Trap Registry Parameters (continued)

Short Description	Event Type	Event Subtype	Expedites Polling	Event Source (IMO Name)	Activate Flow	Correlate	Is Correlation Allowed	Weight	Auto Clear	Severity	Is Ticketable	Auto Remove	Flapping
IMA Group Up Trap	IMA Group Failure trap	IMA Group Up Trap	mtop-ima-group-state,port-status	ImaGroup Oid	F	F	F	0	F	CLEARED	F	T	T
IMA Group local Failure	IMA Group Failure trap	IMA Group local Failure	mtop-ima-group-state,port-status	ImaGroup Oid	F	F	F	0	T	MINOR	F	T	T
IMA Group local insufficient links trap	IMA Group Failure trap	IMA Group local insufficient links trap	mtop-ima-group-state,port-status	ImaGroup Oid	F	F	F	0	T	MAJOR	F	T	T
Ima Link Loss of delay Frame Trap	IMA Link Failure trap	Ima Link Loss of delay Frame Trap	mtop-ima-group-state,port-status	ImaGroup Oid	F	F	F	0	T	MINOR	F	T	T
Ima Link Loss of ima Frame Trap	IMA Link Failure trap	Ima Link Loss of ima Frame Trap	mtop-ima-group-state,port-status	ImaGroup Oid	F	T	F	0	T	MINOR	F	T	T
Ima Link Rcv Failure Trap	IMA Link Failure trap	Ima Link Rcv Failure Trap	mtop-ima-group-state,port-status	ImaGroup Oid	F	T	F	0	T	MINOR	F	T	T
Ima Link Remote Failure Trap	IMA Link Failure trap	Ima Link Remote Failure Trap	mtop-ima-group-state,port-status	ImaGroup Oid	F	T	F	0	T	MINOR	F	T	T
Ima Link Up Trap	IMA Link Failure trap	Ima Link Up Trap	mtop-ima-group-state,port-status	ImaGroup Oid	F	F	F	0	F	CLEARED	F	T	T

Table 16-19 Cisco IOS V1 Trap Registry Parameters (continued)

Short Description	Event Type	Event Subtype	Expedites Polling	Event Source (IMO Name)	Activate Flow	Correlate	Is Correlation Allowed	Weight	Auto Clear	Severity	Is Ticketable	Auto Remove	Flapping
Ima Link Xmt Failure Trap	IMA Link Failure trap	Ima Link Xmt Failure Trap	mtop-ima-group-state,port-status	ImaGroupOid	F	T	F	0	T	MINOR	F	T	T
Cisco UMT state Change trap	Cisco UMT state Change trap	Cisco UMT state Change trap	N/A	PortLayer1Oid	F	F	F	0	F	info	F	T	F
Cisco GSM state Change trap	Cisco GSM state Change trap	Cisco GSM state Change trap	N/A	PortLayer1Oid	F	F	F	0	F	info	F	T	F
IPRAN Backhaul Received Util Acceptable Trap	IPRAN Backhaul Received Util Trap	IPRAN Backhaul Received Util Acceptable Trap	N/A	PortLayer1Oid	F	F	F	0	F	clr	F	T	F
IPRAN Backhaul Received Util Warning Trap	IPRAN Backhaul Received Util Trap	IPRAN Backhaul Received Util Warning Trap	N/A	PortLayer1Oid	F	F	F	0	T	wrn	F	T	F
IPRAN Backhaul Received Util Overloaded Trap	IPRAN Backhaul Received Util Trap	IPRAN Backhaul Received Util Overloaded Trap	N/A	PortLayer1Oid	F	F	F	0	T	maj	F	T	F
IPRAN Backhaul Sent Util Acceptable Trap	IPRAN Backhaul Sent Util Trap	IPRAN Backhaul Sent Util Acceptable Trap	N/A	PortLayer1Oid	F	F	F	0	F	clr	F	T	F
IPRAN Backhaul Sent Util Overloaded Trap	IPRAN Backhaul Sent Util Trap	IPRAN Backhaul Sent Util Overloaded Trap	N/A	PortLayer1Oid	F	F	F	0	T	wrn	F	T	F
IPRAN Backhaul Sent Util Warning Trap	IPRAN Backhaul Sent Util Trap	IPRAN Backhaul Sent Util WarningTrap	N/A	PortLayer1Oid	F	F	F	0	T	maj	F	T	F

Table 16-19 Cisco IOS V1 Trap Registry Parameters (continued)

Short Description	Event Type	Event Subtype	Expedites Polling	Event Source (IMO Name)	Activate Flow	Correlate	Is Correlation Allowed	Weight	Auto Clear	Severity	Is Ticketable	Auto Remove	Flapping
Connection Loss detected by ipsla icmp echo trap	ipsla echo connloss trap	connection loss detected by ipsla icmp echo trap	N/A	Managed Element	F	F	F	0	F	minor	T	T	F
Connection re-establish detected by ipsla icmp echo trap	ipsla echo connloss trap	connection re-establish detected by ipsla icmp echo trap	N/A	Managed Element	F	F	F	0	F	clr	F	T	F
Timeout detected by ipsla icmp echo trap	ipsla ip or lsp echo timeout trap	timeout detected by ipsla icmp echo trap	N/A	Managed Element	F	F	F	0	F	info	F	T	F
Connection re-establish detected by ipsla icmp echo trap	ipsla ip or lsp echo timeout trap	connection re-establish detected by ipsla icmp echo trap	N/A	Managed Element	F	F	F	0	F	info	F	T	F
Threshold crossing under trap	ipsla threshold notification trap	threshold crossing under trap	N/A	Managed Element	F	F	F	0	F	info	F	T	F
Threshold crossing over trap	ipsla threshold notification trap	threshold crossing over trap	N/A	Managed Element	F	F	F	0	F	info	F	T	F
Data corruption in rtt operation trap	ipsla threshold notification trap	data corruption in rtt operation trap	N/A	Managed Element	F	F	F	0	F	info	F	T	F
Data corruption cleared in rtt operation trap	ipsla threshold notification trap	data corruption cleared in rtt operation trap	N/A	Managed Element	F	F	F	0	F	info	F	T	F
Connection Loss detected by ipsla icmp echo trap	ipsla echo connloss trap	connection loss detected by ipsla icmp echo trap	N/A	Managed Element	F	F	F	0	F	maj	T	T	F

Table 16-19 Cisco IOS V1 Trap Registry Parameters (continued)

Short Description	Event Type	Event Subtype	Expedites Polling	Event Source (IMO Name)	Activate Flow	Correlate	Is Correlation Allowed	Weight	Auto Clear	Severity	Is Ticketable	Auto Remove	Flapping
Connection Loss detected by ipsla LSP icmp echo trap	ipsla echo connloss trap	connection loss detected by ipsla lsp icmp echo trap	N/A	Managed Element	F	F	F	0	F	minor	T	T	F
Connection re-establish detected by ipsla icmp echo trap	ipsla echo connloss trap	connection re-establish detected by ipsla icmp echo trap	N/A	Managed Element	F	F	F	0	F	clr	F	T	F
Connection re-establish detected by ipsla LSP icmp echo trap	ipsla echo connloss trap	connection re-establish detected by ipsla lsp icmp echo trap	N/A	Managed Element	F	F	F	0	F	clr	F	T	F
Timeout detected by ipsla icmp echo trap	ipsla echo timeout trap	timeout detected by ipsla icmp echo trap	N/A	Managed Element	F	F	F	0	F	minor	T	T	F
Timeout detected by ipsla LSP icmp echo trap	ipsla echo timeout trap	timeout detected by ipsla lsp icmp echo trap	N/A	Managed Element	F	F	F	0	F	minor	T	T	F
Connection re-establish detected by ipsla icmp echo trap	ipsla echo timeout trap	connection re-establish detected by ipsla icmp echo trap	N/A	Managed Element	F	F	F	0	F	clr	F	T	F
Connection re-establish detected by ipsla LSP icmp echo trap	ipsla echo timeout trap	connection re-establish detected by ipsla lsp icmp echo trap	N/A	Managed Element	F	F	F	0	F	clr	F	T	F
RTT threshold crossing over trap	ipsla echo rtt trap	rtt threshold crossing over trap	N/A	Managed Element	F	F	F	0	F	info	F	T	F
RTT threshold crossing under trap	ipsla echo rtt trap	rtt threshold crossing under trap	N/A	Managed Element	F	F	F	0	F	info	F	T	F

Table 16-19 Cisco IOS V1 Trap Registry Parameters (continued)

Short Description	Event Type	Event Subtype	Expedites Polling	Event Source (IMO Name)	Activate Flow	Correlate	Is Correlation Allowed	Weight	Auto Clear	Severity	Is Ticketable	Auto Remove	Flapping
IPSLA LSP path discovery failure trap	ipsla lpd discovery trap	ipsla lsp path discovery failure trap	N/A	Managed Element	F	F	F	0	F	minor	T	T	F
IPSLA LSP path rediscovery trap	ipsla lpd discovery trap	ipsla lsp path rediscovery trap	N/A	Managed Element	F	F	F	0	F	clr	F	T	F
IPSLA LDP group status failure trap	ipsla lpd group status trap	ipsla ldp group status failure trap	N/A	Managed Element	F	F	F	0	F	minor	T	T	F
IPSLA LDP group status restoration trap	ipsla lpd group status trap	ipsla ldp group status restoration trap	N/A	Managed Element	F	F	F	0	F	clr	F	T	F
FRR Protected Trap	frr trigger trap	frr protected trap	N/A	PortLayer 1	F	T	F	0	F	info	F	T	F
FRR Unprotected Trap	frr trigger trap	frr unprotected trap	N/A	PortLayer 1	F	T	F	0	F	info	F	T	F
Pseudo wire tunnel up	pseudo wire tunnel traps	Pseudo wire tunnel up	ce-pw-tunnels-status-trap	IPTPLayer2MplsTunnel	F	F	F	0	F	clr	F	T	T
Pseudo wire tunnel down	pseudo wire tunnel traps	Pseudo wire tunnel down	ce-pw-tunnels-status-trap	IPTPLayer2MplsTunnel	F	T	F	0	T	min	F	T	T
vtp configuration revision number error trap	vtp notification prefix trap	vtp Config Rev Number Error	N	VtpKey	F	F	F	0	F	wrn	F	T	F
vtp configuration digest error trap	vtp notification prefix trap	vtp Config Digest Error	N	VtpKey	F	F	F	0	F	maj	F	T	F
vtp VersionOne Device Detected trap	vtp notification prefix trap	vtp VersionOne Device Detected	N	VtpKey	F	F	F	0	F	min	F	T	F

Table 16-19 Cisco IOS V1 Trap Registry Parameters (continued)

Short Description	Event Type	Event Subtype	Expedites Polling	Event Source (IMO Name)	Activate Flow	Correlate	Is Correlation Allowed	Weight	Auto Clear	Severity	Is Ticketable	Auto Remove	Flapping
vtp Local Mode Changed trap	vtp notification prefix trap	vtp Local Mode Changed	N	VtpKey	F	F	F	0	F	min	F	T	F
vtp VersionInUse Changed trap	vtp notification prefix trap	vtp VersionInUse Changed	N	VtpKey	F	F	F	0	F	info	F	T	F
Vlan trunk port dynamic status changed to trunking	vlan-trunk-port-dynamic-status	trunking	N	IPortLayer1	F	F	F	0	F	wrn	F	T	F
Vlan trunk port dynamic status changed to not trunking	vlan-trunk-port-dynamic-status	not trunking	N	IPortLayer1	F	T	F	0	F	wrn	F	T	F
REP port state fully operational Trap	REP port operational state change	REP port state fully operational	N/A	IREPService	F	F	F	0	F	clr	F	T	F
REP port state not operational Trap	REP port operational state change	REP port state not operational	N/A	IREPService	F	T	F	0	T	min	F	T	F
REP port role failed Trap	REP port role change trap	REP port role failed	N/A	IREPService	F	T	F	0	F	min	T	T	F
REP port role clear Trap	REP port role change trap	REP port role clear	N/A	IREPService	F	F	F	0	F	clr	F	T	F
Cisco Sonet vt status changed to error	sonet vt status changed	sonet vt status changed to error	N	IPortLayer1	F	T	F	0	T	maj	T	T	T
Cisco Sonet vt status changed to clear	sonet vt status changed	sonet vt status changed to clear	N	IPortLayer1	F	F	F	0	F	clr	F	T	T
CFM cc mep up trap	cisco cfm cc mep down trap	mep up	N/A	ICfmServiceOid	F	F	F	0	F	clr	F	T	F

Table 16-19 Cisco IOS V1 Trap Registry Parameters (continued)

Short Description	Event Type	Event Subtype	Expedites Polling	Event Source (IMO Name)	Activate Flow	Correlate	Is Correlation Allowed	Weight	Auto Clear	Severity	Is Ticketable	Auto Remove	Flapping
CFM cc mep down due to timeout trap	cisco cfm cc mep down trap	timeout	N/A	ICfmServiceOid	F	T	F	0	T	minor	F	T	F
CFM cc mep down due to last gasp trap	cisco cfm cc mep down trap	lastgasp	N/A	ICfmServiceOid	F	T	F	0	T	minor	F	T	F
CFM cc cross-connected service error trap	cisco cfm cc cross-connected service error trap	cross-connected service error trap	N/A	ICfmServiceOid	F	F	F	0	F	info	F	T	F
CFM cc cross-connected service error trap clear	cisco cfm cc cross-connected service error trap	cross-connected service error trap clear	N/A	ICfmServiceOid	F	F	F	0	F	clr	F	T	F
CFM cc loop trap	cisco cfm cc loop trap	loop trap	N/A	ICfmServiceOid	F	F	F	0	F	info	F	T	F
CFM cc loop trap clear	cisco cfm cc loop trap	loop trap clear	N/A	ICfmServiceOid	F	F	F	0	F	clr	F	T	F
CFM cc config error trap	cisco cfm cc config error trap	config error trap	N/A	ICfmServiceOid	F	T	F	0	F	info	F	T	F
CFM cc config error trap clear	cisco cfm cc config error trap	config error trap clear	N/A	ICfmServiceOid	F	F	F	0	F	clr	F	T	F
CFM crossconnect mep missing trap	cisco cfm crossconnect mep missing trap	mep missing trap	N/A	ICfmServiceOid	F	T	F	0	T	minor	F	T	F
CFM crossconnect mep unknown trap	cisco cfm crossconnect mep unknown trap	mepunknown trap	N/A	ICfmServiceOid	F	T	F	0	T	minor	F	T	F
CFM crossconnect mep unknown trap clear	cisco cfm crossconnect mep unknown trap	mepunknown trap clear	N/A	ICfmServiceOid	F	F	F	0	F	clr	F	T	F

Table 16-19 Cisco IOS V1 Trap Registry Parameters (continued)

Short Description	Event Type	Event Subtype	Expedites Polling	Event Source (IMO Name)	Activate Flow	Correlate	Is Correlation Allowed	Weight	Auto Clear	Severity	Is Ticketable	Auto Remove	Flapping
CFM crossconnect mep service up trap	cisco cfm crossconnect mep service up trap	mep service up trap	N/A	ICfmServiceOid	F	F	F	0	F	clr	T	T	F
Vrrp trap auth failure trap	vrrp trap auth failure trap	vrrp trap auth failure trap	N	IManaged Element	F	F	F	0	T	minor	F	T	F
Vrrp trap new master trap	vrrp trap new master trap	vrrp trap new master trap	N	IManaged Element	F	F	F	0	T	info	F	T	F
OAM Non-threshold crossing link fault trap	OAM non-threshold crossing trap	linkFault	oam	IPhysical Layer	F	T	F	0	F	info	F	T	F
OAM Non-threshold crossing dying gasp trap	OAM non-threshold crossing trap	dyingGaspEvent	oam	IPhysical Layer	F	T	F	0	F	info	F	T	F
OAM Non-threshold crossing critical Link trap	OAM non-threshold crossing trap	criticalLinkEvent	oam	IPhysical Layer	F	T	F	0	F	info	F	T	F
OAM threshold errored Symbol trap	OAM threshold crossing trap	erroredSymbolEvent	oam	IPhysical Layer	F	T	F	0	F	info	F	T	F
OAM threshold errored Frame Period trap	OAM threshold crossing trap	erroredFramePeriodEvent	oam	IPhysical Layer	F	T	F	0	F	info	F	T	F
OAM threshold errored Frame trap	OAM threshold crossing trap	erroredFrameEvent	oam	IPhysical Layer	F	T	F	0	F	info	F	T	F
OAM threshold errored Frame Seconds trap	OAM threshold crossing trap	erroredFrameSecondsEvent	oam	IPhysical Layer	F	T	F	0	F	info	F	T	F

Table 16-19 Cisco IOS V1 Trap Registry Parameters (continued)

Short Description	Event Type	Event Subtype	Expedites Polling	Event Source (IMO Name)	Activate Flow	Correlate	Is Correlation Allowed	Weight	Auto Clear	Severity	Is Ticketable	Auto Remove	Flapping
CBF File operation state indicator	cbf define file completion	cbf define file completion	N	IManaged Element	F	F	F	0	T	info	F	T	F
Cisco BGP backward transition trap	cisco bgp trap	cisco bgp backward transition trap	N	IBgpNeighbourEntry	F	T	F	0	T	info	F	T	T
Cisco BGP down trap	cisco bgp trap	cisco bgp down trap	N	IBgpNeighbourEntry	F	T	T	0	T	maj	F	T	T
Cisco BGP established trap	cisco bgp trap	cisco bgp established trap	N	IBgpNeighbourEntry	F	F	F	0	T	clr	F	T	T
Cisco BGP prefix threshold exceeded	cisco bgp prefix threshold exceeded	cisco bgp prefix threshold exceeded	N	IProfileContainer (BGP)	F	T	F	0	T	wrn	F	T	T
Cisco BGP prefix threshold clear	cisco bgp prefix threshold exceeded	cisco bgp prefix threshold clear	N	IProfileContainer (BGP)	F	F	F	0	T	clr	F	T	T
Cisco Configuration management event notification	cisco config man event	cisco config man event	N	IManaged Element	F	F	F	0	T	info	F	T	F
cefc fan-tray oper status down	cefc fan tray status changed	cefc fan status down	physical-command	IModule	F	T	T	0	T	cri	F	T	T
cefc fan-tray oper status up	cefc fan tray status changed	cefc fan status up	physical-command	IModule	F	F	F	0	T	clr	F	T	T
cefc FRU inserted	cefc fru removed	cefc fru inserted	physical-command	IModule	F	F	F	0	T	clr	F	T	T
cefc FRU removed	cefc fru removed	cefc fru removed	physical-command	IModule	F	T	T	0	T	maj	F	T	T

Table 16-19 Cisco IOS V1 Trap Registry Parameters (continued)

Short Description	Event Type	Event Subtype	Expedites Polling	Event Source (IMO Name)	Activate Flow	Correlate	Is Correlation Allowed	Weight	Auto Clear	Severity	Is Ticketable	Auto Remove	Flapping
cefc module oper status down	cefc module oper status changed	cefc module oper down	physical-command	IModule	F	T	T	0	T	maj	F	T	T
cefc module oper status up	cefc module oper status changed	cefc module oper up	physical-command	IModule	F	F	F	0	F	clr	F	T	T
cefc power status down	cefc power status changed	cefc power status down	physical-command	IModule	F	T	T	0	T	maj	F	T	T
cefc power status up	cefc power status changed	cefc power status up	physical-command	IModule	F	F	F	0	F	clr	F	T	T
sensor value crossed threshold in entSensorThresholdTable	entity sensor threshold notification	entity sensor threshold notification	N	IManagedElement	F	F	F	0	F	maj	T	T	T
Cisco flash copy failed	cisco flash copy completed	cisco flash copy failed	N	IManagedElement	F	F	F	0	F	info	F	T	F
Cisco flash copy completion	cisco flash copy completed	cisco flash copy completed	N	IManagedElement	F	F	F	0	F	info	F	T	F
Cisco flash copy in progress	cisco flash copy completed	cisco flash copy in progress	N	IManagedElement	F	F	F	0	F	info	F	T	F
Cisco Flash device changed	cisco flash device changed	cisco flash device changed	N	IManagedElement	F	F	F	0	F	wrn	F	T	F
Cisco Flash device inserted	cisco flash device removed	cisco flash device inserted	N	IManagedElement	F	F	F	0	F	clr	F	T	T
Cisco Flash device removed	cisco flash device removed	cisco flash device removed	N	IManagedElement	F	F	F	0	F	wrn	F	T	T
Cisco Flash device inserted	cisco flash device removed	cisco flash device inserted	N	IManagedElement	F	F	F	0	F	clr	F	T	T

Table 16-19 Cisco IOS V1 Trap Registry Parameters (continued)

Short Description	Event Type	Event Subtype	Expedites Polling	Event Source (IMO Name)	Activate Flow	Correlate	Is Correlation Allowed	Weight	Auto Clear	Severity	Is Ticketable	Auto Remove	Flapping
Cisco Flash device removed	cisco flash device removed	cisco flash device removed	N	IManaged Element	F	F	F	0	F	wrn	F	T	T
Cisco Flash miscellaneous operation failed	cisco flash operation completed	cisco flash operation failed	N	IManaged Element	F	F	F	0	F	info	F	T	F
Cisco Flash miscellaneous operation completed	cisco flash operation completed	cisco flash operation completed	N	IManaged Element	F	F	F	0	F	info	F	T	F
Cisco Flash miscellaneous operation in progress	cisco flash operation completed	cisco flash operation in progress	N	IManaged Element	F	F	F	0	F	info	F	T	F
chassis alarm off	chassis alarm trap	chassis alarm off	N	IManaged Element	F	F	F	0	F	clr	F	T	F
chassis alarm on	chassis alarm trap	chassis alarm on	N	IManaged Element	F	T	F	0	T	min	F	T	F
Cisco PIM neighbor lost	cisco pim neighbor lost	cisco pim neighbor lost	N	IRoutingEntry	F	T	T	0	F	info	T	T	T
Cisco ping completion	cisco ping completion	cisco ping completion	N	IManaged Element	F	F	F	0	F	info	F	T	F
Cisco Sonet section status changed to error	sonet section status changed	sonet section status changed to error	N	IPortLayer1	F	T	T	0	F	maj	F	T	T
Cisco Sonet section status changed to clear	sonet section status changed	sonet section status changed to clear	N	IPortLayer1	F	F	F	0	F	clr	F	T	T
Cisco Sonet line status changed to error	sonet line status changed	sonet line status changed to error	N	IPortLayer1	F	T	T	0	F	maj	F	T	T

Table 16-19 Cisco IOS V1 Trap Registry Parameters (continued)

Short Description	Event Type	Event Subtype	Expedites Polling	Event Source (IMO Name)	Activate Flow	Correlate	Is Correlation Allowed	Weight	Auto Clear	Severity	Is Ticketable	Auto Remove	Flapping
Cisco Sonet line status changed to clear	sonet line status changed	sonet line status changed to clear	N	IPortLayer1	F	F	F	0	F	clr	F	T	T
Cisco Sonet path status changed to error	sonet path status changed	sonet path status changed to error	N	IPortLayer1	F	T	T	0	F	maj	F	T	T
Cisco Sonet path status changed to clear	sonet path status changed	sonet path status changed to clear	N	IPortLayer1	F	F	F	0	F	clr	F	T	T
MPLS LDP init session threshold exceeded Trap	mpls ldp session down	mpls ldp init session thresh exceeded	N	IPortLayer1	F	T	F	0	T	wrn	F	T	T
MPLS LDP session down Trap	mpls ldp session down	mpls ldp session down	mpls interfaces' and 'label switching table'	IPortLayer1	T	T	T	0	T	min	F	T	T
MPLS LDP session up Trap	mpls ldp session down	mpls ldp session up	mpls interfaces' and 'label switching table'	IPortLayer1	F	T	F	0	T	clr	F	T	T
MPLS-TE tunnel up trap	mpls te tunnel down trap	mpls te tunnel up trap	mpls traffic engineering tunnel information	IMplsTETunnel	F	F	F	0	F	clr	F	T	F
MPLS-TE tunnel down trap	mpls te tunnel down trap	mpls te tunnel down trap	mpls traffic engineering tunnel information	IMplsTETunnel	F	T	F	0	T	maj	F	T	T

Table 16-19 Cisco IOS V1 Trap Registry Parameters (continued)

Short Description	Event Type	Event Subtype	Expedites Polling	Event Source (IMO Name)	Activate Flow	Correlate	Is Correlation Allowed	Weight	Auto Clear	Severity	Is Ticketable	Auto Remove	Flapping
MPLS-TE tunnel rerouted trap	mpls te tunnel rerouted trap	mpls te tunnel rerouted trap	N	IMplsTETunnel	F	T	F	0	F	info	T	T	T
Failed receive multicast router heartbeat	cisco multicast router heartbeat failed	cisco multicast router heartbeat failed	N	IManagedElement	F	T	F	0	F	info	F	T	F
Cisco VSS Shelf 1 is Disabled	VSS RF State Change	Shelf 1 is Disabled	vss-shelfs-status-command	IShelf	F	F	F	110000	F	info	T	T	F
Cisco VSS Shelf 1 is Standby Cold	VSS RF State Change	Shelf 1 is Standby Cold	vss-shelfs-status-command	IShelf	F	F	F	110000	F	info	T	T	F
Cisco VSS Shelf 1 is Standby Hot	VSS RF State Change	Shelf 1 is Standby Hot	vss-shelfs-status-command	IShelf	F	F	F	110000	F	info	T	T	F
Cisco VSS Shelf 2 is Disabled	VSS RF State Change	Shelf 2 is Disabled	vss-shelfs-status-command	IShelf	F	F	F	110000	F	info	T	T	F
Cisco VSS Shelf 2 is Standby Cold	VSS RF State Change	Shelf 2 is Standby Cold	vss-shelfs-status-command	IShelf	F	F	F	110000	F	info	T	T	F
Cisco VSS Shelf 2 is Standby Hot	VSS RF State Change	Shelf 2 is Standby Hot	vss-shelfs-status-command	IShelf	F	F	F	110000	F	info	T	T	F
VSL Connection Changed: Down	VSL Connection State Change	VSL Connection State Down	physical-entity-mib-snmp-cisco6500vss + vss-shelfs-status-command	IShelf	F	F	F	110000	F	info	T	T	F

Table 16-19 Cisco IOS V1 Trap Registry Parameters (continued)

Short Description	Event Type	Event Subtype	Expedites Polling	Event Source (IMO Name)	Activate Flow	Correlate	Is Correlation Allowed	Weight	Auto Clear	Severity	Is Ticketable	Auto Remove	Flapping
VSL Connection Change: Up	VSL Connection State Change	VSL Connection State Up	physical-entity-mib-snmp-cisco6500vss + vss-shelfs-status-command	IShelf	F	F	F	110000	F	info	T	T	F
dot1qBridge trap	dot1qBridge trap	dot1qBridge trap	N	IStpService	F	T	F	0	F	info	F	T	F
Mep up trap	mep trap	mep up	N	IManagedElement	F	F	F	0	F	clr	F	T	F
Mep down trap	mep trap	mep down	N	IManagedElement	F	F	F	0	T	maj	F	T	F
Cold start trap	cold start trap	cold start trap	N	IManagedElement	F	F	T	190000	F	info	T	T	F
Cisco hsrp state standby	cisco hsrp state change	cisco hsrp state standby	hsrp information (command under forwarding investigator)	IIPInterface	F	T	F	0	F	info	T	T	T
Cisco hsrp state non active	cisco hsrp state change	cisco hsrp state non active	hsrp information (command under forwarding investigator)	IIPInterface	F	T	F	0	F	info	T	T	T

Table 16-19 Cisco IOS V1 Trap Registry Parameters (continued)

Short Description	Event Type	Event Subtype	Expedites Polling	Event Source (IMO Name)	Activate Flow	Correlate	Is Correlation Allowed	Weight	Auto Clear	Severity	Is Ticketable	Auto Remove	Flapping
Cisco hsrp state active	cisco hsrp state change	cisco hsrp state active	hsrp information (command under forwarding investigator)	IIPInterface	F	T	F	0	F	info	T	T	T
Cisco Environment Monitoring Fan Notification - Critical	cisco-Environment-Monitoring-Fan-Notification	critical	N	IManaged Element + identifier index	F	F	F	0	F	cri	T	T	F
Cisco Environment Monitoring Fan Notification - Normal	cisco-Environment-Monitoring-Fan-Notification	normal	N	IManaged Element + identifier index	F	F	F	0	F	clr	T	T	F
Cisco Environment Monitoring Fan Notification - Not Functioning	cisco-Environment-Monitoring-Fan-Notification	notFunctioning	N	IManaged Element + identifier index	F	F	F	0	F	maj	T	T	F
Cisco Environment Monitoring Fan Notification - Not Present	cisco-Environment-Monitoring-Fan-Notification	notPresent	N	IManaged Element + identifier index	T	F	F	0	F	maj	T	T	F
Cisco Environment Monitoring Fan Notification - Shutdown	cisco-Environment-Monitoring-Fan-Notification	shutdown	N	IManaged Element + identifier index	F	F	F	0	F	cri	T	T	F

Table 16-19 Cisco IOS V1 Trap Registry Parameters (continued)

Short Description	Event Type	Event Subtype	Expedites Polling	Event Source (IMO Name)	Activate Flow	Correlate	Is Correlation Allowed	Weight	Auto Clear	Severity	Is Ticketable	Auto Remove	Flapping
Cisco Environment Monitoring Fan Notification - Warning	cisco-Environment-Monitoring-Fan-Notification	warning	N	IManaged Element + identifier index	F	F	F	0	F	wrn	T	T	F
Redundant Supply State - Critical	cisco-EnvMon-Redundant-Supply-Notification-Trap	critical	N	IManaged Element + identifier index	F	F	F	0	F	cri	F	T	F
Redundant Supply State - Normal	cisco-EnvMon-Redundant-Supply-Notification-Trap	normal	N	IManaged Element + identifier index	F	F	F	0	F	clr	T	T	F
Redundant Supply State - Not Functioning	cisco-EnvMon-Redundant-Supply-Notification-Trap	notFunctioning	N	IManaged Element + identifier index	F	F	F	0	F	maj	T	T	F
Redundant Supply State - Not Present	cisco-EnvMon-Redundant-Supply-Notification-Trap	notPresent	N	IManaged Element + identifier index	T	F	F	0	F	maj	T	T	F
Redundant Supply State - Shutdown	cisco-EnvMon-Redundant-Supply-Notification-Trap	shutdown	N	IManaged Element + identifier index	F	F	F	0	F	cri	T	T	F
Redundant Supply State - Warning	cisco-EnvMon-Redundant-Supply-Notification-Trap	warning	N	IManaged Element + identifier index	F	F	F	0	F	wrn	T	T	F
new root trap	new root trap	new root trap	N	IStpService	F	F	F	0	F	info	F	T	F
stpx port inconsistency discovered	stpx port inconsistency update	stpx port inconsistency discovered	N	IStpService	F	T	F	0	F	maj	T	T	F
stpx port inconsistency resolved	stpx port inconsistency update	stpx port inconsistency resolved	N	IStpService	F	F	F	0	F	clr	T	T	F
stpx loop inconsistency discovered	stpx loop inconsistency update	stpx loop inconsistency discovered	N	IStpService	F	T	F	0	F	maj	T	T	F

Table 16-19 Cisco IOS V1 Trap Registry Parameters (continued)

Short Description	Event Type	Event Subtype	Expedites Polling	Event Source (IMO Name)	Activate Flow	Correlate	Is Correlation Allowed	Weight	Auto Clear	Severity	Is Ticketable	Auto Remove	Flapping
stpx loop inconsistency resolved	stpx loop inconsistency update	stpx loop inconsistency resolved	N	IStpService	F	F	F	0	F	clr	T	T	F
stpx root inconsistency discovered	stpx root inconsistency update	stpx root inconsistency discovered	N	IStpService	F	T	F	0	F	maj	T	T	F
stpx root inconsistency resolved	stpx root inconsistency update	stpx root inconsistency resolved	N	IStpService	F	F	F	0	F	clr	T	T	F
vtp configuration revision number error trap	vtp notification prefix trap	vtp Config Rev Number Error	N	VtpKey	F	F	F	0	F	wrn	F	T	F
vtp configuration digest error trap	vtp notification prefix trap	vtp Config Digest Error	N	VtpKey	F	F	F	0	F	info	F	T	F
cisco EnvMon Shutdown Notification Trap	cisco-EnvMon-Shutdown-Notification-Trap	cisco-EnvMon-Shutdown-Notification-Trap	N	IManagedElement	F	F	F	0	F	info	F	T	F
caem Temperature Notification Trap	caem-MIB-Notifications-Trap	caem Temperature Notification	N	IManagedElement	F	F	F	0	F	min	F	T	F
caem Voltage Notification Trap	caem-MIB-Notifications-Trap	caem Voltage Notification	N	IManagedElement	F	F	F	0	F	min	F	T	F
cmn Mac Changed Notification Trap	cmn-Mac-Changed-Notification-Trap	cmn-Mac-Changed-Notification-Trap	N	IManagedElement	F	F	F	0	F	info	F	T	F
cmn Mac Move Notification Trap	cmn-Mac-Move-Notification-Trap	cmn-Mac-Move-Notification-Trap	N	IManagedElement + identifier index	F	F	F	0	F	info	F	T	F

Table 16-19 Cisco IOS V1 Trap Registry Parameters (continued)

Short Description	Event Type	Event Subtype	Expedites Polling	Event Source (IMO Name)	Activate Flow	Correlate	Is Correlation Allowed	Weight	Auto Clear	Severity	Is Ticketable	Auto Remove	Flapping
vtp VersionOne Device Detected trap	vtp notification prefix trap	vtp VersionOne Device Detected	N	VtpKey	F	F	F	0	F	min	F	T	F
vtp Local Mode Changed trap	vtp notification prefix trap	vtp Local Mode Changed	N	VtpKey	F	F	F	0	F	info	F	T	F
vtp VersionInUse Changed trap	vtp notification prefix trap	vtp VersionInUse Changed	N	VtpKey	F	F	F	0	F	info	F	T	F
Vlan trunk port dynamic status changed to trunking	vlan-trunk-port-dynamic-status	trunking	N	IPortLayer1	F	F	F	0	F	wrn	F	T	F
Vlan trunk port dynamic status changed to not trunking	vlan-trunk-port-dynamic-status	not trunking	N	IPortLayer1	F	T	F	0	F	wrn	F	T	F
cps Secure MacAddr Violation Trap	cps-Secure-Mac Addr-Violation-Trap	cps-Secure-MacAddr-Violation-Trap	N	IPortLayer1	F	F	T	0	F	maj	T	T	F
cps IfVlan Secure MacAddr Violation Trap	cps-IfVlan-Secure-MacAddr-Violation-Trap	cps-IfVlan-Secure-MacAddr-Violation-Trap	N	IPortLayer1	F	F	T	0	F	maj	T	T	F
cisco L2 Control VlanMacLimit Notif Trap	cisco-L2-Control-VlanMacLimit-Notifs-Trap	clc VlanMacLimit Notif	N	IPortLayer1	F	F	F	0	F	info	F	T	F
cisco L2 Control VlanMacLimit High Notif Trap	cisco-L2-Control-VlanMacLimit-Notifs-Trap	clc VlanMacLimit High Notif	N	IPortLayer1	F	F	F	0	F	info	F	T	F

Table 16-19 Cisco IOS V1 Trap Registry Parameters (continued)

Short Description	Event Type	Event Subtype	Expedites Polling	Event Source (IMO Name)	Activate Flow	Correlate	Is Correlation Allowed	Weight	Auto Clear	Severity	Is Ticketable	Auto Remove	Flapping
cisco L2 Control IfMacLimit Low Notif Trap	cisco-L2-Control-IfMacLimit-Notifs-Trap	clc IfMacLimit Low Notif	N	IPortLayer1	F	F	F	0	F	info	F	T	F
cisco L2 Control IfMacLimit High Notif Trap	cisco-L2-Control-IfMacLimit-Notifs-Trap	clc IfMacLimit High Notif	N	IPortLayer1	F	F	F	0	F	info	F	T	F
cisco L2 Control IfVlanMacLimit Low Notif Trap	cisco-L2-Control-IfVlanMacLimit-Notifs-Trap	clc IfVlanMacLimit Low Notif	N	IPortLayer1	F	F	F	0	F	info	F	T	F
cisco L2 Control IfVlanMacLimit High Notif Trap	cisco-L2-Control-IfVlanMacLimit-Notifs-Trap	clc IfVlanMacLimit High Notif	N	IPortLayer1	F	F	F	0	F	info	F	T	F
Cisco SBC source alert off trap	cisco sbc source alert trap	off	N	ISbcService	F	F	F	0	F	clr	F	T	F
Cisco SBC source alert on trap	cisco sbc source alert trap	on	N	ISbcService	F	F	F	0	F	wrn	T	T	F
Cisco SBC source alert informational trap	cisco sbc source alert trap	informational	N	ISbcService	F	F	F	0	F	info	F	T	F
Cisco SBC dynamic blacklist trap	cisco sbc dynamic blacklist trap	cisco sbc dynamic blacklist trap	N	ISbcService	F	F	F	0	F	info	F	T	F
Cisco SBC adjacency state up trap	cisco sbc adjacency state change trap	up	N	ISbcService	F	F	F	0	F	clr	F	T	F
Cisco SBC adjacency state down trap	cisco sbc adjacency state change trap	down	N	ISbcService	F	F	F	0	F	maj	T	T	F

Table 16-19 Cisco IOS V1 Trap Registry Parameters (continued)

Short Description	Event Type	Event Subtype	Expedites Polling	Event Source (IMO Name)	Activate Flow	Correlate	Is Correlation Allowed	Weight	Auto Clear	Severity	Is Ticketable	Auto Remove	Flapping
Cisco SBC adjacency state informational trap	cisco sbc adjacency state change trap	informational	N	ISbcService	F	F	F	0	F	info	F	T	F
Cisco SBC service state up trap	cisco sbc service state change trap	up	sbc	ISbcService	F	F	F	0	F	clr	F	T	F
Cisco SBC service state down trap	cisco sbc service state change trap	down	sbc	ISbcService	F	F	F	0	F	cri	T	T	F
Cisco SBC service state informational trap	cisco sbc service state change trap	informational	sbc	ISbcService	F	F	F	0	F	info	F	T	F
Cisco SBC system congestion cleared trap	cisco sbc system congestion trap	cleared	N	ISbcService	F	F	F	0	F	clr	F	T	F
Cisco SBC system congestion raised trap	cisco sbc system congestion trap	raised	N	ISbcService	F	F	F	0	F	wrn	T	T	F
Cisco SBC system congestion informational trap	cisco sbc system congestion trap	informational	N	ISbcService	F	F	F	0	F	info	F	T	F
Cisco SBC SLA violation off trap	cisco sbc sla violation trap	off	N	ISbcService	F	F	F	0	F	clr	F	T	F
Cisco SBC SLA violation on trap	cisco sbc sla violation trap	on	N	ISbcService	F	F	F	0	F	min	T	T	F
Cisco SBC SLA violation informational trap	cisco sbc sla violation trap	informational	N	ISbcService	F	F	F	0	F	info	F	T	F

Table 16-19 Cisco IOS V1 Trap Registry Parameters (continued)

Short Description	Event Type	Event Subtype	Expedites Polling	Event Source (IMO Name)	Activate Flow	Correlate	Is Correlation Allowed	Weight	Auto Clear	Severity	Is Ticketable	Auto Remove	Flapping
Cisco SBC radius connection state up trap	cisco sbc radius connection state change trap	up	N	ISbcService	F	F	F	0	F	clr	F	T	F
Cisco SBC radius connection state down trap	cisco sbc radius connection state change trap	down	N	ISbcService	F	F	F	0	F	maj	T	T	F
Cisco SBC radius connection state informational trap	cisco sbc radius connection state change trap	informational	N	ISbcService	F	F	F	0	F	info	F	T	F
Cisco SBC H248 controller state up trap	cisco sbc h248 controller state change trap	up	N	ISbcService	F	F	F	0	F	clr	F	T	F
Cisco SBC H248 controller state down trap	cisco sbc h248 controller state change trap	down	N	ISbcService	F	F	F	0	F	wrn	T	T	F
Cisco SBC H248 controller state informational trap	cisco sbc h248 controller state change trap	informational	N	ISbcService	F	F	F	0	F	info	F	T	F

Cisco IOS V2/V3 Trap Registry Parameters

Table 16-20 lists the associated event types, event subtypes, and Prime Network registry parameters for the Cisco IOS SNMP V2/V3 traps shown in Table 16-4.

Table 16-20 Cisco IOS V2/V3 Trap Registry Parameters

Short Description	Event Type	Event Subtype	Expedites Polling	Event Source (IMO Name)	Activate Flow	Correlate	Is Correlation Allowed	Weight	Auto Clear	Severity	Is Ticketable	Auto Remove	Flapping
CBF File operation state indicator	cbf define file completion	cbf define file completion	N	IManagedElement	F	F	F	0	T	info	F	T	F
Cisco BGP backward transition trap	cisco bgp trap	cisco bgp backward transition trap	N	IBgpNeighborEntry	F	T	F	0	T	info	F	T	T
Cisco BGP down trap	cisco bgp trap	cisco bgp down trap	N	IBgpNeighborEntry	F	T	T	0	T	maj	F	T	T
Cisco BGP established trap	cisco bgp trap	cisco bgp established trap	N	IBgpNeighborEntry	F	F	F	0	T	clr	F	T	T
Cisco BGP prefix threshold exceeded	cisco bgp prefix threshold exceeded	cisco bgp prefix threshold exceeded	N	IProfileContainer (BGP)	F	T	F	0	T	wrn	F	T	T
Cisco BGP prefix threshold clear	cisco bgp prefix threshold exceeded	cisco bgp prefix threshold clear	N	IProfileContainer (BGP)	F	F	F	0	T	clr	F	T	T
Config-copy request completion	cc copy completion	cc copy completion	N	IManagedElement	F	F	F	0	T	info	F	T	F
Cisco Configuration management event notification	cisco config man event	cisco config man event	N	IManagedElement	F	F	F	0	T	info	F	T	F
cefc fan-tray oper status down	cefc fan tray status changed	cefc fan status down	physical-command	IModule	F	T	T	0	T	cri	F	T	T
cefc fan-tray oper status up	cefc fan tray status changed	cefc fan status up	physical-command	IModule	F	F	F	0	T	clr	F	T	T
cefc FRU inserted	cefc fru removed	cefc fru inserted	physical-command	IModule	F	F	F	0	T	clr	F	T	T
cefc FRU removed	cefc fru removed	cefc fru removed	physical-command	IModule	F	T	T	0	T	maj	F	T	T
cefc module oper status down	cefc module oper status changed	cefc module oper down	physical-command	IModule	F	T	T	0	T	maj	F	T	T

Table 16-20 Cisco IOS V2/V3 Trap Registry Parameters (continued)

Short Description	Event Type	Event Subtype	Expedites Polling	Event Source (IMO Name)	Activate Flow	Correlate	Is Correlation Allowed	Weight	Auto Clear	Severity	Is Ticketable	Auto Remove	Flapping
cefc module oper status up	cefc module oper status changed	cefc module oper up	physical-command	IModule	F	F	F	0	F	clr	F	T	T
cefc power status down	cefc power status changed	cefc power status down	physical-command	IModule	F	T	T	0	T	maj	F	T	T
cefc power status up	cefc power status changed	cefc power status up	physical-command	IModule	F	F	F	0	F	clr	F	T	T
sensor value crossed threshold in entSensorThresholdTable	entity sensor threshold notification	entity sensor threshold notification	N	IManagedElement	F	F	F	0	F	maj	T	T	T
Cisco flash copy failed	cisco flash copy completed	cisco flash copy failed	N	IManagedElement	F	F	F	0	F	info	F	T	F
Cisco flash copy completion	cisco flash copy completed	cisco flash copy completed	N	IManagedElement	F	F	F	0	F	info	F	T	F
Cisco flash copy in progress	cisco flash copy completed	cisco flash copy in progress	N	IManagedElement	F	F	F	0	F	info	F	T	F
Cisco Flash device changed	cisco flash device changed	cisco flash device changed	N	IManagedElement	F	F	F	0	F	wrn	F	T	F
Cisco Flash device inserted	cisco flash device removed	cisco flash device inserted	N	IManagedElement	F	F	F	0	F	clr	F	T	T
Cisco Flash device removed	cisco flash device removed	cisco flash device removed	N	IManagedElement	F	F	F	0	F	wrn	F	T	T
Cisco Flash device inserted	cisco flash device removed	cisco flash device inserted	N	IManagedElement	F	F	F	0	F	clr	F	T	T
Cisco Flash device removed	cisco flash device removed	cisco flash device removed	N	IManagedElement	F	F	F	0	F	wrn	F	T	T
Cisco Flash miscellaneous operation failed	cisco flash operation completed	cisco flash operation failed	N	IManagedElement	F	F	F	0	F	info	F	T	F

Table 16-20 Cisco IOS V2/V3 Trap Registry Parameters (continued)

Short Description	Event Type	Event Subtype	Expedites Polling	Event Source (IMO Name)	Activate Flow	Correlate	Is Correlation Allowed	Weight	Auto Clear	Severity	Is Ticketable	Auto Remove	Flapping
Cisco Flash miscellaneous operation completed	cisco flash operation completed	cisco flash operation completed	N	IManagedElement	F	F	F	0	F	info	F	T	F
Cisco Flash miscellaneous operation in progress	cisco flash operation completed	cisco flash operation in progress	N	IManagedElement	F	F	F	0	F	info	F	T	F
chassis alarm off	chassis alarm trap	chassis alarm off	N	IManagedElement	F	F	F	0	F	clr	F	T	F
chassis alarm on	chassis alarm trap	chassis alarm on	N	IManagedElement	F	T	F	0	T	min	F	T	F
Cisco PIM neighbor lost	cisco pim neighbor lost	cisco pim neighbor lost	N	IRoutingEntry	F	T	T	0	F	info	T	T	T
Cisco ping completion	cisco ping completion	cisco ping completion	N	IManagedElement	F	F	F	0	F	info	F	T	F
Cisco Sonet section status changed to error	sonet section status changed	sonet section status changed to error	N	IPortLayer1	F	T	T	0	F	maj	F	T	T
Cisco Sonet section status changed to clear	sonet section status changed	sonet section status changed to clear	N	IPortLayer1	F	F	F	0	F	clr	F	T	T
Cisco Sonet line status changed to error	sonet line status changed	sonet line status changed to error	N	IPortLayer1	F	T	T	0	F	maj	F	T	T
Cisco Sonet line status changed to clear	sonet line status changed	sonet line status changed to clear	N	IPortLayer1	F	F	F	0	F	clr	F	T	T
Cisco Sonet path status changed to error	sonet path status changed	sonet path status changed to error	N	IPortLayer1	F	T	T	0	F	maj	F	T	T
Cisco Sonet path status changed to clear	sonet path status changed	sonet path status changed to clear	N	IPortLayer1	F	F	F	0	F	clr	F	T	T

Table 16-20 Cisco IOS V2/V3 Trap Registry Parameters (continued)

Short Description	Event Type	Event Subtype	Expedites Polling	Event Source (IMO Name)	Activate Flow	Correlate	Is Correlation Allowed	Weight	Auto Clear	Severity	Is Ticketable	Auto Remove	Flapping
MPLS LDP init session threshold exceeded Trap	mpls ldp session down	mpls ldp init session thresh exceeded	N	IPortLayer 1	F	T	F	0	T	wrn	F	T	T
MPLS LDP session down Trap	mpls ldp session down	mpls ldp session down	mpls interfaces' and 'label switching table	IPortLayer 1	T	T	T	0	T	min	F	T	T
MPLS LDP session up Trap	mpls ldp session down	mpls ldp session up	mpls interfaces' and 'label switching table	IPortLayer 1	F	T	F	0	T	clr	F	T	T
MPLS TE tunnel up trap	mpls te tunnel down trap	mpls te tunnel up trap	mpls traffic engineering tunnel information	IMplsTETunnel	F	F	F	0	F	clr	F	T	F
MPLS TE tunnel down trap	mpls te tunnel down trap	mpls te tunnel down trap	mpls traffic engineering tunnel information	IMplsTETunnel	F	T	F	0	T	maj	F	T	T
MPLS TE tunnel rerouted trap	mpls te tunnel rerouted trap	mpls te tunnel rerouted trap	N	IMplsTETunnel	F	T	F	0	F	info	T	T	T
Failed receive multicast router heartbeat	cisco multicast router heartbeat failed	cisco multicast router heartbeat failed	N	IManagedElement	F	T	F	0	F	info	F	T	F
Cisco VSS Shelf 1 is Disabled	VSS RF State Change	Shelf 1 is Disabled	vss-shelfs-status-command	IShelf	F	F	F	110000	F	info	T	T	F
Cisco VSS Shelf 1 is Standby Cold	VSS RF State Change	Shelf 1 is Standby Cold	vss-shelfs-status-command	IShelf	F	F	F	110000	F	info	T	T	F
Cisco VSS Shelf 1 is Standby Hot	VSS RF State Change	Shelf 1 is Standby Hot	vss-shelfs-status-command	IShelf	F	F	F	110000	F	info	T	T	F

Table 16-20 Cisco IOS V2/V3 Trap Registry Parameters (continued)

Short Description	Event Type	Event Subtype	Expedites Polling	Event Source (IMO Name)	Activate Flow	Correlate	Is Correlation Allowed	Weight	Auto Clear	Severity	Is Ticketable	Auto Remove	Flapping
Cisco VSS Shelf 2 is Disabled	VSS RF State Change	Shelf 2 is Disabled	vss-shelfs-status-command	IShelf	F	F	F	110000	F	info	T	T	F
Cisco VSS Shelf 2 is Standby Cold	VSS RF State Change	Shelf 2 is Standby Cold	vss-shelfs-status-command	IShelf	F	F	F	110000	F	info	T	T	F
Cisco VSS Shelf 2 is Standby Hot	VSS RF State Change	Shelf 2 is Standby Hot	vss-shelfs-status-command	IShelf	F	F	F	110000	F	info	T	T	F
VSL Connection Changed: Down	VSL Connection State Change	VSL Connection State Down	physical-entity-mib-snmp-cisco 6500vss + vss-shelfs-status-command	IShelf	F	F	F	110000	F	info	T	T	F
VSL Connection Change: Up	VSL Connection State Change	VSL Connection State Up	physical-entity-mib-snmp-cisco 6500vss + vss-shelfs-status-command	IShelf	F	F	F	110000	F	info	T	T	F
dot1qBridge trap	dot1qBridge trap	dot1qBridge trap	N	IManagedElement	F	T	F	0	F	info	F	T	F
Mep up trap	mep trap	mep up	N	IManagedElement	F	F	F	0	F	clr	F	T	F
Mep down trap	mep trap	mep down	N	IManagedElement	F	F	F	0	T	maj	F	T	F
Cold start trap	cold start trap	cold start trap	N	IManagedElement	F	F	T	190000	F	info	T	T	F
Cisco hsrp state standby	cisco hsrp state change	cisco hsrp state standby	hsrp information(command under forwarding investigator)	IIPInterface	F	T	F	0	F	info	T	T	T

Table 16-20 Cisco IOS V2/V3 Trap Registry Parameters (continued)

Short Description	Event Type	Event Subtype	Expedites Polling	Event Source (IMO Name)	Activate Flow	Correlate	Is Correlation Allowed	Weight	Auto Clear	Severity	Is Ticketable	Auto Remove	Flapping
Cisco hsrp state non active	cisco hsrp state change	cisco hsrp state non active	hsrp information(command under forwarding investigator)	IIPInterface	F	T	F	0	F	info	T	T	T
Cisco hsrp state active	cisco hsrp state change	cisco hsrp state active	hsrp information(command under forwarding investigator)	IIPInterface	F	T	F	0	F	info	T	T	T
Cisco Environment Monitoring Fan Notification - Critical	cisco-Environment-Monitoring-Fan-Notification	critical	N	IManagedElement + identifier index	F	F	F	0	F	cri	T	T	F
Cisco Environment Monitoring Fan Notification - Normal	cisco-Environment-Monitoring-Fan-Notification	normal	N	IManagedElement + identifier index	F	F	F	0	F	clr	T	T	F
Cisco Environment Monitoring Fan Notification - Not Functioning	cisco-Environment-Monitoring-Fan-Notification	notFunctioning	N	IManagedElement + identifier index	F	F	F	0	F	maj	T	T	F
Cisco Environment Monitoring Fan Notification - Not Present	cisco-Environment-Monitoring-Fan-Notification	notPresent	N	IManagedElement + identifier index	T	F	F	0	F	maj	T	T	F
Cisco Environment Monitoring Fan Notification - Shutdown	cisco-Environment-Monitoring-Fan-Notification	shutdown	N	IManagedElement + identifier index	F	F	F	0	F	cri	T	T	F

Table 16-20 Cisco IOS V2/V3 Trap Registry Parameters (continued)

Short Description	Event Type	Event Subtype	Expedites Polling	Event Source (IMO Name)	Activate Flow	Correlate	Is Correlation Allowed	Weight	Auto Clear	Severity	Is Ticketable	Auto Remove	Flapping
Cisco Environment Monitoring Fan Notification - Warning	cisco-Environment-Monitoring-Fan-Notification	warning	N	IManagedElement + identifier index	F	F	F	0	F	wrn	T	T	F
Redundant Supply State - Critical	cisco-EnvMon-Redundant-Supply-Notification-Trap	critical	N	IManagedElement + identifier index	F	F	F	0	F	cri	F	T	F
Redundant Supply State - Normal	cisco-EnvMon-Redundant-Supply-Notification-Trap	normal	N	IManagedElement + identifier index	F	F	F	0	F	clr	T	T	F
Redundant Supply State - Not Functioning	cisco-EnvMon-Redundant-Supply-Notification-Trap	notFunctioning	N	IManagedElement + identifier index	F	F	F	0	F	maj	T	T	F
Redundant Supply State - Not Present	cisco-EnvMon-Redundant-Supply-Notification-Trap	notPresent	N	IManagedElement + identifier index	T	F	F	0	F	maj	T	T	F
Redundant Supply State - Shutdown	cisco-EnvMon-Redundant-Supply-Notification-Trap	shutdown	N	IManagedElement + identifier index	F	F	F	0	F	cri	T	T	F
Redundant Supply State - Warning	cisco-EnvMon-Redundant-Supply-Notification-Trap	warning	N	IManagedElement + identifier index	F	F	F	0	F	wrn	T	T	F
Critical Temperature	cisco-Environment-Monitoring-Temperature-Notification	critical	N	IManagedElement + identifier index	F	F	F	0	F	cri	T	T	F

Table 16-20 Cisco IOS V2/V3 Trap Registry Parameters (continued)

Short Description	Event Type	Event Subtype	Expedites Polling	Event Source (IMO Name)	Activate Flow	Correlate	Is Correlation Allowed	Weight	Auto Clear	Severity	Is Ticketable	Auto Remove	Flapping
Normal Temperature	cisco-Environment-Monitoring-Temperature-Notification	normal	N	IManagedElement + identifier index	F	F	F	0	F	clr	T	T	F
Not Functioning	cisco-Environment-Monitoring-Temperature-Notification	notFunctioning	N	IManagedElement + identifier index	F	F	F	0	F	maj	T	T	F
Not Present	cisco-Environment-Monitoring-Temperature-Notification	notPresent	N	IManagedElement + identifier index	F	F	F	0	F	maj	T	T	F
Critical Temperature - Device Shutdown	cisco-Environment-Monitoring-Temperature-Notification	shutdown	N	IManagedElement + identifier index	F	F	F	0	F	cri	T	T	F
Temperature Rising	cisco-Environment-Monitoring-Temperature-Notification	warning	N	IManagedElement + identifier index	F	F	F	0	F	wrn	T	T	F
new root trap	new root trap	new root trap	N	IStpService	F	F	F	0	F	info	F	T	F
stpx port inconsistency discovered	stpx port inconsistency update	stpx port inconsistency discovered	N	IStpService	F	T	F	0	F	maj	T	T	F
stpx port inconsistency resolved	stpx port inconsistency update	stpx port inconsistency resolved	N	IStpService	F	F	F	0	F	clr	T	T	F
stpx loop inconsistency discovered	stpx loop inconsistency update	stpx loop inconsistency discovered	N	IStpService	F	T	F	0	F	maj	T	T	F
stpx loop inconsistency resolved	stpx loop inconsistency update	stpx loop inconsistency resolved	N	IStpService	F	F	F	0	F	clr	T	T	F
stpx root inconsistency discovered	stpx root inconsistency update	stpx root inconsistency discovered	N	IStpService	F	T	F	0	F	maj	T	T	F

Table 16-20 Cisco IOS V2/V3 Trap Registry Parameters (continued)

Short Description	Event Type	Event Subtype	Expedites Polling	Event Source (IMO Name)	Activate Flow	Correlate	Is Correlation Allowed	Weight	Auto Clear	Severity	Is Ticketable	Auto Remove	Flapping
stpx root inconsistency resolved	stpx root inconsistency update	stpx root inconsistency resolved	N	IStpService	F	F	F	0	F	clr	T	T	F
vtp configuration revision number error trap	vtp notification prefix trap	vtp Config Rev Number Error	N	VtpKey	F	F	F	0	F	wrn	F	T	F
vtp configuration digest error trap	vtp notification prefix trap	vtp Config Digest Error	N	VtpKey	F	F	F	0	F	maj	F	T	F
cisco EnvMon Shutdown Notification Trap	cisco-EnvMon-Shutdown-Notification-Trap	cisco-EnvMon-Shutdown-Notification-Trap	N	IManagedElement	F	F	F	0	F	info	F	T	F
caem Temperature Notification Trap	caem-MIB-Notifications-Trap	caem Temperature Notification	N	IManagedElement	F	F	F	0	F	min	F	T	F
caem Voltage Notification Trap	caem-MIB-Notifications-Trap	caem Voltage Notification	N	IManagedElement	F	F	F	0	F	min	F	T	F
cmn Mac Changed Notification Trap	cmn-Mac-Changed-Notification-Trap	cmn-Mac-Changed-Notification-Trap	N	IManagedElement	F	F	F	0	F	min	F	T	F
cmn Mac Move Notification Trap	cmn-Mac-Move-Notification-Trap	cmn-Mac-Move-Notification-Trap	N	IManagedElement + identifier index	F	F	F	0	F	min	F	T	F
vtp VersionOne Device Detected trap	vtp notification prefix trap	vtp VersionOne Device Detected	N	VtpKey	F	F	F	0	F	info	F	T	F
vtp Local Mode Changed trap	vtp notification prefix trap	vtp Local Mode Changed	N	VtpKey	F	F	F	0	F	min	F	T	F
vtp VersionInUse Changed trap	vtp notification prefix trap	vtp VersionInUse Changed	N	VtpKey	F	F	F	0	F	info	F	T	F
Vlan trunk port dynamic status changed to trunking	vlan-trunk-port-dynamic-status	trunking	N	IPortLayer1	F	F	F	0	F	wrn	F	T	F

Table 16-20 Cisco IOS V2/V3 Trap Registry Parameters (continued)

Short Description	Event Type	Event Subtype	Expedites Polling	Event Source (IMO Name)	Activate Flow	Correlate	Is Correlation Allowed	Weight	Auto Clear	Severity	Is Ticketable	Auto Remove	Flapping
Vlan trunk port dynamic status changed to not trunking	vlan-trunk-port-dynamic-status	not trunking	N	IPortLayer1	F	T	F	0	F	wrn	F	T	F
cps Secure MacAddr Violation Trap	cps-Secure-MacAddr-Violation-Trap	cps-Secure-MacAddr-Violation-Trap	N	IPortLayer1	F	F	T	0	F	maj	T	T	F
cps IfVlan Secure MacAddr Violation Trap	cps-IfVlan-Secure-MacAddr-Violation-Trap	cps-IfVlan-Secure-MacAddr-Violation-Trap	N	IPortLayer1	F	F	T	0	F	maj	T	T	F
cisco L2 Control VlanMacLimit Notif Trap	cisco-L2-Control-VlanMacLimit-Notifs-Trap	clc VlanMacLimit Notif	N	IPortLayer1	F	F	F	0	F	info	F	T	F
cisco L2 Control VlanMacLimit High Notif Trap	cisco-L2-Control-VlanMacLimit-Notifs-Trap	clc VlanMacLimit High Notif	N	IPortLayer1	F	F	F	0	F	info	F	T	F
cisco L2 Control IfMacLimit Low Notif Trap	cisco-L2-Control-IfMacLimit-Notifs-Trap	clc IfMacLimit Low Notif	N	IPortLayer1	F	F	F	0	F	info	F	T	F
cisco L2 Control IfMacLimit High Notif Trap	cisco-L2-Control-IfMacLimit-Notifs-Trap	clc IfMacLimit High Notif	N	IPortLayer1	F	F	F	0	F	info	F	T	F
cisco L2 Control IfVlanMacLimit Low Notif Trap	cisco-L2-Control-IfVlanMacLimit-Notifs-Trap	clc IfVlanMacLimit Low Notif	N	IPortLayer1	F	F	F	0	F	info	F	T	F
cisco L2 Control IfVlanMacLimit High Notif Trap	cisco-L2-Control-IfVlanMacLimit-Notifs-Trap	clc IfVlanMacLimit High Notif	N	IPortLayer1	F	F	F	0	F	info	F	T	F
Cisco SBC source alert off trap	cisco sbc source alert trap	off	N	ISbcService	F	F	F	0	F	clr	F	T	F

Table 16-20 Cisco IOS V2/V3 Trap Registry Parameters (continued)

Short Description	Event Type	Event Subtype	Expedites Polling	Event Source (IMO Name)	Activate Flow	Correlate	Is Correlation Allowed	Weight	Auto Clear	Severity	Is Ticketable	Auto Remove	Flapping
Cisco SBC source alert on trap	cisco sbc source alert trap	on	N	ISbcService	F	F	F	0	F	wrn	T	T	F
Cisco SBC source alert informational trap	cisco sbc source alert trap	informational	N	ISbcService	F	F	F	0	F	info	F	T	F
Cisco SBC dynamic blacklist trap	cisco sbc dynamic blacklist trap	cisco sbc dynamic blacklist trap	N	ISbcService	F	F	F	0	F	info	F	T	F
Cisco SBC adjacency state up trap	cisco sbc adjacency state change trap	up	N	ISbcService	F	F	F	0	F	clr	F	T	F
Cisco SBC adjacency state down trap	cisco sbc adjacency state change trap	down	N	ISbcService	F	F	F	0	F	maj	T	T	F
Cisco SBC adjacency state informational trap	cisco sbc adjacency state change trap	informational	N	ISbcService	F	F	F	0	F	info	F	T	F
Cisco SBC service state up trap	cisco sbc service state change trap	up	sbc	ISbcService	F	F	F	0	F	clr	F	T	F
Cisco SBC service state down trap	cisco sbc service state change trap	down	sbc	ISbcService	F	F	F	0	F	cri	T	T	F
Cisco SBC service state informational trap	cisco sbc service state change trap	informational	sbc	ISbcService	F	F	F	0	F	info	F	T	F
Cisco SBC system congestion cleared trap	cisco sbc system congestion trap	cleared	N	ISbcService	F	F	F	0	F	clr	F	T	F
Cisco SBC system congestion raised trap	cisco sbc system congestion trap	raised	N	ISbcService	F	F	F	0	F	wrn	T	T	F

Table 16-20 Cisco IOS V2/V3 Trap Registry Parameters (continued)

Short Description	Event Type	Event Subtype	Expedites Polling	Event Source (IMO Name)	Activate Flow	Correlate	Is Correlation Allowed	Weight	Auto Clear	Severity	Is Ticketable	Auto Remove	Flapping
Cisco SBC system congestion informational trap	cisco sbc system congestion trap	informational	N	ISbcService	F	F	F	0	F	info	F	T	F
Cisco SBC SLA violation off trap	cisco sbc sla violation trap	off	N	ISbcService	F	F	F	0	F	clr	F	T	F
Cisco SBC SLA violation on trap	cisco sbc sla violation trap	on	N	ISbcService	F	F	F	0	F	min	T	T	F
Cisco SBC SLA violation informational trap	cisco sbc sla violation trap	informational	N	ISbcService	F	F	F	0	F	info	F	T	F
Cisco SBC radius connection state up trap	cisco sbc radius connection state change trap	up	N	ISbcService	F	F	F	0	F	clr	F	T	F
Cisco SBC radius connection state down trap	cisco sbc radius connection state change trap	down	N	ISbcService	F	F	F	0	F	maj	T	T	F
Cisco SBC radius connection state informational trap	cisco sbc radius connection state change trap	informational	N	ISbcService	F	F	F	0	F	info	F	T	F
Cisco SBC H248 controller state up trap	cisco sbc h248 controller state change trap	up	N	ISbcService	F	F	F	0	F	clr	F	T	F
Cisco SBC H248 controller state down trap	cisco sbc h248 controller state change trap	down	N	ISbcService	F	F	F	0	F	wrn	T	T	F

Table 16-20 Cisco IOS V2/V3 Trap Registry Parameters (continued)

Short Description	Event Type	Event Subtype	Expedites Polling	Event Source (IMO Name)	Activate Flow	Correlate	Is Correlation Allowed	Weight	Auto Clear	Severity	Is Ticketable	Auto Remove	Flapping
Cisco SBC H248 controller state informational trap	cisco sbc h248 controller state change trap	informational	N	ISbcService	F	F	F	0	F	info	F	T	F
RTT Connection Change	RTT Connection Change	RTT Connection Change	N	IManagedElement	F	F	F	0	F	info	T	T	F
RTT Operation Timeout	RTT Operation Timeout	RTT Operation Timeout	N	IManagedElement	F	F	F	0	F	info	T	T	F
RTT Operation Threshold Violation	RTT Operation Threshold Violation	RTT Operation Threshold Violation	N	IManagedElement	F	F	F	0	F	info	T	T	F
RTT Verify Error	RTT Verify Error	RTT Verify Error	N	IManagedElement	F	F	F	0	F	info	T	T	F
RTT threshold violation or clearance	rtt threshold violation or clearance	rtt threshold violation or clearance	N	IManagedElement	F	F	F	0	F	info	T	T	F
RTT Lpd Discovery	RTT Lpd Discovery	RTT Lpd Discovery	N	IManagedElement	F	F	F	0	F	info	T	T	F
RTT Lpd Grp Status	RTT Lpd Grp Status	RTT Lpd Grp Status	N	IManagedElement	F	F	F	0	F	info	T	T	F
IMA Group Remote Failure	IMA Group Failure trap	IMA Group Remote Failure	mtop-ima-group-state,port-status	ImaGroup Oid	F	F	F	0	T	min	F	T	T
IMA Group Remote insufficient links trap	IMA Group Failure trap	IMA Group Remote insufficient links trap	mtop-ima-group-state,port-status	ImaGroup Oid	F	F	F	0	T	maj	F	T	T
IMA Group Up Trap	IMA Group Failure trap	IMA Group Up Trap	mtop-ima-group-state,port-status	ImaGroup Oid	F	F	F	0	F	clr	F	T	T
IMA Group local Failure	IMA Group Failure trap	IMA Group local Failure	mtop-ima-group-state,port-status	ImaGroup Oid	F	F	F	0	T	min	F	T	T
IMA Group local insufficient links trap	IMA Group Failure trap	IMA Group local insufficient links trap	mtop-ima-group-state,port-status	ImaGroup Oid	F	F	F	0	T	maj	F	T	T

Table 16-20 Cisco IOS V2/V3 Trap Registry Parameters (continued)

Short Description	Event Type	Event Subtype	Expedites Polling	Event Source (IMO Name)	Activate Flow	Correlate	Is Correlation Allowed	Weight	Auto Clear	Severity	Is Ticketable	Auto Remove	Flapping
Ima Link Loss of delay Frame Trap	IMA Link Failure trap	Ima Link Loss of delay Frame Trap	mtop-ima-group-state ,port-status	ImaGroup Oid	F	F	F	0	T	min	F	T	T
Ima Link Loss of ima Frame Trap	IMA Link Failure trap	Ima Link Loss of ima Frame Trap	mtop-ima-group-state ,port-status	ImaGroup Oid	F	T	F	0	T	min	F	T	T
Ima Link Rcv Failure Trap	IMA Link Failure trap	Ima Link Rcv Failure Trap	mtop-ima-group-state ,port-status	ImaGroup Oid	F	T	F	0	T	min	F	T	T
Ima Link Remote Failure Trap	IMA Link Failure trap	Ima Link Remote Failure Trap	mtop-ima-group-state ,port-status	ImaGroup Oid	F	T	F	0	T	min	F	T	T
Ima Link Up Trap	IMA Link Failure trap	Ima Link Up Trap	mtop-ima-group-state ,port-status	ImaGroup Oid	F	F	F	0	F	clr	F	T	T
Ima Link Xmt Failure Trap	IMA Link Failure trap	Ima Link Xmt Failure Trap	mtop-ima-group-state ,port-status	ImaGroup Oid	F	T	F	0	T	min	F	T	T
Cisco UMT state Change trap	Cisco UMT state Change trap	Cisco UMT state Change trap	N/A	PortLayer1 Oid	F	F	F	0	F	info	F	T	F
Cisco GSM state Change trap	Cisco GSM state Change trap	Cisco GSM state Change trap	N/A	PortLayer1 Oid	F	F	F	0	F	info	F	T	F
IPRAN Backhaul Received Util Acceptable Trap	IPRAN Backhaul Received Util Trap	IPRAN Backhaul Received Util Acceptable Trap	N/A	PortLayer1 Oid	F	F	F	0	F	clr	F	T	F
IPRAN Backhaul Received Util Warning Trap	IPRAN Backhaul Received Util Trap	IPRAN Backhaul Received Util Warning Trap	N/A	PortLayer1 Oid	F	F	F	0	T	wrn	F	T	F
IPRAN Backhaul Received Util Overloaded Trap	IPRAN Backhaul Received Util Trap	IPRAN Backhaul Received Util Overloaded Trap	N/A	PortLayer1 Oid	F	F	F	0	T	maj	F	T	F

Table 16-20 Cisco IOS V2/V3 Trap Registry Parameters (continued)

Short Description	Event Type	Event Subtype	Expedites Polling	Event Source (IMO Name)	Activate Flow	Correlate	Is Correlation Allowed	Weight	Auto Clear	Severity	Is Ticketable	Auto Remove	Flapping
IPRAN Backhaul Sent Util Acceptable Trap	IPRAN Backhaul Sent Util Trap	IPRAN Backhaul Sent Util Acceptable Trap	N/A	PortLayer1 Oid	F	F	F	0	F	clr	F	T	F
IPRAN Backhaul Sent Util Overloaded Trap	IPRAN Backhaul Sent Util Trap	IPRAN Backhaul Sent Util Overloaded Trap	N/A	PortLayer1 Oid	F	F	F	0	T	wrn	F	T	F
IPRAN Backhaul Sent Util Warning Trap	IPRAN Backhaul Sent Util Trap	IPRAN Backhaul Sent Util Warning Trap	N/A	PortLayer1 Oid	F	F	F	0	T	maj	F	T	F
Connection Loss detected by ipsla icmp echo trap	ipsla echo connloss trap	connection loss detected by ipsla icmp echo trap	N/A	ManagedElement	F	F	F	0	F	info	T	T	F
Connection re-establish detected by ipsla icmp echo trap	ipsla echo connloss trap	connection re-establish detected by ipsla icmp echo trap	N/A	ManagedElement	F	F	F	0	F	info	F	T	F
Timeout detected by ipsla icmp echo trap	ipsla ip or lsp echo timeout trap	timeout detected by ipsla icmp echo trap	N/A	ManagedElement	F	F	F	0	F	info	F	T	F
Connection re-establish detected by ipsla icmp echo trap	ipsla ip or lsp echo timeout trap	connection re-establish detected by ipsla icmp echo trap	N/A	ManagedElement	F	F	F	0	F	info	F	T	F
Threshold crossing under trap	ipsla threshold notification trap	threshold crossing under trap	N/A	ManagedElement	F	F	F	0	F	info	F	T	F
Threshold crossing over trap	ipsla threshold notification trap	threshold crossing over trap	N/A	ManagedElement	F	F	F	0	F	info	F	T	F

Table 16-20 Cisco IOS V2/V3 Trap Registry Parameters (continued)

Short Description	Event Type	Event Subtype	Expedites Polling	Event Source (IMO Name)	Activate Flow	Correlate	Is Correlation Allowed	Weight	Auto Clear	Severity	Is Ticketable	Auto Remove	Flapping
Data corruption in rtt operation trap	ipsla threshold notification trap	data corruption in rtt operation trap	N/A	ManagedElement	F	F	F	0	F	info	F	T	F
Data corruption cleared in rtt operation trap	ipsla threshold notification trap	data corruption cleared in rtt operation trap	N/A	ManagedElement	F	F	F	0	F	info	F	T	F
Connection Loss detected by ipsla icmp echo trap	ipsla echo connloss trap	connection loss detected by ipsla icmp echo trap	N/A	ManagedElement	F	F	F	0	F	info	T	T	F
Connection Loss detected by ipsla LSP icmp echo trap	ipsla echo connloss trap	connection loss detected by ipsla lsp icmp echo trap	N/A	ManagedElement	F	F	F	0	F	info	T	T	F
Connection re-establish detected by ipsla icmp echo trap	ipsla echo connloss trap	connection re-establish detected by ipsla icmp echo trap	N/A	ManagedElement	F	F	F	0	F	info	F	T	F
Connection re-establish detected by ipsla LSP icmp echo trap	ipsla echo connloss trap	connection re-establish detected by ipsla lsp icmp echo trap	N/A	ManagedElement	F	F	F	0	F	clr	F	T	F
Timeout detected by ipsla icmp echo trap	ipsla echo timeout trap	timeout detected by ipsla icmp echo trap	N/A	ManagedElement	F	F	F	0	F	maj	T	T	F
Timeout detected by ipsla LSP icmp echo trap	ipsla echo timeout trap	timeout detected by ipsla lsp icmp echo trap	N/A	ManagedElement	F	F	F	0	F	maj	T	T	F

Table 16-20 Cisco IOS V2/V3 Trap Registry Parameters (continued)

Short Description	Event Type	Event Subtype	Expedites Polling	Event Source (IMO Name)	Activate Flow	Correlate	Is Correlation Allowed	Weight	Auto Clear	Severity	Is Ticketable	Auto Remove	Flapping
Connection re-establish detected by ipsla icmp echo trap	ipsla echo timeout trap	connection re-establish detected by ipsla icmp echo trap	N/A	ManagedElement	F	F	F	0	F	info	F	T	F
Connection re-establish detected by ipsla LSP icmp echo trap	ipsla echo timeout trap	connection re-establish detected by ipsla lsp icmp echo trap	N/A	ManagedElement	F	F	F	0	F	clr	F	T	F
RTT threshold crossing over trap	ipsla echo rtt trap	rtt threshold crossing over trap	N/A	ManagedElement	F	F	F	0	F	info	F	T	F
RTT threshold crossing under trap	ipsla echo rtt trap	rtt threshold crossing under trap	N/A	ManagedElement	F	F	F	0	F	info	F	T	F
IPSLA LSP path discovery failure trap	ipsla lpd discovery trap	ipsla lsp path discovery failure trap	N/A	ManagedElement	F	F	F	0	F	maj	T	T	F
IPSLA LSP path rediscovery trap	ipsla lpd discovery trap	ipsla lsp path rediscovery trap	N/A	ManagedElement	F	F	F	0	F	clr	F	T	F
IPSLA LDP group status failure trap	ipsla lpd group status trap	ipsla ldp group status failure trap	N/A	ManagedElement	F	F	F	0	F	maj	T	T	F
IPSLA LDP group status restoration trap	ipsla lpd group status trap	ipsla ldp group status restoration trap	N/A	ManagedElement	F	F	F	0	F	clr	F	T	F
FRR Protected Trap	frr trigger trap	frr protected trap	N/A	PortLayer1	F	T	F	0	F	info	F	T	F
FRR Unprotected Trap	frr trigger trap	frr unprotected trap	N/A	PortLayer1	F	T	F	0	F	info	F	T	F
Pseudo wire tunnel up	pseudo wire tunnel traps	Pseudo wire tunnel up	ce-pw-tunnel-status-snmp, ce-vfi-status-telnet	IPTPLayer2MplsTunnel	F	F	F	0	F	clr	F	T	T

Table 16-20 Cisco IOS V2/V3 Trap Registry Parameters (continued)

Short Description	Event Type	Event Subtype	Expedites Polling	Event Source (IMO Name)	Activate Flow	Correlate	Is Correlation Allowed	Weight	Auto Clear	Severity	Is Ticketable	Auto Remove	Flapping
Pseudo wire tunnel down	pseudo wire tunnel traps	Pseudo wire tunnel down	ce-pw-tunnel-status-snmp, ce-vfi-status-telnet	IPTPLayer2MplsTunnel	F	T	F	0	T	min	F	T	T
REP port state fully operational Trap	REP port operational state change	REP port state fully operational	N/A	IREPService	F	F	F	0	F	clr	F	T	F
REP port state not operational Trap	REP port operational state change	REP port state not operational	N/A	IREPService	F	T	F	0	T	min	F	T	F
REP port role failed Trap	REP port role change trap	REP port role failed	N/A	IREPService	F	T	F	0	F	min	T	T	F
REP port role clear Trap	REP port role change trap	REP port role clear	N/A	IREPService	F	F	F	0	F	clr	F	T	F
Cisco Sonet vt status changed to error	sonet vt status changed	sonet vt status changed to error	N	IPortLayer1	F	T	F	0	F	maj	T	T	T
Cisco Sonet vt status changed to clear	sonet vt status changed	sonet vt status changed to clear	N	IPortLayer1	F	F	F	0	F	clr	F	T	T
CFM cc mep up trap	cisco cfm cc mep down trap	mep up	N/A	ICfmServiceOid	F	F	F	0	F	clr	F	T	F
CFM cc mep down due to timeout trap	cisco cfm cc mep down trap	lastgap	N/A	ICfmServiceOid	F	T	F	0	T	minor	F	T	F
CFM cc mep down due to last gasp trap	cisco cfm cc mep down trap	lastgap	N/A	ICfmServiceOid	F	T	F	0	T	minor	F	T	F
CFM cc cross-connected service error trap	cisco cfm cc cross-connected service error trap	cross-connected service error trap	N/A	ICfmServiceOid	F	F	F	0	F	info	F	T	F

Table 16-20 Cisco IOS V2/V3 Trap Registry Parameters (continued)

Short Description	Event Type	Event Subtype	Expedites Polling	Event Source (IMO Name)	Activate Flow	Correlate	Is Correlation Allowed	Weight	Auto Clear	Severity	Is Ticketable	Auto Remove	Flapping
CFM cc cross-connected service error trap clear	cisco cfm cc cross-connected service error trap	cross-connected service error trap clear	N/A	ICfmServiceOid	F	F	F	0	F	clr	F	T	F
CFM cc loop trap	cisco cfm cc loop trap	loop trap	N/A	ICfmServiceOid	F	F	F	0	F	info	F	T	F
CFM cc loop trap clear	cisco cfm cc loop trap	loop trap clear	N/A	ICfmServiceOid	F	F	F	0	F	clr	F	T	F
CFM cc config error trap	cisco cfm cc config error trap	config error trap	N/A	ICfmServiceOid	F	T	F	0	F	info	F	T	F
CFM cc config error trap clear	cisco cfm cc config error trap	config error trap clear	N/A	ICfmServiceOid	F	F	F	0	F	clr	F	T	F
CFM crossconnect mep missing trap	cisco cfm crossconnect mep missing trap	mep missing trap	N/A	ICfmServiceOid	F	T	F	0	T	minor	F	T	F
CFM crossconnect mep unknown trap	cisco cfm crossconnect mep unknown trap	mep unknown trap	N/A	ICfmServiceOid	F	T	F	0	T	minor	F	T	F
CFM crossconnect mep unknown trap clear	cisco cfm crossconnect mep unknown trap	mep unknown trap clear	N/A	ICfmServiceOid	F	F	F	0	F	clr	F	T	F
CFM crossconnect mep service up trap	cisco cfm crossconnect mep service up trap	mep service up trap	N/A	ICfmServiceOid	F	F	F	0	F	clr	F	T	F
Vrrp trap auth failure trap	vrrp trap auth failure trap	vrrp trap auth failure trap	N	IManagedElement	F	F	F	0	T	minor	F	T	F
Vrrp trap new master trap	vrrp trap new master trap	vrrp trap new master trap	N	IManagedElement	F	F	F	0	T	minor	F	T	F

Table 16-20 Cisco IOS V2/V3 Trap Registry Parameters (continued)

Short Description	Event Type	Event Subtype	Expedites Polling	Event Source (IMO Name)	Activate Flow	Correlate	Is Correlation Allowed	Weight	Auto Clear	Severity	Is Ticketable	Auto Remove	Flapping
OAM Non-threshold crossing link fault trap	OAM non-threshold crossing trap	linkFault	oam	IPhysicalLayer	F	T	F	0	F	info	F	T	F
OAM Non-threshold crossing dying gasp trap	OAM non-threshold crossing trap	dyingGaspEvent	oam	IPhysicalLayer	F	T	F	0	F	info	F	T	F
OAM Non-threshold crossing critical Link trap	OAM non-threshold crossing trap	criticalLinkEvent	oam	IPhysicalLayer	F	T	F	0	F	info	F	T	F
OAM threshold errored Symbol trap	OAM threshold crossing trap	erroredSymbolEvent	oam	IPhysicalLayer	F	T	F	0	F	info	F	T	F
OAM threshold errored Frame Period trap	OAM threshold crossing trap	erroredFramePeriodEvent	oam	IPhysicalLayer	F	T	F	0	F	info	F	T	F
OAM threshold errored Frame trap	OAM threshold crossing trap	erroredFrameEvent	oam	IPhysicalLayer	F	T	F	0	F	info	F	T	F
OAM threshold errored Frame Seconds trap	OAM threshold crossing trap	erroredFrameSecondsEvent	oam	IPhysicalLayer	F	T	F	0	F	info	F	T	F
Power Supply - Critical	cisco-EnvMon-Supply-State-Notification-Trap	critical	N	IManagedElement	F	F	F	0	F	cri	T	T	F
Power Supply - Normal	cisco-EnvMon-Supply-State-Notification-Trap	normal	N	IManagedElement	F	F	F	0	F	clr	T	T	F
Power Supply - Not Functioning	cisco-EnvMon-Supply-State-Notification-Trap	notFunctioning	N	IManagedElement	F	F	F	0	F	maj	T	T	F

Table 16-20 Cisco IOS V2/V3 Trap Registry Parameters (continued)

Short Description	Event Type	Event Subtype	Expedites Polling	Event Source (IMO Name)	Activate Flow	Correlate	Is Correlation Allowed	Weight	Auto Clear	Severity	Is Ticketable	Auto Remove	Flapping
Power Supply - Not Present	cisco-EnvMon-Supply-State-Notification-Trap	notPresent	N	IManagedElement	T	F	F	0	F	maj	T	T	F
Power Supply - Shutdown	cisco-EnvMon-Supply-State-Notification-Trap	shutdown	N	IManagedElement	F	F	F	0	F	cri	T	T	F
Power Supply - Warning	cisco-EnvMon-Supply-State-Notification-Trap	warning	N	IManagedElement	F	F	F	0	F	wrn	T	T	F

Cisco IOX V1 Trap Registry Parameters

Table 16-21 lists the associated event types, event subtypes, and Prime Network registry parameters for the Cisco IOX SNMP V1 traps shown in Table 16-5.

Table 16-21 Cisco IOX V1 Trap Registry Parameters

Short Description	Event Type	Event Subtype	Expedites Polling	Event Source (IMO Name)	Activate Flow	Correlate	Is Correlation Allowed	Weight	Auto Clear	Severity	Is Ticketable	Auto Remove	Flapping
Pseudo wire tunnel up	pseudo wire tunnel traps	Pseudo wire tunnel up	ce-pw-tunnels-status-trap	IPTPLayer2MplsTunnel	F	F	F	0	F	clr	F	T	T
Pseudo wire tunnel down	pseudo wire tunnel traps	Pseudo wire tunnel down	ce-pw-tunnels-status-trap	IPTPLayer2MplsTunnel	F	T	F	0	T	min	F	T	T
SNMP Link down	snmp link down	snmp link down	Y	IPhysicalLayer	F	T	F	0	T	min	F	T	T
SNMP Link up	snmp link down	snmp link up	Y	IPhysicalLayer	F	T	F	0	F	clr	F	T	T

Table 16-21 Cisco IOX V1 Trap Registry Parameters (continued)

Short Description	Event Type	Event Subtype	Expedites Polling	Event Source (IMO Name)	Activate Flow	Correlate	Is Correlation Allowed	Weight	Auto Clear	Severity	Is Ticketable	Auto Remove	Flapping
Connection Loss detected by ipsla icmp echo trap	ipsla echo connloss trap	connection loss detected by ipsla icmp echo trap	N/A	ManagedElement	F	F	F	0	F	maj	T	T	F
Connection re-establish detected by ipsla icmp echo trap	ipsla echo connloss trap	connection re-establish detected by ipsla icmp echo trap	N/A	ManagedElement	F	F	F	0	F	clr	F	T	F
Timeout detected by ipsla icmp echo trap	ipsla ip or lsp echo timeout trap	timeout detected by ipsla icmp echo trap	N/A	ManagedElement	F	F	F	0	F	info	F	T	F
Connection re-establish detected by ipsla icmp echo trap	ipsla ip or lsp echo timeout trap	connection re-establish detected by ipsla icmp echo trap	N/A	ManagedElement	F	F	F	0	F	info	F	T	F
Threshold crossing under trap	ipsla threshold notification trap	threshold crossing under trap	N/A	ManagedElement	F	F	F	0	F	info	F	T	F
Threshold crossing over trap	ipsla threshold notification trap	threshold crossing over trap	N/A	ManagedElement	F	F	F	0	F	info	F	T	F
Data corruption in rtt operation trap	ipsla threshold notification trap	data corruption in rtt operation trap	N/A	ManagedElement	F	F	F	0	F	info	F	T	F
Data corruption cleared in rtt operation trap	ipsla threshold notification trap	data corruption cleared in rtt operation trap	N/A	ManagedElement	F	F	F	0	F	info	F	T	F
Connection Loss detected by ipsla icmp echo trap	ipsla echo connloss trap	connection loss detected by ipsla icmp echo trap	N/A	ManagedElement	F	F	F	0	F	maj	T	T	F

Table 16-21 Cisco IOX V1 Trap Registry Parameters (continued)

Short Description	Event Type	Event Subtype	Expedites Polling	Event Source (IMO Name)	Activate Flow	Correlate	Is Correlation Allowed	Weight	Auto Clear	Severity	Is Ticketable	Auto Remove	Flapping
Connection Loss detected by ipsla LSP icmp echo trap	ipsla echo connloss trap	connection loss detected by ipsla lsp icmp echo trap	N/A	ManagedElement	F	F	F	0	F	maj	T	T	F
Connection re-establish detected by ipsla icmp echo trap	ipsla echo connloss trap	connection re-establish detected by ipsla icmp echo trap	N/A	ManagedElement	F	F	F	0	F	clr	F	T	F
Connection re-establish detected by ipsla LSP icmp echo trap	ipsla echo connloss trap	connection re-establish detected by ipsla lsp icmp echo trap	N/A	ManagedElement	F	F	F	0	F	clr	F	T	F
Timeout detected by ipsla icmp echo trap	ipsla echo timeout trap	timeout detected by ipsla icmp echo trap	N/A	ManagedElement	F	F	F	0	F	maj	T	T	F
Timeout detected by ipsla LSP icmp echo trap	ipsla echo timeout trap	timeout detected by ipsla lsp icmp echo trap	N/A	ManagedElement	F	F	F	0	F	maj	T	T	F
Connection re-establish detected by ipsla icmp echo trap	ipsla echo timeout trap	connection re-establish detected by ipsla icmp echo trap	N/A	ManagedElement	F	F	F	0	F	clr	F	T	F
Connection re-establish detected by ipsla LSP icmp echo trap	ipsla echo timeout trap	connection re-establish detected by ipsla lsp icmp echo trap	N/A	ManagedElement	F	F	F	0	F	clr	F	T	F
RTT threshold crossing over trap	ipsla echo rtt trap	rtt threshold crossing over trap	N/A	ManagedElement	F	F	F	0	F	info	F	T	F
RTT threshold crossing under trap	ipsla echo rtt trap	rtt threshold crossing under trap	N/A	ManagedElement	F	F	F	0	F	info	F	T	F
IPSLA LSP path discovery failure trap	ipsla lpd discover y trap	ipsla lsp path discovery failure trap	N/A	ManagedElement	F	F	F	0	F	maj	T	T	F

Table 16-21 Cisco IOX V1 Trap Registry Parameters (continued)

Short Description	Event Type	Event Subtype	Expedites Polling	Event Source (IMO Name)	Activate Flow	Correlate	Is Correlation Allowed	Weight	Auto Clear	Severity	Is Ticketable	Auto Remove	Flapping
IPSLA LSP path rediscovery trap	ipsla lpd discovery trap	ipsla lsp path rediscovery trap	N/A	ManagedElement	F	F	F	0	F	clr	F	T	F
IPSLA LDP group status failure trap	ipsla lpd group status trap	ipsla ldp group status failure trap	N/A	ManagedElement	F	F	F	0	F	maj	T	T	F
IPSLA LDP group status restoration trap	ipsla lpd group status trap	ipsla ldp group status restoration trap	N/A	ManagedElement	F	F	F	0	F	clr	F	T	F
FRR Protected Trap	frr trigger trap	frr protected trap	N/A	PortLayer1	F	T	F	0	F	info	F	T	F
FRR Unprotected Trap	frr trigger trap	frr unprotected trap	N/A	PortLayer1	F	T	F	0	F	info	F	T	F
Pseudo wire tunnel up	pseudo wire tunnel traps	Pseudo wire tunnel up	ce-pw-tunnels-status-trap	IPTPLayer2 MplsTunnel	F	F	F	0	F	clr	F	T	T
Pseudo wire tunnel down	pseudo wire tunnel traps	Pseudo wire tunnel down	ce-pw-tunnels-status-trap	IPTPLayer2 MplsTunnel	F	T	F	0	T	min	F	T	T
DSX1 Far end LOF	dsx1 line status change	RcvFarEndLOF	Y	IPhysicalLayer	F	T	F	0	T	maj	F	T	F
DSX1 Near end sending LOF Indication	dsx1 line status change	XmtFarEndLOF	Y	IPhysicalLayer	F	T	F	0	T	maj	F	T	F
DSX1 Far end sending AIS	dsx1 line status change	RcvAIS	Y	IPhysicalLayer	F	T	F	0	T	wrn	F	T	F
DSX1 Near end sending AIS	dsx1 line status change	XmtAIS	Y	IPhysicalLayer	F	T	F	0	T	wrn	F	T	F
DSX1 Near end LOF	dsx1 line status change	LossOfFrame	Y	IPhysicalLayer	F	T	F	0	T	maj	F	T	F

Table 16-21 Cisco IOX V1 Trap Registry Parameters (continued)

Short Description	Event Type	Event Subtype	Expedites Polling	Event Source (IMO Name)	Activate Flow	Correlate	Is Correlation Allowed	Weight	Auto Clear	Severity	Is Ticketable	Auto Remove	Flapping
DSX1 Near end Loss of Signal	dsx1 line status change	LossOfSignal	Y	IPhysicalLayer	F	T	F	0	T	maj	F	T	F
DSX1 Near end is looped	dsx1 line status change	LoopbackState	Y	IPhysicalLayer	F	T	F	0	T	maj	F	T	F
DSX1 E1 TS16 AIS	dsx1 line status change	T16AIS	Y	IPhysicalLayer	F	T	F	0	T	wrn	F	T	F
DSX1 Far End Sending TS16 LOMF	dsx1 line status change	RcvFarEndLOMF	Y	IPhysicalLayer	F	T	F	0	T	maj	F	T	F
DSX1 Near End Sending TS16 LOMF	dsx1 line status change	XmtFarEndLOMF	Y	IPhysicalLayer	F	T	F	0	T	maj	F	T	F
DSX1 Near End detects a test code	dsx1 line status change	RcvTestCode	Y	IPhysicalLayer	F	T	F	0	T	maj	F	T	F
DSX1 any line status not defined here	dsx1 line status change	OtherFailure	Y	IPhysicalLayer	F	T	F	0	T	min	F	T	F
DSX1 Near End in Unavailable Signal State	dsx1 line status change	UnavailSigState	Y	IPhysicalLayer	F	T	F	0	T	maj	F	T	F
DSX1 Carrier Equipment Out of Service	dsx1 line status change	NetEquipOOS	Y	IPhysicalLayer	F	T	F	0	T	maj	F	T	F
DSX1 DS2 Payload AIS	dsx1 line status change	RcvPayloadAIS	Y	IPhysicalLayer	F	T	F	0	T	wrn	F	T	F
DSX1 DS2 Performance Threshold Exceeded	dsx1 line status change	Ds2PerfThreshold	Y	IPhysicalLayer	F	T	F	0	T	maj	F	T	F
DSX1 combination of bitmaps due to multiple failures	dsx1 line status change	MultipleFailures	Y	IPhysicalLayer	F	T	F	0	T	maj	F	T	F
DSX1 No alarm present	dsx1 line status change	NoAlarm	Y	IPhysicalLayer	F	T	F	0	F	clr	F	T	F

Table 16-21 Cisco IOX V1 Trap Registry Parameters (continued)

Short Description	Event Type	Event Subtype	Expedites Polling	Event Source (IMO Name)	Activate Flow	Correlate	Is Correlation Allowed	Weight	Auto Clear	Severity	Is Ticketable	Auto Remove	Flapping
DSX3 Receiving Yellow/Remote Alarm Indication	dsx3 line status change	RcvRAIFailure	Y	IPhysicalLayer	F	T	F	0	T	maj	F	T	F
DSX3 Transmitting Yellow/Remote Alarm Indication	dsx3 line status change	XmitRAIAlarm	Y	IPhysicalLayer	F	T	F	0	T	maj	F	T	F
DSX3 Receiving AIS failure state	dsx3 line status change	RcvAIS	Y	IPhysicalLayer	F	T	F	0	T	wrn	F	T	F
DSX3 Transmitting AIS	dsx3 line status change	XmtAIS	Y	IPhysicalLayer	F	T	F	0	T	wrn	F	T	F
DSX3 Receiving LOF failure state	dsx3 line status change	LossOfFrame	Y	IPhysicalLayer	F	T	F	0	T	maj	F	T	F
DSX3 Receiving LOS failure state	dsx3 line status change	LossOfSignal	Y	IPhysicalLayer	F	T	F	0	T	maj	F	T	F
DSX3 Looping the received signal	dsx3 line status change	LoopbackState	Y	IPhysicalLayer	F	T	F	0	T	maj	F	T	F
DSX3 Receiving a Test Pattern	dsx3 line status change	RcvTestCode	Y	IPhysicalLayer	F	T	F	0	T	maj	F	T	F
DSX3 any line status not defined here	dsx3 line status change	OtherFailure	Y	IPhysicalLayer	F	T	F	0	T	min	F	T	F
DSX3 Near End in Unavailable Signal State	dsx3 line status change	UnavailSigState	Y	IPhysicalLayer	F	T	F	0	T	maj	F	T	F
DSX3 Carrier Equipment Out of Service	dsx3 line status change	NetEquipOOS	Y	IPhysicalLayer	F	T	F	0	T	maj	F	T	F
DSX3 combination of bitmaps due to multiple failures	dsx3 line status change	MultipleFailures	Y	IPhysicalLayer	F	T	F	0	T	maj	F	T	F
DSX3 No alarm present	dsx3 line status change	NoAlarm	Y	IPhysicalLayer	F	T	F	0	F	clr	F	T	F

Table 16-21 Cisco IOX V1 Trap Registry Parameters (continued)

Short Description	Event Type	Event Subtype	Expedites Polling	Event Source (IMO Name)	Activate Flow	Correlate	Is Correlation Allowed	Weight	Auto Clear	Severity	Is Ticketable	Auto Remove	Flapping
Entity table configuration changed	Entity table configuration changed	Entity table configuration changed	N	IManagedElement	F	F	T	0	F	info	F	T	F
FR DLCI status invalid trap	fr dlci status change trap	fr dlci status invalid trap	N	IPortLayer1	T	F	F	0	F	maj	F	T	F
FR DLCI status inactive trap	fr dlci status change trap	fr dlci status inactive trap	N	IPortLayer1	T	F	F	0	F	maj	F	T	F
FR DLCI status active trap	fr dlci status change trap	fr dlci status active trap	N	IPortLayer1	T	F	F	0	F	clr	F	T	F
Cisco Sonet vt status changed to error	sonet vt status changed	sonet vt status changed to error	N	IPortLayer1	F	T	F	0	F	maj	T	T	T
Cisco Sonet vt status changed to clear	sonet vt status changed	sonet vt status changed to clear	N	IPortLayer1	F	F	F	0	F	clr	F	T	T
Vrrp trap auth failure trap	vrrp trap auth failure trap	vrrp trap auth failure trap	N	IManagedElement	F	F	F	0	T	minor	F	T	F
Vrrp trap new master trap	vrrp trap new master trap	vrrp trap new master trap	N	IManagedElement	F	F	F	0	T	minor	F	T	F
Cisco bfd session down trap	Cisco bfd session change trap	Cisco bfd session down trap	bfd session	BfdService	F	T	F	0	T	maj	F	T	F
Cisco bfd session up trap	Cisco bfd session change trap	Cisco bfd session up trap	bfd session	BfdService	F	F	F	0	F	clr	F	T	F

Table 16-21 Cisco IOX V1 Trap Registry Parameters (continued)

Short Description	Event Type	Event Subtype	Expedites Polling	Event Source (IMO Name)	Activate Flow	Correlate	Is Correlation Allowed	Weight	Auto Clear	Severity	Is Ticketable	Auto Remove	Flapping
Cisco BGP backward transition trap	cisco bgp trap	cisco bgp backward transition trap	N	IBgpNeighbourEntry	F	T	F	0	T	info	F	T	T
Cisco BGP down trap	cisco bgp trap	cisco bgp down trap	N	IBgpNeighbourEntry	F	T	T	0	T	maj	F	T	T
Cisco BGP established trap	cisco bgp trap	cisco bgp established trap	N	IBgpNeighbourEntry	F	F	F	0	T	clr	F	T	T
Config-copy request completion	cc copy completion	cc copy completion	N	IManagedElement	F	F	F	0	F	info	F	T	F
cfh bundle link status down	cfh bundle link status notification	cfh bundle link status down	N	IManagedElement	F	F	F	0	F	maj	F	T	T
cfh bundle link status up	cfh bundle link status notification	cfh bundle link status up	N	IManagedElement	F	F	F	0	F	clr	F	T	T
cfh Fabric bundle operational state changed to Down	cfh bundle state notification	cfh bundle state down	N	IManagedElement	F	F	F	0	F	maj	F	T	T
cfh Fabric bundle operational state changed to Up	cfh bundle state notification	cfh bundle state up	N	IManagedElement	F	F	F	0	F	clr	F	T	T
cfh Fabric plane status down	cfh plane state notification	cfh plane status down	N	IManagedElement	F	F	F	0	F	maj	F	T	T
cfh Fabric plane status up	cfh plane state notification	cfh plane status up	N	IManagedElement	F	F	F	0	F	clr	F	T	T

Table 16-21 Cisco IOX V1 Trap Registry Parameters (continued)

Short Description	Event Type	Event Subtype	Expedites Polling	Event Source (IMO Name)	Activate Flow	Correlate	Is Correlation Allowed	Weight	Auto Clear	Severity	Is Ticketable	Auto Remove	Flapping
Pseudo wire tunnel up	pseudo wire tunnel traps	Pseudo wire tunnel up	ce-pw-tunnel-status-snmp, ce-vfi-status-telnet	IPTPLayer2MplsTunnel	F	F	F	0	F	clr	F	T	T
Pseudo wire tunnel down	pseudo wire tunnel traps	Pseudo wire tunnel down	ce-pw-tunnel-status-snmp, ce-vfi-status-telnet	IPTPLayer2MplsTunnel	F	T	F	0	T	min	F	T	T
Cisco RF Swap Status - Unsupported	cisco RF swap notification trap	cisco RF status is unsupported	N	IManagedElement	F	F	F	0	F	info	F	T	F
Cisco RF Swap Status - None	cisco RF swap notification trap	cisco RF status is none	N	IManagedElement	F	F	F	0	F	info	F	T	F
Cisco RF Swap Status - Not Known	cisco RF swap notification trap	cisco RF status is notknown	N	IManagedElement	F	F	F	0	F	info	F	T	F
Cisco RF Swap Status - UserInitiated	cisco RF swap notification trap	cisco RF status is userInitiated	N	IManagedElement	F	F	F	0	F	info	F	T	F
Cisco RF Swap Status - UserForced	cisco RF swap notification trap	cisco RF status is userForced	N	IManagedElement	F	F	F	0	F	info	F	T	F
Cisco RF Swap Status - ActiveUnitFailed	cisco RF swap notification trap	cisco RF status is activeUnitFailed	N	IManagedElement	F	F	F	0	F	info	F	T	F
Cisco RF Swap Status - ActiveUnitRemoved	cisco RF swap notification trap	cisco RF status is activeUnitRemoved	N	IManagedElement	F	F	F	0	F	info	F	T	F
Atm interface PVC failures trap	Atm interface PVC failures trap	Atm interface PVC failures trap	N	IPhysicalLayer	T	T	F	0	T	min	F	T	F

Cisco IOX V2/V3 Trap Registry Parameters

Table 16-22 lists the associated event types, event subtypes, and Prime Network registry parameters for the Cisco IOX SNMP V2/V3 traps shown in Table 16-6.

Table 16-22 Cisco IOX V2/V3 Trap Registry Parameters

Short Description	Event Type	Event Subtype	Expedites Polling	Event Source (IMO Name)	Activate Flow	Correlate	Is Correlation Allowed	Weight	Auto Clear	Severity	Is Ticketable	Auto Remove	Flapping
CBF File operation state indicator	cbf define file completion	cbf define file completion	N	IManaged Element	F	F	F	0	F	info	F	T	F
Cisco BGP backward transition trap	cisco bgp trap	cisco bgp backward transition trap	N	IBgpNeighborEntry	F	T	F	0	T	info	F	T	T
Cisco BGP down trap	cisco bgp trap	cisco bgp down trap	N	IBgpNeighborEntry	F	T	T	0	T	maj	F	T	T
Cisco BGP established trap	cisco bgp trap	cisco bgp established trap	N	IBgpNeighborEntry	F	F	F	0	T	clr	F	T	T
Cisco BGP prefix threshold exceeded	cisco bgp prefix threshold exceeded	cisco bgp prefix threshold exceeded	N	IProfileContainer (BGP)	F	T	F	0	F	wrn	T	T	T
Cisco BGP prefix threshold clear	cisco bgp prefix threshold exceeded	cisco bgp prefix threshold clear	N	IProfileContainer (BGP)	F	F	F	0	F	clr	F	T	T
Config-copy request completion	cc copy completion	cc copy completion	N	IManaged Element	F	F	F	0	F	info	F	T	F
cefc fan-tray oper status down	cefc fan tray status changed	cefc fan status down	physical-command	IModule	F	T	T	0	T	cri	F	T	T
cefc fan-tray oper status up	cefc fan tray status changed	cefc fan status up	physical-command	IModule	F	F	F	0	T	clr	F	T	T
cefc FRU inserted	cefc fru removed	cefc fru inserted	physical-command	IModule	F	F	F	0	T	clr	F	T	T
cefc FRU removed	cefc fru removed	cefc fru removed	physical-command	IModule	F	T	T	0	T	maj	F	T	T
cefc module oper status down	cefc module oper status changed	cefc module oper down	physical-command	IModule	F	T	T	0	T	maj	F	F	T

Table 16-22 Cisco IOX V2/V3 Trap Registry Parameters (continued)

Short Description	Event Type	Event Subtype	Expedites Polling	Event Source (IMO Name)	Activate Flow	Correlate	Is Correlation Allowed	Weight	Auto Clear	Severity	Is Ticketable	Auto Remove	Flapping
cefc module oper status up	cefc module oper status changed	cefc module oper up	physical-command	IModule	F	F	F	0	F	clr	F	T	T
cefc power status down	cefc power status changed	cefc power status down	physical-command	IModule	F	T	T	0	T	maj	F	T	T
cefc power status up	cefc power status changed	cefc power status up	physical-command	IModule	F	F	F	0	F	clr	F	T	T
cfh bundle link status down	cfh bundle link status notification	cfh bundle link status down	N	IManaged Element	F	F	F	0	F	maj	F	T	T
cfh bundle link status up	cfh bundle link status notification	cfh bundle link status up	N	IManaged Element	F	F	F	0	F	clr	F	T	T
cfh Fabric bundle operational state changed to Down	cfh bundle state notification	cfh bundle state down	N	IManaged Element	F	F	F	0	F	maj	F	T	T
cfh Fabric bundle operational state changed to Up	cfh bundle state notification	cfh bundle state up	N	IManaged Element	F	F	F	0	F	clr	F	T	T
cfh Fabric plane status down	cfh plane state notification	cfh plane status down	N	IManaged Element	F	F	F	0	F	maj	F	T	T
cfh Fabric plane status up	cfh plane state notification	cfh plane status up	N	IManaged Element	F	F	F	0	F	clr	F	T	T
Cisco Configuration management event notification	cisco config man event	cisco config man event	N	IManaged Element	F	F	F	0	F	info	F	T	F
Cisco flash copy failed	cisco flash copy completed	cisco flash copy failed	N	IManaged Element	F	F	F	0	F	info	F	T	F
Cisco flash copy completion	cisco flash copy completed	cisco flash copy completed	N	IManaged Element	F	F	F	0	F	info	F	T	F
Cisco flash copy in progress	cisco flash copy completed	cisco flash copy in progress	N	IManaged Element	F	F	F	0	F	info	F	T	F

Table 16-22 Cisco IOX V2/V3 Trap Registry Parameters (continued)

Short Description	Event Type	Event Subtype	Expedites Polling	Event Source (IMO Name)	Activate Flow	Correlate	Is Correlation Allowed	Weight	Auto Clear	Severity	Is Ticketable	Auto Remove	Flapping
Cisco Flash device changed	cisco flash device changed	cisco flash device changed	N	IManaged Element	F	F	F	0	F	wrn	F	T	F
Cisco Flash device inserted	cisco flash device removed	cisco flash device inserted	N	IManaged Element	F	F	F	0	F	clr	F	T	T
Cisco Flash device removed	cisco flash device removed	cisco flash device removed	N	IManaged Element	F	F	F	0	F	wrn	F	T	T
Cisco Flash miscellaneous operation failed	cisco flash operation completed	cisco flash operation failed	N	IManaged Element	F	F	F	0	F	info	F	T	F
Cisco Flash miscellaneous operation completed	cisco flash operation completed	cisco flash operation completed	N	IManaged Element	F	F	F	0	F	info	F	T	F
Cisco Flash miscellaneous operation in progress	cisco flash operation completed	cisco flash operation in progress	N	IManaged Element	F	F	F	0	F	info	F	T	F
Cisco ping completion	cisco ping completion	cisco ping completion	N	IManaged Element	F	F	F	0	F	info	F	T	F
Cisco Sonet section status changed to error	sonet section status changed	sonet section status changed to error	N	IPortLayer 1	F	T	T	0	F	maj	F	T	T
Cisco Sonet section status changed to clear	sonet section status changed	sonet section status changed to clear	N	IPortLayer 1	F	F	F	0	F	clr	F	T	T
Cisco Sonet line status changed to error	sonet line status changed	sonet line status changed to error	N	IPortLayer 1	F	T	T	0	F	maj	F	T	T
Cisco Sonet line status changed to clear	sonet line status changed	sonet line status changed to clear	N	IPortLayer 1	F	F	F	0	F	clr	F	T	T
Cisco Sonet path status changed to error	sonet path status changed	sonet path status changed to error	N	IPortLayer 1	F	T	T	0	F	maj	F	T	T

Table 16-22 Cisco IOX V2/V3 Trap Registry Parameters (continued)

Short Description	Event Type	Event Subtype	Expedites Polling	Event Source (IMO Name)	Activate Flow	Correlate	Is Correlation Allowed	Weight	Auto Clear	Severity	Is Ticketable	Auto Remove	Flapping
Cisco Sonet path status changed to clear	sonet path status changed	sonet path status changed to clear	N	IPortLayer 1	F	F	F	0	F	clr	F	T	T
Cisco syslog message generated	cisco syslog message generated	cisco syslog message generated	N	IManaged Element	F	T	F	0	F	info	F	T	F
Cisco PIM neighbor lost	cisco pim neighbor lost	cisco pim neighbor lost	N	IRoutingEntry	F	T	T	0	F	info	T	T	T
sensor value crossed threshold in entSensorThresholdTable	entity sensor threshold notification	entity sensor threshold notification	N	IManaged Element	F	F	F	0	F	maj	T	T	T
RTT threshold violation or clearance	rtt threshold violation or clearance	rtt threshold violation or clearance	N	IManaged Element	F	F	F	0	F	info	T	T	F
Pseudo wire tunnel up	pseudo wire tunnel traps	Pseudo wire tunnel up	ce-pw-tunnel-status-snmp,ce-vfi-status-telnet	IPTPLayer 2MplsTunnel	F	F	F	0	F	clr	F	T	T
Pseudo wire tunnel down	pseudo wire tunnel traps	Pseudo wire tunnel down	ce-pw-tunnel-status-snmp,ce-vfi-status-telnet	IPTPLayer 2MplsTunnel	F	T	F	0	T	min	F	T	T
Cisco RF Swap Status - Unsupported	cisco RF swap notification trap	cisco RF status is unsupported	N	IManaged Element	F	F	F	0	F	info	F	T	F
Cisco RF Swap Status - None	cisco RF swap notification trap	cisco RF status is none	N	IManaged Element	F	F	F	0	F	info	F	T	F
Cisco RF Swap Status - Not Known	cisco RF swap notification trap	cisco RF status is notknown	N	IManaged Element	F	F	F	0	F	info	F	T	F
Cisco RF Swap Status - UserInitiated	cisco RF swap notification trap	cisco RF status is userInitiated	N	IManaged Element	F	F	F	0	F	info	F	T	F
Cisco RF Swap Status - UserForced	cisco RF swap notification trap	cisco RF status is userForced	N	IManaged Element	F	F	F	0	F	info	F	T	F

Table 16-22 Cisco IOX V2/V3 Trap Registry Parameters (continued)

Short Description	Event Type	Event Subtype	Expedites Polling	Event Source (IMO Name)	Activate Flow	Correlate	Is Correlation Allowed	Weight	Auto Clear	Severity	Is Ticketable	Auto Remove	Flapping
Cisco RF Swap Status - ActiveUnitFailed	cisco RF swap notification trap	cisco RF status is activeUnitFailed	N	IManaged Element	F	F	F	0	F	info	F	T	F
Cisco RF Swap Status - ActiveUnitRemoved	cisco RF swap notification trap	cisco RF status is activeUnitRemoved	N	IManaged Element	F	F	F	0	F	info	F	T	F
cefc FRU inserted with unsupported product ID	cefc unrecognized fru inserted	cefc unrecognized fru inserted	N	IModule	F	T	F	0	T	info	F	T	F
cefc Power supply output capacity changed	cefc power supply output changed	cefc power supply output changed	N	IModule	F	T	F	0	T	info	F	T	F
RTT Connection Change	RTT Connection Change	RTT Connection Change	N	IManaged Element	F	F	F	0	F	info	T	T	F
RTT Operation Timeout	RTT Operation Timeout	RTT Operation Timeout	N	IManaged Element	F	F	F	0	F	info	T	T	F
RTT Operation Threshold Violation	RTT Operation Threshold Violation	RTT Operation Threshold Violation	N	IManaged Element	F	F	F	0	F	info	T	T	F
RTT Verify Error	RTT Verify Error	RTT Verify Error	N	IManaged Element	F	F	F	0	F	info	T	T	F
RTT threshold violation or clearance	rtt threshold violation or clearance	rtt threshold violation or clearance	N	IManaged Element	F	F	F	0	F	info	T	T	F
RTT Lpd Discovery	RTT Lpd Discovery	RTT Lpd Discovery	N	IManaged Element	F	F	F	0	F	info	T	T	F
RTT Lpd Grp Status	RTT Lpd Grp Status	RTT Lpd Grp Status	N	IManaged Element	F	F	F	0	F	info	T	T	F
IPv6 BGP down trap	ipv6 bgp trap	ipv6 bgp down trap	N	IManaged Element	F	T	F	0	F	maj	F	T	T
ipv6 BGP FSM state changed trap	ipv6 bgp trap	ipv6 bgp state changed trap	N	IManaged Element	F	T	F	0	F	info	F	T	T
IPv6 BGP established trap	ipv6 bgp trap	ipv6 bgp established trap	N	IManaged Element	F	F	F	0	F	clr	F	T	T

Table 16-22 Cisco IOX V2/V3 Trap Registry Parameters (continued)

Short Description	Event Type	Event Subtype	Expedites Polling	Event Source (IMO Name)	Activate Flow	Correlate	Is Correlation Allowed	Weight	Auto Clear	Severity	Is Ticketable	Auto Remove	Flapping
Connection Loss detected by ipsla icmp echo trap	ipsla echo connloss trap	connection loss detected by ipsla icmp echo trap	N/A	ManagedElement	F	F	F	0	F	info	T	T	F
Connection re-establish detected by ipsla icmp echo trap	ipsla echo connloss trap	connection re-establish detected by ipsla icmp echo trap	N/A	ManagedElement	F	F	F	0	F	info	F	T	F
Timeout detected by ipsla icmp echo trap	ipsla ip or lsp echo timeout trap	timeout detected by ipsla icmp echo trap	N/A	ManagedElement	F	F	F	0	F	info	F	T	F
Connection re-establish detected by ipsla icmp echo trap	ipsla ip or lsp echo timeout trap	connection re-establish detected by ipsla icmp echo trap	N/A	ManagedElement	F	F	F	0	F	info	F	T	F
Threshold crossing under trap	ipsla threshold notification trap	threshold crossing under trap	N/A	ManagedElement	F	F	F	0	F	info	F	T	F
Threshold crossing over trap	ipsla threshold notification trap	threshold crossing over trap	N/A	ManagedElement	F	F	F	0	F	info	F	T	F
Data corruption in rtt operation trap	ipsla threshold notification trap	data corruption in rtt operation trap	N/A	ManagedElement	F	F	F	0	F	info	F	T	F
Data corruption cleared in rtt operation trap	ipsla threshold notification trap	data corruption cleared in rtt operation trap	N/A	ManagedElement	F	F	F	0	F	info	F	T	F
Connection Loss detected by ipsla icmp echo trap	ipsla echo connloss trap	connection loss detected by ipsla icmp echo trap	N/A	ManagedElement	F	F	F	0	F	info	T	T	F
Connection Loss detected by ipsla LSP icmp echo trap	ipsla echo connloss trap	connection loss detected by ipsla lsp icmp echo trap	N/A	ManagedElement	F	F	F	0	F	maj	T	T	F
Connection re-establish detected by ipsla icmp echo trap	ipsla echo connloss trap	connection re-establish detected by ipsla icmp echo trap	N/A	ManagedElement	F	F	F	0	F	clr	F	T	F

Table 16-22 Cisco IOX V2/V3 Trap Registry Parameters (continued)

Short Description	Event Type	Event Subtype	Expedites Polling	Event Source (IMO Name)	Activate Flow	Correlate	Is Correlation Allowed	Weight	Auto Clear	Severity	Is Ticketable	Auto Remove	Flapping
Connection re-establish detected by ipsla LSP icmp echo trap	ipsla echo connloss trap	connection re-establish detected by ipsla lsp icmp echo trap	N/A	ManagedElement	F	F	F	0	F	clr	F	T	F
Timeout detected by ipsla icmp echo trap	ipsla echo timeout trap	timeout detected by ipsla icmp echo trap	N/A	ManagedElement	F	F	F	0	F	maj	T	T	F
Timeout detected by ipsla LSP icmp echo trap	ipsla echo timeout trap	timeout detected by ipsla lsp icmp echo trap	N/A	ManagedElement	F	F	F	0	F	maj	T	T	F
Connection re-establish detected by ipsla icmp echo trap	ipsla echo timeout trap	connection re-establish detected by ipsla icmp echo trap	N/A	ManagedElement	F	F	F	0	F	clr	F	T	F
Connection re-establish detected by ipsla LSP icmp echo trap	ipsla echo timeout trap	connection re-establish detected by ipsla lsp icmp echo trap	N/A	ManagedElement	F	F	F	0	F	clr	F	T	F
RTT threshold crossing over trap	ipsla echo rtt trap	rtt threshold crossing over trap	N/A	ManagedElement	F	F	F	0	F	info	F	T	F
RTT threshold crossing under trap	ipsla echo rtt trap	rtt threshold crossing under trap	N/A	ManagedElement	F	F	F	0	F	info	F	T	F
IPSLA LSP path discovery failure trap	ipsla lpd discovery trap	ipsla lsp path discovery failure trap	N/A	ManagedElement	F	F	F	0	F	maj	T	T	F
IPSLA LSP path rediscovery trap	ipsla lpd discovery trap	ipsla lsp path rediscovery trap	N/A	ManagedElement	F	F	F	0	F	clr	F	T	F
IPSLA LDP group status failure trap	ipsla lpd group status trap	ipsla ldp group status failure trap	N/A	ManagedElement	F	F	F	0	F	maj	T	T	F
IPSLA LDP group status restoration trap	ipsla lpd group status trap	ipsla ldp group status restoration trap	N/A	ManagedElement	F	F	F	0	F	clr	F	T	F
FRR Protected Trap	frr trigger trap	frr protected trap	N/A	PortLayer1	F	T	F	0	F	info	F	T	F

Table 16-22 Cisco IOX V2/V3 Trap Registry Parameters (continued)

Short Description	Event Type	Event Subtype	Expedites Polling	Event Source (IMO Name)	Activate Flow	Correlate	Is Correlation Allowed	Weight	Auto Clear	Severity	Is Ticketable	Auto Remove	Flapping
FRR Unprotected Trap	frr trigger trap	frr unprotected trap	N/A	PortLayer1	F	T	F	0	F	info	F	T	F
Pseudo wire tunnel up	pseudo wire tunnel traps	Pseudo wire tunnel up	ce-pw-tunnel-status-snmp,ce-vfi-status-telnet	IPTPLayer2MplsTunnel	F	F	F	0	F	clr	F	T	T
Pseudo wire tunnel down	pseudo wire tunnel traps	Pseudo wire tunnel down	ce-pw-tunnel-status-snmp,ce-vfi-status-telnet	IPTPLayer2MplsTunnel	F	T	F	0	T	min	F	T	T
DSX1 Far end LOF	dsx1 line status change	RcvFarEndLOF	Y	IPhysicalLayer	F	T	F	0	T	maj	F	T	F
DSX1 Near end sending LOF Indication	dsx1 line status change	XmtFarEndLOF	Y	IPhysicalLayer	F	T	F	0	T	maj	F	T	F
DSX1 Far end sending AIS	dsx1 line status change	RcvAIS	Y	IPhysicalLayer	F	T	F	0	T	wrn	F	T	F
DSX1 Near end sending AIS	dsx1 line status change	XmtAIS	Y	IPhysicalLayer	F	T	F	0	T	wrn	F	T	F
DSX1 Near end LOF	dsx1 line status change	LossOfFrame	Y	IPhysicalLayer	F	T	F	0	T	maj	F	T	F
DSX1 Near end Loss of Signal	dsx1 line status change	LossOfSignal	Y	IPhysicalLayer	F	T	F	0	T	maj	F	T	F
DSX1 Near end is looped	dsx1 line status change	LoopbackState	Y	IPhysicalLayer	F	T	F	0	T	maj	F	T	F
DSX1 E1 TS16 AIS	dsx1 line status change	T16AIS	Y	IPhysicalLayer	F	T	F	0	T	wrn	F	T	F
DSX1 Far End Sending TS16 LOMF	dsx1 line status change	RcvFarEndLOMF	Y	IPhysicalLayer	F	T	F	0	T	maj	F	T	F
DSX1 Near End Sending TS16 LOMF	dsx1 line status change	XmtFarEndLOMF	Y	IPhysicalLayer	F	T	F	0	T	maj	F	T	F
DSX1 Near End detects a test code	dsx1 line status change	RcvTestCode	Y	IPhysicalLayer	F	T	F	0	T	maj	F	T	F

Table 16-22 Cisco IOX V2/V3 Trap Registry Parameters (continued)

Short Description	Event Type	Event Subtype	Expedites Polling	Event Source (IMO Name)	Activate Flow	Correlate	Is Correlation Allowed	Weight	Auto Clear	Severity	Is Ticketable	Auto Remove	Flapping
DSX1 any line status not defined here	dsx1 line status change	OtherFailure	Y	IPhysicalLayer	F	T	F	0	T	min	F	T	F
DSX1 Near End in Unavailable Signal State	dsx1 line status change	UnavailSigState	Y	IPhysicalLayer	F	T	F	0	T	maj	F	T	F
DSX1 Carrier Equipment Out of Service	dsx1 line status change	NetEquipOOS	Y	IPhysicalLayer	F	T	F	0	T	maj	F	T	F
DSX1 DS2 Payload AIS	dsx1 line status change	RcvPayloadAIS	Y	IPhysicalLayer	F	T	F	0	T	wrn	F	T	F
DSX1 DS2 Performance Threshold Exceeded	dsx1 line status change	Ds2PerfThreshold	Y	IPhysicalLayer	F	T	F	0	T	maj	F	T	F
DSX1 combination of bitmaps due to multiple failures	dsx1 line status change	MultipleFailures	Y	IPhysicalLayer	F	T	F	0	T	maj	F	T	F
DSX1 No alarm present	dsx1 line status change	NoAlarm	Y	IPhysicalLayer	F	T	F	0	F	clr	F	T	F
DSX3 Receiving Yellow/Remote Alarm Indication	dsx3 line status change	RcvRAIFailure	Y	IPhysicalLayer	F	T	F	0	T	maj	F	T	F
DSX3 Transmitting Yellow/Remote Alarm Indication	dsx3 line status change	XmitRAIAlarm	Y	IPhysicalLayer	F	T	F	0	T	maj	F	T	F
DSX3 Receiving AIS failure state	dsx3 line status change	RcvAIS	Y	IPhysicalLayer	F	T	F	0	T	wrn	F	T	F
DSX3 Transmitting AIS	dsx3 line status change	XmtAIS	Y	IPhysicalLayer	F	T	F	0	T	wrn	F	T	F
DSX3 Receiving LOF failure state	dsx3 line status change	LossOfFrame	Y	IPhysicalLayer	F	T	F	0	T	maj	F	T	F
DSX3 Receiving LOS failure state	dsx3 line status change	LossOfSignal	Y	IPhysicalLayer	F	T	F	0	T	maj	F	T	F

Table 16-22 Cisco IOX V2/V3 Trap Registry Parameters (continued)

Short Description	Event Type	Event Subtype	Expedites Polling	Event Source (IMO Name)	Activate Flow	Correlate	Is Correlation Allowed	Weight	Auto Clear	Severity	Is Ticketable	Auto Remove	Flapping
DSX3 Looping the received signal	dsx3 line status change	LoopbackState	Y	IPhysicalLayer	F	T	F	0	T	maj	F	T	F
DSX3 Receiving a Test Pattern	dsx3 line status change	RcvTestCode	Y	IPhysicalLayer	F	T	F	0	T	maj	F	T	F
DSX3 any line status not defined here	dsx3 line status change	OtherFailure	Y	IPhysicalLayer	F	T	F	0	T	min	F	T	F
DSX3 Near End in Unavailable Signal State	dsx3 line status change	UnavailSigState	Y	IPhysicalLayer	F	T	F	0	T	maj	F	T	F
DSX3 Carrier Equipment Out of Service	dsx3 line status change	NetEquipOOS	Y	IPhysicalLayer	F	T	F	0	T	maj	F	T	F
DSX3 combination of bitmaps due to multiple failures	dsx3 line status change	MultipleFailures	Y	IPhysicalLayer	F	T	F	0	T	maj	F	T	F
DSX3 No alarm present	dsx3 line status change	NoAlarm	Y	IPhysicalLayer	F	T	F	0	F	clr	F	T	F
Entity table configuration changed	Entity table configuration changed	Entity table configuration changed	N	IManagedElement	F	F	T	0	F	info	F	T	F
FR DLCI status invalid trap	fr dlci status change trap	fr dlci status invalid trap	N	IPortLayer1	T	F	F	0	F	maj	F	T	F
FR DLCI status inactive trap	fr dlci status change trap	fr dlci status inactive trap	N	IPortLayer1	T	F	F	0	F	maj	F	T	F
FR DLCI status active trap	fr dlci status change trap	fr dlci status active trap	N	IPortLayer1	T	F	F	0	F	clr	F	T	F
Cisco Sonet vt status changed to error	sonet vt status changed	sonet vt status changed to error	N	IPortLayer1	F	T	F	0	F	maj	T	T	T
Cisco Sonet vt status changed to clear	sonet vt status changed	sonet vt status changed to clear	N	IPortLayer1	F	F	F	0	F	clr	F	T	T
Vrrp trap auth failure trap	vrrp trap auth failure trap	vrrp trap auth failure trap	N	IManagedElement	F	F	F	0	T	minor	F	T	F
Vrrp trap new master trap	vrrp trap new master trap	vrrp trap new master trap	N	IManagedElement	F	F	F	0	T	minor	F	T	F

Table 16-22 Cisco IOX V2/V3 Trap Registry Parameters (continued)

Short Description	Event Type	Event Subtype	Expedites Polling	Event Source (IMO Name)	Activate Flow	Correlate	Is Correlation Allowed	Weight	Auto Clear	Severity	Is Ticketable	Auto Remove	Flapping
Cisco bfd session down trap	Cisco bfd session change trap	Cisco bfd session down trap	bfd session	BfdService	F	T	F	0	T	maj	F	T	T
Cisco bfd session up trap	Cisco bfd session change trap	Cisco bfd session up trap	bfd session	BfdService	F	F	F	0	F	clr	F	T	T
Atm interface PVC failures trap	Atm interface PVC failures trap	Atm interface PVC failures trap	N	IPhysicalLayer	T	T	F	0	T	min	F	T	F

Cisco MIB2 V1 Trap Registry Parameters

Table 16-23 lists the associated event types, event subtypes, and Prime Network registry parameters for the Cisco MIB2 SNMP V1 traps shown in Table 16-7.

Table 16-23 Cisco MIB2 V1 Trap Registry Parameter

Short Description	Event Type	Event Subtype	Expedites Polling	Event Source (IMO Name)	Activate Flow	Correlate	Is Correlation Allowed	Weight	Auto Clear	Severity	Is Ticketable	Auto Remove	Flapping
dummy ticket trap	dummy ticket trap	dummy ticket trap	N	IManagedElement	F	F	F	0	F	clr	F		
SNMP Link down	snmp link down	snmp link down	ce-efp-status-telnet/mtop-mlppbundle-status-telnet/mtop-ima-group-state-telnet/mtop-cem-group-status/bundle-status/mpls traffic engineering tunnel information/basetech-lldp-neighbors-snmp/port-status/ip interface oper status	IPhysicalLayer / Efp Oid	F	T	F	0	T	min	F	T	T

Table 16-23 Cisco MIB2 V1 Trap Registry Parameter (continued)

Short Description	Event Type	Event Subtype	Expedites Polling	Event Source (IMO Name)	Activate Flow	Correlate	Is Correlation Allowed	Weight	Auto Clear	Severity	Is Ticketable	Auto Remove	Flapping
SNMP Link up	snmp link down	snmp link up	ce-efp-status-telnet/mtop-mlppbundle-status-telnet/mtop-ima-group-state-telnet/mtop-cem-group-status/bundle-status/mpls traffic engineering tunnel information/basetech-lldp-neighbors-snmp/port-status/ip interface oper status	IPhysicalLayer / Efp Oid	F	T	F	0	F	clr	F	T	T
DSX1 Far end LOF	dsx1 line status change	RcvFarEndLOF	Y	IPhysicalLayer	F	T	F	0	T	maj	F	T	F
DSX1 Near end sending LOF Indication	dsx1 line status change	XmtFarEndLOF	Y	IPhysicalLayer	F	T	F	0	T	maj	F	T	F
DSX1 Far end sending AIS	dsx1 line status change	RcvAIS	Y	IPhysicalLayer	F	T	F	0	T	wrn	F	T	F
DSX1 Near end sending AIS	dsx1 line status change	XmtAIS	Y	IPhysicalLayer	F	T	F	0	T	wrn	F	T	F
DSX1 Near end LOF	dsx1 line status change	LossOfFrame	Y	IPhysicalLayer	F	T	F	0	T	maj	F	T	F
DSX1 Near end Loss of Signal	dsx1 line status change	LossOfSignal	Y	IPhysicalLayer	F	T	F	0	T	maj	F	T	F
DSX1 Near end is looped	dsx1 line status change	LoopbackState	Y	IPhysicalLayer	F	T	F	0	T	maj	F	T	F
DSX1 E1 TS16 AIS	dsx1 line status change	T16AIS	Y	IPhysicalLayer	F	T	F	0	T	wrn	F	T	F

Table 16-23 Cisco MIB2 V1 Trap Registry Parameter (continued)

Short Description	Event Type	Event Subtype	Expedites Polling	Event Source (IMO Name)	Activate Flow	Correlate	Is Correlation Allowed	Weight	Auto Clear	Severity	Is Ticketable	Auto Remove	Flapping
DSX1 Far End Sending TS16 LOMF	dsx1 line status change	RcvFarEndLOMF	Y	IPhysicalLayer	F	T	F	0	T	maj	F	T	F
DSX1 Near End Sending TS16 LOMF	dsx1 line status change	XmtFarEndLOMF	Y	IPhysicalLayer	F	T	F	0	T	maj	F	T	F
DSX1 Near End detects a test code	dsx1 line status change	RcvTestCode	Y	IPhysicalLayer	F	T	F	0	T	maj	F	T	F
DSX1 any line status not defined here	dsx1 line status change	OtherFailure	Y	IPhysicalLayer	F	T	F	0	T	min	F	T	F
DSX1 Near End in Unavailable Signal State	dsx1 line status change	UnavailSigState	Y	IPhysicalLayer	F	T	F	0	T	maj	F	T	F
DSX1 Carrier Equipment Out of Service	dsx1 line status change	NetEquipOOS	Y	IPhysicalLayer	F	T	F	0	T	maj	F	T	F
DSX1 DS2 Payload AIS	dsx1 line status change	RcvPayloadAIS	Y	IPhysicalLayer	F	T	F	0	T	wrn	F	T	F
DSX1 DS2 Performance Threshold Exceeded	dsx1 line status change	Ds2PerfThreshold	Y	IPhysicalLayer	F	T	F	0	T	maj	F	T	F
DSX1 combination of bitmaps due to multiple failures	dsx1 line status change	MultipleFailures	Y	IPhysicalLayer	F	T	F	0	T	maj	F	T	F
DSX1 No alarm present	dsx1 line status change	NoAlarm	Y	IPhysicalLayer	F	T	F	0	F	clr	F	T	F
DSX3 Receiving Yellow/Remote Alarm Indication	dsx3 line status change	RcvRAIFailure	Y	IPhysicalLayer	F	T	F	0	T	maj	F	T	F
DSX3 Transmitting Yellow/Remote Alarm Indication	dsx3 line status change	XmitRAIAlarm	Y	IPhysicalLayer	F	T	F	0	T	maj	F	T	F

Table 16-23 Cisco MIB2 V1 Trap Registry Parameter (continued)

Short Description	Event Type	Event Subtype	Expedites Polling	Event Source (IMO Name)	Activate Flow	Correlate	Is Correlation Allowed	Weight	Auto Clear	Severity	Is Ticketable	Auto Remove	Flapping
DSX3 Receiving AIS failure state	dsx3 line status change	RcvAIS	Y	IPhysicalLayer	F	T	F	0	T	wrn	F	T	F
DSX3 Transmitting AIS	dsx3 line status change	XmtAIS	Y	IPhysicalLayer	F	T	F	0	T	wrn	F	T	F
DSX3 Receiving LOF failure state	dsx3 line status change	LossOfFrame	Y	IPhysicalLayer	F	T	F	0	T	maj	F	T	F
DSX3 Receiving LOS failure state	dsx3 line status change	LossOfSignal	Y	IPhysicalLayer	F	T	F	0	T	maj	F	T	F
DSX3 Looping the received signal	dsx3 line status change	LoopbackState	Y	IPhysicalLayer	F	T	F	0	T	maj	F	T	F
DSX3 Receiving a Test Pattern	dsx3 line status change	RcvTestCode	Y	IPhysicalLayer	F	T	F	0	T	maj	F	T	F
DSX3 any line status not defined here	dsx3 line status change	OtherFailure	Y	IPhysicalLayer	F	T	F	0	T	min	F	T	F
DSX3 Near End in Unavailable Signal State	dsx3 line status change	UnavailSigState	Y	IPhysicalLayer	F	T	F	0	T	maj	F	T	F
DSX3 Carrier Equipment Out of Service	dsx3 line status change	NetEquipOOS	Y	IPhysicalLayer	F	T	F	0	T	maj	F	T	F
DSX3 combination of bitmaps due to multiple failures	dsx3 line status change	MultipleFailures	Y	IPhysicalLayer	F	T	F	0	T	maj	F	T	F
DSX3 No alarm present	dsx3 line status change	NoAlarm	Y	IPhysicalLayer	F	T	F	0	F	clr	F	T	F
Entity table configuration changed	Entity table configuration changed	Entity table configuration changed	N	IManagedElement	F	F	T	0	F	info	F	T	F

Table 16-23 Cisco MIB2 V1 Trap Registry Parameter (continued)

Short Description	Event Type	Event Subtype	Expedites Polling	Event Source (IMO Name)	Activate Flow	Correlate	Is Correlation Allowed	Weight	Auto Clear	Severity	Is Ticketable	Auto Remove	Flapping
FR DLCI status invalid trap	fr dlci status change trap	fr dlci status invalid trap	N	FREncapKey	T	F	F	0	F	maj	F	T	F
FR DLCI status inactive trap	fr dlci status change trap	fr dlci status inactive trap	N	FREncapKey	T	F	F	0	F	maj	F	T	F
FR DLCI status active trap	fr dlci status change trap	fr dlci status active trap	N	FREncapKey	T	F	F	0	F	clr	F	T	F
Cold start trap	cold start trap	cold start trap	N	IManagedElement	F	F	T	1900000	F	info	T	T	F
BGP down trap	bgp trap	bgp down trap	N	IBgpNeighbourEntry	F	T	T	0	T	maj	F	T	T
BGP established trap	bgp trap	bgp established trap	N	IBgpNeighbourEntry	F	F	F	0	F	clr	F	T	T
SNMP authentication failure	snmp authentication failure	snmp authentication failure	N	IManagedElement	F	T	F	0	F	info	F	T	F
OSPF interface state changed to Down	ospf if state down	ospf if state down	N	IIPInterface	F	T	T	0	F	min	F	T	T
OSPF interface state changed to Up	ospf if state down	ospf if state up	N	IIPInterface	F	F	F	0	F	clr	F	T	T
OSPF virtual interface state changed to Down	ospf virtual if state down	ospf virtual if state down	N	IProfileContainer (OSPF)	F	T	T	0	T	min	F	T	T
OSPF neighbor state down	ospf neighbor state down	ospf neighbor state down	N	IIPInterface	T	T	T	0	F	maj	F	T	T

Table 16-23 Cisco MIB2 V1 Trap Registry Parameter (continued)

Short Description	Event Type	Event Subtype	Expedites Polling	Event Source (IMO Name)	Activate Flow	Correlate	Is Correlation Allowed	Weight	Auto Clear	Severity	Is Ticketable	Auto Remove	Flapping
OSPF neighbor state up	ospf neighbor state down	ospf neighbor state up	N	IIPInterface	F	F	F	0	F	clr	F	T	T
OSPF virtual neighbor state down	ospf-virtual-neighbor-state-changed	ospf-virtual-neighbor-state-down	N	IOspfEntry	T	T	T	0	T	min	T	T	T
OSPF virtual neighbor state up	ospf-virtual-neighbor-state-changed	ospf-virtual-neighbor-state-up	N	IOspfEntry	F	F	F	0	F	clr	F	T	T
OSPF interface configuration error	ospf-if-config-err	ospf-if-config-err	N	IIPInterface	F	T	F	0	T	wrn	T	T	F
OSPF virtual interface configuration error	ospf-virtual-if-config-err	ospf-virtual-if-config-err	N	IManagedElement	F	T	F	0	F	min	F	T	F
OSPF interface authentication failure	ospf-if-authentic-fail	ospf-if-authentic-fail	N	IIPInterface	F	T	F	0	F	wrn	T	T	F
OSPF virtual interface authentication failure	ospf-virtual-if-authentic-fail	ospf-virtual-if-authentic-fail	N	IManagedElement	F	T	F	0	F	wrn	T	T	F
OSPF bad packet received	ospf-if-bad-packet	ospf-if-bad-packet	N	IIPInterface	F	T	F	0	T	min	F	T	F
OSPF bad packet received on virtual interface	ospf-virtual-if-bad-packet	ospf-virtual-if-bad-packet	N	IManagedElement	F	T	F	0	T	min	F	T	F
OSPF packet retransmitted	ospf-if-packet-retransmit	ospf-if-packet-retransmit	N	IManagedElement	F	T	F	0	T	min	F	T	F
OSPF packet retransmitted on virtual interface	ospf-virtual-if-packet-retransmit	ospf-virtual-if-packet-retransmit	N	IManagedElement	F	T	F	0	T	min	F	T	F
OSPF new LSA originated	ospf-new-lsa-originated	ospf-new-lsa-originated	N	IManagedElement	F	T	F	0	T	min	F	T	F

Table 16-23 Cisco MIB2 V1 Trap Registry Parameter (continued)

Short Description	Event Type	Event Subtype	Expedites Polling	Event Source (IMO Name)	Activate Flow	Correlate	Is Correlation Allowed	Weight	Auto Clear	Severity	Is Ticketable	Auto Remove	Flapping
OSPF LSA aged to MaxAge	ospf-lsa-reached-maxage	ospf-lsa-reached-maxage	N	IManagedElement	F	F	F	0	F	info	F	T	F
mte event set failure	cisco mte event set failure	cisco mte event set failure	N	IManagedElement	F	T	F	0	F	wrn	T	T	T
Cisco mte trigger falling	cisco mte trigger rising	cisco mte trigger falling	N	IManagedElement	F	F	F	0	F	clr	T	T	T
mte trigger fired	cisco mte trigger fired	cisco mte trigger fired	N	IManagedElement	F	T	F	0	F	info	T	T	T
Cisco mte trigger rising	cisco mte trigger rising	cisco mte trigger rising	N	IManagedElement	F	T	F	0	F	wrn	T	T	T
Entity table configuration changed	Entity table configuration changed	Entity table configuration changed	N	IManagedElement	F	F	T	0	F	info	F	T	F
ipv6 interface state changed	ipv6-if-state-changed	ipv6-if-state-changed	N	IManagedElement	F	F	F	0	T	min	F	T	F
mpls l3 vpn numvrf routemax thresh cleared Trap	mpls l3 vpn vrf routemid thresh exceeded	mpls l3 vpn numvrf routemax thresh cleared	N	IVrf	F	T	F	0	T	clr	F	T	F
mpls l3 vpn vrf Down Trap	mpls l3 vpn vrf Down	mpls l3 vpn vrf Down	N	IVrf	T	T	F	0	T	maj	T	T	F
mpls l3 vpn vrf numvrf routemax thresh exceeded Trap	mpls l3 vpn vrf routemid thresh exceeded	mpls l3 vpn vrf numvrf routemax thresh exceeded	N	IVrf	F	T	F	0	T	wrn	F	T	F
mpls l3 vpn vrf routemid thresh exceeded Trap	mpls l3 vpn vrf routemid thresh exceeded	mpls l3 vpn vrf routemid thresh exceeded	N	IVrf	F	T	F	0	F	wrn	F	T	F

Table 16-23 Cisco MIB2 V1 Trap Registry Parameter (continued)

Short Description	Event Type	Event Subtype	Expedites Polling	Event Source (IMO Name)	Activate Flow	Correlate	Is Correlation Allowed	Weight	Auto Clear	Severity	Is Ticketable	Auto Remove	Flapping
mpls l3 vpn vrf Up Trap	mpls l3 vpn vrf Down	mpls l3 vpn vrf Up	N	IVrf	F	T	F	0	F	clr	F	T	F
MPLS LDP init session threshold exceeded Trap	mpls ldp session down	mpls ldp init session thresh exceeded	mpls interfaces + label switching table	IPortLayer1	F	T	F	0	T	wrn	F	T	T
MPLS LDP session down Trap	mpls ldp session down	mpls ldp session down	mpls interfaces + label switching table	IPortLayer1	T	T	T	0	T	min	F	T	T
MPLS LDP session up Trap	mpls ldp session down	mpls ldp session up	mpls interfaces + label switching table	IPortLayer1	F	T	F	0	T	clr	F	T	T
MPLS-TE tunnel rerouted trap	mpls te tunnel rerouted trap	mpls te tunnel rerouted trap	N	IMplsTETunnel	F	T	F	0	F	info	T	T	T
MPLS-TE tunnel reoptimized trap	mpls te tunnel reoptimized trap	mpls te tunnel reoptimized trap	N	IMplsTETunnel	F	T	F	0	F	info	F	T	T
MPLS-TE tunnel down	mpls te tunnel down	mpls te tunnel down	Y	IMplsTETunnel	T	T	T	800	F	maj	T	T	T
MPLS-TE tunnel up	mpls te tunnel down	mpls te tunnel up	Y	IMplsTETunnel	F	F	F	0	F	clr	F	T	T

Cisco MIB2 V2/V3 Trap Registry Parameters

Table 16-24 lists the associated event types, event subtypes, and Prime Network registry parameters for the Cisco MIB2 SNMP V2/V3 traps shown in Table 16-8.

Table 16-24 Cisco MIB2 V2/V3 Trap Registry Parameters

Short Description	Event Type	Event Subtype	Expedites Polling	Event Source (IMO Name)	Activate Flow	Correlate	Is Correlation Allowed	Weight	Auto Clear	Severity	Is Ticketable	Auto Remove	Flapping
BGP down trap	bgp trap	bgp down trap	N	IBgpNeighborEntry	F	T	T	0	T	maj	F	T	T
BGP established trap	bgp trap	bgp established trap	N	IBgpNeighborEntry	F	F	F	0	F	clr	F	T	T
mte event set failure	cisco mte event set failure	cisco mte event set failure	N	IManagedElement	F	T	F	0	F	wrn	T	T	T
Cisco mte trigger falling	cisco mte trigger rising	cisco mte trigger falling	N	IManagedElement	F	F	F	0	F	clr	T	T	T
mte trigger fired	cisco mte trigger fired	cisco mte trigger fired	N	IManagedElement	F	T	F	0	F	info	T	T	T
Cisco mte trigger rising	cisco mte trigger rising	cisco mte trigger rising	N	IManagedElement	F	T	F	0	F	wrn	T	T	T
Entity table configuration changed	Entity table configuration changed	Entity table configuration changed	N	IManagedElement	F	F	T	0	F	info	F	T	F
Cold start trap	cold start trap	cold start trap	N	IManagedElement	F	F	T	190000	F	info	T	T	F
Warm start trap	warm start trap	warm start trap	N	IManagedElement	F	F	F	0	F	min	T	T	F
SNMP authentication failure	snmp authentication failure	snmp authentication failure	N	IManagedElement	F	T	F	0	F	info	F	T	F

Table 16-24 Cisco MIB2 V2/V3 Trap Registry Parameters (continued)

Short Description	Event Type	Event Subtype	Expedites Polling	Event Source (IMO Name)	Activate Flow	Correlate	Is Correlation Allowed	Weight	Auto Clear	Severity	Is Ticketable	Auto Remove	Flapping
SNMP Link down	snmp link down	snmp link down	ce-efp-status-telnet/mtop-mlppbundle-status-telnet/mtop-ima-group-state-telnet/mtop-cem-group-status/bundle-status/mpls traffic engineering tunnel information/basetech-lldp-neighbors-snmp/basetech-cdp-neighbors-snmp/port-status/ip interface oper status	IPhysicalLayer	F	T	T	0	T	min	F	T	T

Table 16-24 Cisco MIB2 V2/V3 Trap Registry Parameters (continued)

Short Description	Event Type	Event Subtype	Expedites Polling	Event Source (IMO Name)	Activate Flow	Correlate	Is Correlation Allowed	Weight	Auto Clear	Severity	Is Ticketable	Auto Remove	Flapping
SNMP Link up	snmp link down	snmp link up	ce-efp-status-telnet/mtop-mlppbundle-status-telnet/mtop-ima-group-state-telnet/mtop-cem-group-status/bundle-status/mpls traffic engineering tunnel information/basetech-lldp-neighbors-snmp/basetech-cdp-neighbors-snmp/port-status/ip interface oper status	IPhysicalLayer	F	F	F	0	F	clr	F	T	T
ipv6 interface state changed	ipv6-if-state-changed	ipv6-if-state-changed	N	IManagedElement	F	F	F	0	T	min	F	T	F
OSPF interface state changed to Down	ospf if state down	ospf if state down	N	IIPInterface	F	T	T	0	F	min	F	T	T
OSPF interface state changed to Up	ospf if state down	ospf if state up	N	IIPInterface	F	F	F	0	F	clr	F	T	T
OSPF virtual interface state changed to Down	ospf virtual if state down	ospf virtual if state down	N	IProfileContainer (OSPF)	F	T	T	0	F	min	F	T	T
OSPF neighbor state down	ospf neighbor state down	ospf neighbor state down	N	IIPInterface	T	T	T	0	F	maj	F	T	T
OSPF neighbor state up	ospf neighbor state down	ospf neighbor state up	N	IIPInterface	F	F	F	0	F	clr	F	T	T

Table 16-24 Cisco MIB2 V2/V3 Trap Registry Parameters (continued)

Short Description	Event Type	Event Subtype	Expedites Polling	Event Source (IMO Name)	Activate Flow	Correlate	Is Correlation Allowed	Weight	Auto Clear	Severity	Is Ticketable	Auto Remove	Flapping
OSPF virtual neighbor state down	ospf-virtual-neighbor-state-changed	ospf-virtual-neighbor-state-down	N	IOspfEntry	T	T	T	0	F	min	T	T	T
OSPF virtual neighbor state up	ospf-virtual-neighbor-state-changed	ospf-virtual-neighbor-state-up	N	IOspfEntry	F	F	F	0	F	clr	F	T	T
OSPF interface configuration error	ospf-if-config-err	ospf-if-config-err	N	IIPInterface	F	T	F	0	F	wrn	T	T	F
OSPF virtual interface configuration error	ospf-virtual-if-config-err	ospf-virtual-if-config-err	N	IProfileContainer (OSPF)	F	T	F	0	F	min	F	T	F
OSPF interface authentication failure	ospf-if-authentic-fail	ospf-if-authentic-fail	N	IIPInterface	F	T	F	0	F	wrn	T	T	F
OSPF virtual interface authentication failure	ospf-virtual-if-authentic-fail	ospf-virtual-if-authentic-fail	N	IProfileContainer (OSPF)	F	T	F	0	F	wrn	T	T	F
OSPF bad packet received	ospf-if-bad-packet	ospf-if-bad-packet	N	IIPInterface	F	T	F	0	T	min	F	T	F
OSPF bad packet received on virtual interface	ospf-virtual-if-bad-packet	ospf-virtual-if-bad-packet	N	IProfileContainer (OSPF)	F	T	F	0	T	min	F	T	F
OSPF packet retransmitted	ospf-if-packet-retransmit	ospf-if-packet-retransmit	N	IProfileContainer (OSPF)	F	T	F	0	T	min	F	T	F
OSPF packet retransmitted on virtual interface	ospf-virtual-if-packet-retransmit	ospf-virtual-if-packet-retransmit	N	IProfileContainer (OSPF)	F	T	F	0	T	min	F	T	F
OSPF new LSA originated	ospf-new-lsa-originated	ospf-new-lsa-originated	N	IProfileContainer (OSPF)	F	T	F	0	T	min	F	T	F
OSPF LSA aged to MaxAge	ospf-lsa-reached-maxage	ospf-lsa-reached-maxage	N	IManagedElement	F	F	F	0	F	info	F	T	F
mpls l3 vpn numvrf routemax thresh cleared Trap	mpls l3 vpn vrf routemid thresh exceeded	mpls l3 vpn numvrf routemax thresh cleared	N	IVrf	F	T	F	0	F	clr	F	T	F

Table 16-24 Cisco MIB2 V2/V3 Trap Registry Parameters (continued)

Short Description	Event Type	Event Subtype	Expedites Polling	Event Source (IMO Name)	Activate Flow	Correlate	Is Correlation Allowed	Weight	Auto Clear	Severity	Is Ticketable	Auto Remove	Flapping
mpls l3 vpn vrf Down Trap	mpls l3 vpn vrf Down	mpls l3 vpn vrf Down	N	IVrf	T	T	F	0	F	maj	T	T	F
mpls l3 vpn vrf numvrf routemax thresh exceeded Trap	mpls l3 vpn vrf routemid thresh exceeded	mpls l3 vpn vrf numvrf routemax thresh exceeded	N	IVrf	F	T	F	0	F	wrn	F	T	F
mpls l3 vpn vrf routemid thresh exceeded Trap	mpls l3 vpn vrf routemid thresh exceeded	mpls l3 vpn vrf routemid thresh exceeded	N	IVrf	F	T	F	0	F	wrn	F	T	F
mpls l3 vpn vrf Up Trap	mpls l3 vpn vrf Down	mpls l3 vpn vrf Up	N	IVrf	F	T	F	0	F	clr	F	T	F
MPLS LDP init session threshold exceeded Trap	mpls ldp session down	mpls ldp init session thresh exceeded	mpls interfaces + label switching table	IPortLayer 1	F	T	F	0	T	wrn	F	T	T
MPLS LDP session down Trap	mpls ldp session down	mpls ldp session down	mpls interfaces + label switching table	IPortLayer 1	T	T	T	0	T	min	F	F	T
MPLS LDP session up Trap	mpls ldp session down	mpls ldp session up	mpls interfaces + label switching table	IPortLayer 1	F	T	F	0	T	clr	F	F	T
MPLS TE tunnel rerouted trap	mpls te tunnel rerouted trap	mpls te tunnel rerouted trap	N	IMplsTETunnel	F	T	F	0	F	info	T	T	T
MPLS TE tunnel reoptimized trap	mpls te tunnel reoptimized trap	mpls te tunnel reoptimized trap	N	IMplsTETunnel	F	T	F	0	F	info	F	T	T
MPLS TE tunnel down	mpls te tunnel down	mpls te tunnel down	Y	IMplsTETunnel	T	T	T	800	F	maj	T	T	T
MPLS TE tunnel up	mpls te tunnel down	mpls te tunnel up	Y	IMplsTETunnel	F	F	F	0	F	clr	F	T	T
DSX1 Far end LOF	dsx1 line status change	RcvFarEndLOF	Y	IPhysicalLayer	F	T	F	0	T	maj	F	T	F

Table 16-24 Cisco MIB2 V2/V3 Trap Registry Parameters (continued)

Short Description	Event Type	Event Subtype	Expedites Polling	Event Source (IMO Name)	Activate Flow	Correlate	Is Correlation Allowed	Weight	Auto Clear	Severity	Is Ticketable	Auto Remove	Flapping
DSX1 Near end sending LOF Indication	dsx1 line status change	XmtFarEndLOF	Y	IPhysicalLayer	F	T	F	0	T	maj	F	T	F
DSX1 Far end sending AIS	dsx1 line status change	RcvAIS	Y	IPhysicalLayer	F	T	F	0	T	wrn	F	T	F
DSX1 Near end sending AIS	dsx1 line status change	XmtAIS	Y	IPhysicalLayer	F	T	F	0	T	wrn	F	T	F
DSX1 Near end LOF	dsx1 line status change	LossOfFrame	Y	IPhysicalLayer	F	T	F	0	T	maj	F	T	F
DSX1 Near end Loss of Signal	dsx1 line status change	LossOfSignal	Y	IPhysicalLayer	F	T	F	0	T	maj	F	T	F
DSX1 Near end is looped	dsx1 line status change	LoopbackState	Y	IPhysicalLayer	F	T	F	0	T	maj	F	T	F
DSX1 E1 TS16 AIS	dsx1 line status change	T16AIS	Y	IPhysicalLayer	F	T	F	0	T	wrn	F	T	F
DSX1 Far End Sending TS16 LOMF	dsx1 line status change	RcvFarEndLOMF	Y	IPhysicalLayer	F	T	F	0	T	maj	F	T	F
DSX1 Near End Sending TS16 LOMF	dsx1 line status change	XmtFarEndLOMF	Y	IPhysicalLayer	F	T	F	0	T	maj	F	T	F
DSX1 Near End detects a test code	dsx1 line status change	RcvTestCode	Y	IPhysicalLayer	F	T	F	0	T	maj	F	T	F
DSX1 any line status not defined here	dsx1 line status change	OtherFailure	Y	IPhysicalLayer	F	T	F	0	T	min	F	T	F
DSX1 Near End in Unavailable Signal State	dsx1 line status change	UnavailSigState	Y	IPhysicalLayer	F	T	F	0	T	maj	F	T	F
DSX1 Carrier Equipment Out of Service	dsx1 line status change	NetEquipOOS	Y	IPhysicalLayer	F	T	F	0	T	maj	F	T	F
DSX1 DS2 Payload AIS	dsx1 line status change	RcvPayloadAIS	Y	IPhysicalLayer	F	T	F	0	T	wrn	F	T	F
DSX1 DS2 Performance Threshold Exceeded	dsx1 line status change	Ds2PerfThreshold	Y	IPhysicalLayer	F	T	F	0	T	maj	F	T	F

Table 16-24 Cisco MIB2 V2/V3 Trap Registry Parameters (continued)

Short Description	Event Type	Event Subtype	Expedites Polling	Event Source (IMO Name)	Activate Flow	Correlate	Is Correlation Allowed	Weight	Auto Clear	Severity	Is Ticketable	Auto Remove	Flapping
DSX1 combination of bitmaps due to multiple failures	dsx1 line status change	MultipleFailures	Y	IPhysicalLayer	F	T	F	0	T	maj	F	T	F
DSX1 No alarm present	dsx1 line status change	NoAlarm	Y	IPhysicalLayer	F	T	F	0	F	clr	F	T	F
DSX3 Receiving Yellow/Remote Alarm Indication	dsx3 line status change	RcvRAIFailure	Y	IPhysicalLayer	F	T	F	0	T	maj	F	T	F
DSX3 Transmitting Yellow/Remote Alarm Indication	dsx3 line status change	XmitRAIAlarm	Y	IPhysicalLayer	F	T	F	0	T	maj	F	T	F
DSX3 Receiving AIS failure state	dsx3 line status change	RcvAIS	Y	IPhysicalLayer	F	T	F	0	T	wrn	F	T	F
DSX3 Transmitting AIS	dsx3 line status change	XmtAIS	Y	IPhysicalLayer	F	T	F	0	T	wrn	F	T	F
DSX3 Receiving LOF failure state	dsx3 line status change	LossOfFrame	Y	IPhysicalLayer	F	T	F	0	T	maj	F	T	F
DSX3 Receiving LOS failure state	dsx3 line status change	LossOfSignal	Y	IPhysicalLayer	F	T	F	0	T	maj	F	T	F
DSX3 Looping the received signal	dsx3 line status change	LoopbackState	Y	IPhysicalLayer	F	T	F	0	T	maj	F	T	F
DSX3 Receiving a Test Pattern	dsx3 line status change	RcvTestCode	Y	IPhysicalLayer	F	T	F	0	T	maj	F	T	F
DSX3 any line status not defined here	dsx3 line status change	OtherFailure	Y	IPhysicalLayer	F	T	F	0	T	min	F	T	F
DSX3 Near End in Unavailable Signal State	dsx3 line status change	UnavailSigState	Y	IPhysicalLayer	F	T	F	0	T	maj	F	T	F
DSX3 Carrier Equipment Out of Service	dsx3 line status change	NetEquipOOS	Y	IPhysicalLayer	F	T	F	0	T	maj	F	T	F
DSX3 combination of bitmaps due to multiple failures	dsx3 line status change	MultipleFailures	Y	IPhysicalLayer	F	T	F	0	T	maj	F	T	F
DSX3 No alarm present	dsx3 line status change	NoAlarm	Y	IPhysicalLayer	F	T	F	0	F	clr	F	T	F

Table 16-24 Cisco MIB2 V2/V3 Trap Registry Parameters (continued)

Short Description	Event Type	Event Subtype	Expedites Polling	Event Source (IMO Name)	Activate Flow	Correlate	Is Correlation Allowed	Weight	Auto Clear	Severity	Is Ticketable	Auto Remove	Flapping
FR DLCI status invalid trap	fr dlci status change trap	fr dlci status invalid trap	N	FREncapKey	T	F	F	0	F	maj	F	T	F
FR DLCI status inactive trap	fr dlci status change trap	fr dlci status inactive trap	N	FREncapKey	T	F	F	0	F	maj	F	T	F
FR DLCI status active trap	fr dlci status change trap	fr dlci status active trap	N	FREncapKey	T	F	F	0	F	clr	F	T	F

Cisco ACE V1 Trap Registry Parameters

Table 16-25 lists the associated event types, event subtypes, and Prime Network registry parameters for the Cisco ACE SNMP V1 traps shown in Table 16-9.

Table 16-25 Cisco ACE V1 Trap Registry Parameters

Short Description	Event Type	Event Subtype	Expedites Polling	Event Source (IMO Name)	Activate Flow	Correlate	Is Correlation Allowed	Weight	Auto Clear	Severity	Is Ticketable	Auto Remove	Flapping
ces real server state up trap	ces real server state down trap	ces real server state up trap	N/A	IManagedElement	F	F	F	0	T	Cleared	F	T	F
ces real server state down trap	ces real server state down trap	ces real server state down trap	N/A	IManagedElement	F	F	F	0	T	Minor	F	T	F
ces real server state change trap	ces real server state change trap	ces real server state change trap	N/A	IManagedElement	F	F	F	0	T	Minor	F	T	F
ces R server state up trap	ces R server state down trap	ces R server state up trap	N/A	IManagedElement	F	F	F	0	T	Clear	F	T	F
ces R server state down trap	ces R server state down trap	ces R server state down trap	N/A	IManagedElement	F	F	F	0	T	Minor	F	T	F
ces R server state change trap	ces R server state change trap	ces R server state change trap	N/A	IManagedElement	F	F	F	0	T	Minor	F	T	F
cisco sib V server VIP state change trap	cisco sib V server VIP state trap	cisco sib V server VIP state change trap	N/A	IManagedElement	F	F	F	0	T	Minor	F	T	F

Table 16-25 Cisco ACE V1 Trap Registry Parameters (continued)

Short Description	Event Type	Event Subtype	Expedites Polling	Event Source (IMO Name)	Activate Flow	Correlate	Is Correlation Allowed	Weight	Auto Clear	Severity	Is Ticketable	Auto Remove	Flapping
cisco sib V server state change trap	cisco sib V server state trap	cisco sib V server state change trap	N/A	IManagedElement	F	F	F	0	T	Minor	F	T	F
clm license expiry notify trap	clm license notify trap	clm license expiry notify trap	N/A	IManagedElement	F	F	F	0	T	Minor	F	T	F
clm license file missing notify trap	clm license notify trap	clm license file missing notify trap	N/A	IManagedElement	F	F	F	0	T	Minor	F	T	F
clm license expiry warning notify trap	clm license notify trap	clm license expiry warning notify trap	N/A	IManagedElement	F	F	F	0	T	Minor	F	T	F

Cisco ACE V2/V3 Trap Registry Parameters

Table 16-26 lists the associated event types, event subtypes, and Prime Network registry parameters for the Cisco ACE SNMP V2/V3 traps shown in Table 16-10.

Table 16-26 Cisco ACE V2/V3 Trap Registry Parameters

Short Description	Event Type	Event Subtype	Expedites Polling	Event Source (IMO Name)	Activate Flow	Correlate	Is Correlation Allowed	Weight	Auto Clear	Severity	Is Ticketable	Auto Remove	Flapping
SNMP Link down	snmp link down	snmp link down	ip interface oper status	IPhysicalLayer	F	T	T	0	T	min	F	T	T
SNMP Link up	snmp link down	snmp link up	ip interface oper status	IPhysicalLayer	F	F	F	0	F	clr	F	T	T
ces real server state up trap	ces real server state down trap	ces real server state up trap	N/A	IManagedElement	F	F	F	0	T	clr	F	T	F
ces real server state down trap	ces real server state down trap	ces real server state down trap	N/A	IManagedElement	F	F	F	0	T	Minor	F	T	F
ces real server state change trap	ces real server state change trap	ces real server state change trap	N/A	IManagedElement	F	F	F	0	T	Minor	F	T	F

Table 16-26 Cisco ACE V2/V3 Trap Registry Parameters (continued)

Short Description	Event Type	Event Subtype	Expedites Polling	Event Source (IMO Name)	Activate Flow	Correlate	Is Correlation Allowed	Weight	Auto Clear	Severity	Is Ticketable	Auto Remove	Flapping
ces R server state up trap	ces R server state down trap	ces R server state up trap	N/A	IManagedElement	F	F	F	0	T	clr	F	T	F
ces R server state down trap	ces R server state down trap	ces R server state down trap	N/A	IManagedElement	F	F	F	0	T	Minor	F	T	F
ces R server state change trap	ces R server state change trap	ces R server state change trap	N/A	IManagedElement	F	F	F	0	T	Minor	F	T	F
cisco sib V server VIP state change trap	cisco sib V server VIP state trap	cisco sib V server VIP state change trap	N/A	IManagedElement	F	F	F	0	T	Minor	F	T	F
cisco sib V server state change trap	cisco sib V server state trap	cisco sib V server state change trap	N/A	IManagedElement	F	F	F	0	T	Minor	F	T	F
clm license expiry notify trap	clm license notify trap	clm license expiry notify trap	N/A	IManagedElement	F	F	F	0	T	Minor	F	T	F
clm license file missing notify trap	clm license notify trap	clm license file missing notify trap	N/A	IManagedElement	F	F	F	0	T	Minor	F	T	F
clm license expiry warning notify trap	clm license notify trap	clm license expiry warning notify trap	N/A	IManagedElement	F	F	F	0	T	Minor	F	T	F

Cisco Nexus V1 Trap Registry Parameters

Table 16-27 lists the associated event types, event subtypes, and Prime Network registry parameters for the Cisco ACE SNMP V1 traps shown in Table 16-11.

Table 16-27 Cisco Nexus V1 Trap Registry Parameters

Short Description	Event Type	Event Subtype	Expedites Polling	Event Source (IMO Name)	Activate Flow	Correlate	Is Correlation Allowed	Weight	Auto Clear	Severity	Is Ticketable	Auto Remove	Flapping
BGP established trap	bgp trap	bgp established trap	N	IManagedElement	F	F	F	0	F	clr	F	T	T
BGP down trap	bgp trap	bgp down trap	N	IManagedElement	F	T	T	0	T	maj	F	T	T
new root trap	new root trap	new root trap	N	IManagedElement	F	F	F	0	F	info	F	T	F
Spanning Tree Topology Changed	Spanning Tree Topology Change Trap	Spanning Tree Topology Change	N	IManagedElement	F	T	F	0	F	info	F	T	F
cefc module oper status down	cefc module oper status changed	cefc module oper down	physical-command	IModule	F	T	T	0	T	maj	F	T	T
cefc module oper status up	cefc module oper status changed	cefc module oper up	physical-command	IModule	F	F	F	0	F	clr	F	T	T
cefc power status down	cefc power status changed	cefc power status down	physical-command	IModule	F	T	T	0	T	maj	F	T	T
cefc power status up	cefc power status changed	cefc power status up	physical-command	IModule	F	F	F	0	F	clr	F	T	T
cefc FRU inserted	cefc fru removed	cefc fan status up	physical-command	IModule	F	F	F	0	T	clr	F	T	T
cefc FRU removed	cefc fru removed	cefc fru removed	physical-command	IModule	F	T	T	0	T	maj	F	T	T
sensor value crossed threshold in entSensorThresholdTable	entity sensor threshold notification	entity sensor threshold notification	N	IManagedElement	F	F	F	0	F	maj	T	T	T
cps IfVlan Secure MacAddr Violation Trap	cps-IfVlan-Secure-MacAddr-Violation-Trap	cps-IfVlan-Secure-MacAddr-Violation-Trap	N	IPortLayer1	F	F	T	0	F	maj	T	T	F
cps Secure MacAddr Violation Trap	cps-Secure-MacAddr-Violation-Trap	cps-Secure-MacAddr-Violation-Trap	N	IPortLayer1	F	F	T	0	F	maj	T	T	F

Table 16-27 Cisco Nexus V1 Trap Registry Parameters (continued)

Short Description	Event Type	Event Subtype	Expedites Polling	Event Source (IMO Name)	Activate Flow	Correlate	Is Correlation Allowed	Weight	Auto Clear	Severity	Is Ticketable	Auto Remove	Flapping
Stpx Pvid Inconsistency Trap	stpx port inconsistency update	PvidInconsistent trap	N	IManagedElement	F	T	F	0	F	info	F	T	F
Stpx Type Inconsistency Trap	stpx port inconsistency update	TypeInconsistent trap	N	IManagedElement	F	T	F	0	F	info	F	T	F
stpx loop inconsistency discovered	stpx loop inconsistency update	stpx loop inconsistency discovered	N	IManagedElement	F	T	F	0	F	maj	T	T	F
stpx loop inconsistency resolved	stpx loop inconsistency update	stpx loop inconsistency resolved	N	IManagedElement	F	F	F	0	F	clr	T	T	F
stpx root inconsistency discovered	stpx root inconsistency update	stpx root inconsistency discovered	N	IManagedElement	F	T	F	0	F	maj	T	T	F
stpx root inconsistency resolved	stpx root inconsistency update	stpx root inconsistency resolved	N	IManagedElement	F	F	F	0	F	clr	T	T	F
SNMP Link down	snmp link down	snmp link down	ip interface oper status,port-status	IPhysicalLayer	F	T	F	0	T	min	F	T	T
SNMP Link up	snmp link down	snmp link up	ip interface oper status,port-status	IPhysicalLayer	F	T	F	0	F	clr	F	T	T
RMON Rising Alarm	RMON-Alarm-Trap	Rising Alarm	N	IManagedElement	F	T	F	0	T	WARNING	F	T	F
RMON Falling Alarm	RMON-Alarm-Trap	Falling Alarm	N	IManagedElement	F	T	F	0	T	WARNING	F	T	F
Cold start trap	cold start trap	cold start trap	N	IManagedElement	F	F	T	190000	F	info	T	T	F
OSPF virtual interface state changed to Down	ospf virtual if state down	ospf virtual if state down	N	IManagedElement	F	T	T	0	F	min	F	T	T

Table 16-27 Cisco Nexus V1 Trap Registry Parameters (continued)

Short Description	Event Type	Event Subtype	Expedites Polling	Event Source (IMO Name)	Activate Flow	Correlate	Is Correlation Allowed	Weight	Auto Clear	Severity	Is Ticketable	Auto Remove	Flapping
OSPF neighbor state down	ospf neighbor state down	ospf neighbor state down	N	IManagedElement	T	T	T	0	F	maj	T	T	T
OSPF neighbor state up	ospf neighbor state down	ospf neighbor state up	N	IManagedElement	F	F	F	0	F	clr	F	T	T
OSPF virtual neighbor state down	ospf-virtual-neighbor-state-changed	ospf-virtual-neighbor-state-down	N	IManagedElement	T	T	T	0	F	min	T	T	T
OSPF virtual neighbor state up	ospf-virtual-neighbor-state-changed	ospf-virtual-neighbor-state-up	N	IManagedElement	F	F	F	0	F	clr	F	T	T
OSPF interface configuration error	ospf-if-config-err	ospf-if-config-err	N	IManagedElement	F	T	F	0	F	wrn	T	T	F
OSPF virtual interface configuration error	ospf-virtual-if-config-err	ospf-virtual-if-config-err	N	IManagedElement	F	T	F	0	F	min	F	T	F
OSPF interface authentication failure	ospf-if-authentic-fail	ospf-if-authentic-fail	N	IManagedElement	F	T	F	0	F	wrn	T	T	F
OSPF virtual interface authentication failure	ospf-virtual-if-authentic-fail	ospf-virtual-if-authentic-fail	N	IManagedElement	F	T	F	0	F	wrn	T	T	F
OSPF bad packet received	ospf-if-bad-packet	ospf-if-bad-packet	N	IManagedElement	F	T	F	0	T	min	F	T	F
OSPF bad packet received on virtual interface	ospf-virtual-if-bad-packet	ospf-virtual-if-bad-packet	N	IManagedElement	F	T	F	0	T	min	F	T	F
OSPF packet retransmitted	ospf-if-packet-retransmit	ospf-if-packet-retransmit	N	IManagedElement	F	T	F	0	T	min	F	T	F
OSPF packet retransmitted on virtual interface	ospf-virtual-if-packet-retransmit	ospf-virtual-if-packet-retransmit	N	IManagedElement	F	T	F	0	T	min	F	T	F
OSPF new LSA originated	ospf-new-lsa-originated	ospf-new-lsa-originated	N	IManagedElement	F	T	F	0	T	min	F	T	F
OSPF LSA aged to MaxAge	ospf-lsa-reached-maxage	ospf-lsa-reached-maxage	N	IManagedElement	F	F	F	0	F	info	F	T	F
OSPF lsdb overflow trap	ospf lsdb overflow trap	ospf lsdb overflow trap	N	IManagedElement	F	T	F	0	T	MINOR	F	T	F

Table 16-27 Cisco Nexus V1 Trap Registry Parameters (continued)

Short Description	Event Type	Event Subtype	Expedites Polling	Event Source (IMO Name)	Activate Flow	Correlate	Is Correlation Allowed	Weight	Auto Clear	Severity	Is Ticketable	Auto Remove	Flapping
OSPF lsdb approaching overflow trap	ospf lsdb approaching overflow trap	ospf lsdb approaching overflow trap	N	IManagedElement	F	T	F	0	T	MINOR	F	T	F
OSPF interface state changed to Down	ospf if state down	ospf if state down	N	IManagedElement	F	T	T	0	F	info	F	T	T
OSPF interface state changed to Up	ospf if state down	ospf if state up	N	IManagedElement	F	F	F	0	F	clr	F	T	T
OSPF NSSA translator status change trap	ospf-status-change-trap	ospf nssa translator status change trap	N	IManagedElement	F	F	F	0	F	info	F	T	F
OSPF restart status change trap	ospf-status-change-trap	ospf restart status change trap	N	IManagedElement	F	F	F	0	F	info	F	T	F
OSPF neighbor restart helper status change trap	ospf-status-change-trap	ospf nbr restart helper status change trap	N	IManagedElement	F	F	F	0	F	info	F	T	F
OSPF virtual neighbor restart helper status change trap	ospf-status-change-trap	ospf virt nbr restart helper status change trap	N	IManagedElement	F	F	F	0	F	info	F	T	F

Cisco Nexus V2/V3 Trap Registry Parameters

Table 16-28 lists the associated event types, event subtypes, and Prime Network registry parameters for the Cisco Nexus SNMP V2/V3 traps shown in Table 16-12.

Table 16-28 Cisco Nexus V2/V3 Trap Registry Parameters

Short Description	Event Type	Event Subtype	Expedites Polling	Event Source (IMO Name)	Activate Flow	Correlate	Is Correlation Allowed	Weight	Auto Clear	Severity	Is Ticketable	Auto Remove	Flapping
BGP established trap	bgp trap	bgp established trap	N	IManagedElement	F	F	F	0	F	clr	F	T	T
BGP down trap	bgp trap	bgp down trap	N	IManagedElement	F	T	T	0	T	maj	F	T	T
new root trap	new root trap	new root trap	N	IManagedElement	F	F	F	0	F	info	F	T	F
Spanning Tree Topology Changed	Spanning Tree Topology Change Trap	Spanning Tree Topology Change	N	IManagedElement	F	T	F	0	F	info	F	T	F
cefc module oper status down	cefc module oper status changed	cefc module oper down	physical-command	IModule	F	T	T	0	T	maj	F	T	T
cefc module oper status up	cefc module oper status changed	cefc module oper up	physical-command	IModule	F	F	F	0	F	clr	F	T	T
cefc power status down	cefc power status changed	cefc power status down	physical-command	IModule	F	T	T	0	T	maj	F	T	T
cefc power status up	cefc power status changed	cefc power status up	physical-command	IModule	F	F	F	0	F	clr	F	T	T
cefc FRU inserted	cefc fru removed	cefc fan status up	physical-command	IModule	F	F	F	0	T	clr	F	T	T
cefc FRU removed	cefc fru removed	cefc fru removed	physical-command	IModule	F	T	T	0	T	maj	F	T	T
sensor value crossed threshold in entSensorThresholdTable	entity sensor threshold notification	entity sensor threshold notification	N	IManagedElement	F	F	F	0	F	maj	T	T	T
cps IfVlan Secure MacAddr Violation Trap	cps-IfVlan-Secure-MacAddr-Violation-Trap	cps-IfVlan-Secure-MacAddr-Violation-Trap	N	IPortLayer1	F	F	T	0	F	maj	T	T	F
cps Secure MacAddr Violation Trap	cps-Secure-MacAddr-Violation-Trap	cps-Secure-MacAddr-Violation-Trap	N	IPortLayer1	F	F	T	0	F	maj	T	T	F

Table 16-28 Cisco Nexus V2/V3 Trap Registry Parameters (continued)

Short Description	Event Type	Event Subtype	Expedites Polling	Event Source (IMO Name)	Activate Flow	Correlate	Is Correlation Allowed	Weight	Auto Clear	Severity	Is Ticketable	Auto Remove	Flapping
Stpx Pvid Inconsistency Trap	stpx port inconsistency update	PvidInconsistent trap	N	IManagedElement	F	T	F	0	F	info	F	T	F
Stpx Type Inconsistency Trap	stpx port inconsistency update	TypeInconsistent trap	N	IManagedElement	F	T	F	0	F	info	F	T	F
stpx loop inconsistency discovered	stpx loop inconsistency update	stpx loop inconsistency discovered	N	IManagedElement	F	T	F	0	F	maj	T	T	F
stpx loop inconsistency resolved	stpx loop inconsistency update	stpx loop inconsistency resolved	N	IManagedElement	F	F	F	0	F	clr	T	T	F
stpx root inconsistency discovered	stpx root inconsistency update	stpx root inconsistency discovered	N	IManagedElement	F	T	F	0	F	maj	T	T	F
stpx root inconsistency resolved	stpx root inconsistency update	stpx root inconsistency resolved	N	IManagedElement	F	F	F	0	F	clr	T	T	F
SNMP Link down	snmp link down	snmp link down	ip interface oper status,port-status	IPhysicalLayer	F	T	F	0	T	min	F	T	T
SNMP Link up	snmp link down	snmp link up	ip interface oper status,port-status	IPhysicalLayer	F	T	F	0	F	clr	F	T	T
RMON Rising Alarm	RMON-Alarm-Trap	Rising Alarm	N	IManagedElement	F	T	F	0	T	WARNING	F	T	F
RMON Falling Alarm	RMON-Alarm-Trap	Falling Alarm	N	IManagedElement	F	T	F	0	T	WARNING	F	T	F
Cold start trap	cold start trap	cold start trap	N	IManagedElement	F	F	T	190000	F	info	T	T	F
OSPF virtual interface state changed to Down	ospf virtual if state down	ospf virtual if state down	N	IManagedElement	F	T	T	0	F	min	F	T	T

Table 16-28 Cisco Nexus V2/V3 Trap Registry Parameters (continued)

Short Description	Event Type	Event Subtype	Expedites Polling	Event Source (IMO Name)	Activate Flow	Correlate	Is Correlation Allowed	Weight	Auto Clear	Severity	Is Ticketable	Auto Remove	Flapping
OSPF neighbor state down	ospf neighbor state down	ospf neighbor state down	N	IManagedElement	T	T	T	0	F	maj	T	T	T
OSPF neighbor state up	ospf neighbor state down	ospf neighbor state up	N	IManagedElement	F	F	F	0	F	clr	F	T	T
OSPF virtual neighbor state down	ospf-virtual-neighbor-state-changed	ospf-virtual-neighbor-state-down	N	IManagedElement	T	T	T	0	F	min	T	T	T
OSPF virtual neighbor state up	ospf-virtual-neighbor-state-changed	ospf-virtual-neighbor-state-up	N	IManagedElement	F	F	F	0	F	clr	F	T	T
OSPF interface configuration error	ospf-if-config-err	ospf-if-config-err	N	IManagedElement	F	T	F	0	F	wrn	T	T	F
OSPF virtual interface configuration error	ospf-virtual-if-config-err	ospf-virtual-if-config-err	N	IManagedElement	F	T	F	0	F	min	F	T	F
OSPF interface authentication failure	ospf-if-authentic-fail	ospf-if-authentic-fail	N	IManagedElement	F	T	F	0	F	wrn	T	T	F
OSPF virtual interface authentication failure	ospf-virtual-if-authentic-fail	ospf-virtual-if-authentic-fail	N	IManagedElement	F	T	F	0	F	wrn	T	T	F
OSPF bad packet received	ospf-if-bad-packet	ospf-if-bad-packet	N	IManagedElement	F	T	F	0	T	min	F	T	F
OSPF bad packet received on virtual interface	ospf-virtual-if-bad-packet	ospf-virtual-if-bad-packet	N	IManagedElement	F	T	F	0	T	min	F	T	F
OSPF packet retransmitted	ospf-if-packet-retransmit	ospf-if-packet-retransmit	N	IManagedElement	F	T	F	0	T	min	F	T	F
OSPF packet retransmitted on virtual interface	ospf-virtual-if-packet-retransmit	ospf-virtual-if-packet-retransmit	N	IManagedElement	F	T	F	0	T	min	F	T	F
OSPF new LSA originated	ospf-new-lsa-originated	ospf-new-lsa-originated	N	IManagedElement	F	T	F	0	T	min	F	T	F
OSPF LSA aged to MaxAge	ospf-lsa-reached-maxage	ospf-lsa-reached-maxage	N	IManagedElement	F	F	F	0	F	info	F	T	F
OSPF lsdb overflow trap	ospf lsdb overflow trap	ospf lsdb overflow trap	N	IManagedElement	F	T	F	0	T	MINOR	F	T	F

Table 16-28 Cisco Nexus V2/V3 Trap Registry Parameters (continued)

Short Description	Event Type	Event Subtype	Expedites Polling	Event Source (IMO Name)	Activate Flow	Correlate	Is Correlation Allowed	Weight	Auto Clear	Severity	Is Ticketable	Auto Remove	Flapping
OSPF lsdb approaching overflow trap	ospf lsdb approaching overflow trap	ospf lsdb approaching overflow trap	N	IManagedElement	F	T	F	0	T	MINOR	F	T	F
OSPF interface state changed to Down	ospf if state down	ospf if state down	N	IManagedElement	F	T	T	0	F	info	F	T	T
OSPF interface state changed to Up	ospf if state down	ospf if state up	N	IManagedElement	F	F	F	0	F	clr	F	T	T
OSPF NSSA translator status change trap	ospf-status-change-trap	ospf nssa translator status change trap	N	IManagedElement	F	F	F	0	F	info	F	T	F
OSPF restart status change trap	ospf-status-change-trap	ospf restart status change trap	N	IManagedElement	F	F	F	0	F	info	F	T	F
OSPF neighbor restart helper status change trap	ospf-status-change-trap	ospf nbr restart helper status change trap	N	IManagedElement	F	F	F	0	F	info	F	T	F
OSPF virtual neighbor restart helper status change trap	ospf-status-change-trap	ospf virt nbr restart helper status change trap	N	IManagedElement	F	F	F	0	F	info	F	T	F

Cisco CPT V2 Trap Registry Parameters

Table 16-29 lists the associated event types, event subtypes, and Prime Network registry parameters for the Cisco CPT V2 traps shown in Table 16-13.

Table 16-29 Cisco CPT V2 Trap Registry Parameters

Short Description	Event Type	Event Subtype	Expedites Polling	Event Source (IMO Name)	Activate Flow	Correlate	Is Correlation Allowed	Weight	Auto Clear	Severity	Is Ticketable	Auto Remove	Flapping
Improper Removal	Improper Removal	Improper Removal	N	IManagedElement	F	F	F	0	F	maj	T	T	F
Improper Removal Cleared	Improper Removal	Improper Removal Cleared	N	IManagedElement	F	F	F	0	F	clr	F	T	F
Cold Restart	Cold Restart	Cold Restart	N	IManagedElement	F	F	F	0	F	maj		T	F
Cold Restart Cleared	Cold Restart	Cold Restart Cleared	N	IManagedElement	F	F	F	0	F	clr		T	F

Cisco ASR 5000 Series V2 Trap Registry Parameters

Table 16-30 lists the associated event types, event subtypes, and Prime Network registry parameters for the Cisco ASR 5000 series V2 traps shown in Table 16-14.

Table 16-30 Cisco ASR 5000 Series V2Trap Registry Parameters

Short Description	Event Type	Event Subtype	Expedites Polling	Event Source (IMO Name)	Activate Flow	Correlate	Is Correlation Allowed	Weight	Auto Clear	Severity	Is Ticketable	Auto Remove	Flapping
Card Removed	asr5kCardRemoved	asr5kCardRemoved	N	IModule	F	T	T	0	F	critical	T	T	F
Card Inserted	asr5kCardRemoved	asr5kCardInserted	N	IModule	F	T	T	0	F	clr	T	T	F
Card Reboot Request	asr5kCardRebootRequest	asr5kCardRebootRequest	N	IModule	F	T	T	0	F	maj	T	T	F
Card Voltage Failure	asr5kCardUp	asr5kCardVoltageFailure	N	IModule	F	T	T	0	F	critical	T	T	F
Card Mismatch	asr5kCardUp	asr5kCardMismatch	N	IModule	F	T	T	0	F	maj	T	T	F
Raid Fail	asr5kRaidStatus	asr5kRaidFailed	N	IManagedElement	F	F	F	0	F	maj	T	T	F

Table 16-30 Cisco ASR 5000 Series V2Trap Registry Parameters (continued)

Short Description	Event Type	Event Subtype	Expedites Polling	Event Source (IMO Name)	Activate Flow	Correlate	Is Correlation Allowed	Weight	Auto Clear	Severity	Is Ticketable	Auto Remove	Flapping
Raid Start	asr5kRaidStatus	asr5kRaidStarted	N	IManagedElement	F	F	F	0	F	clr	T	T	F
GGSN Service Stop	asr5kGGSNServiceState	asr5kGGSNServiceStop	N	IManagedElement	F	F	F	0	F	critical	T	T	F
Card Removed	asr5kCardRemoved	asr5kCardRemoved	N	IModule	F	T	T	0	F	critical	T	T	F
Server Cluster State Change	asr5kStrgSrvrClusStateChange	asr5kStrgSrvrClusStateChange	N	IManagedElement	F	F	F	0	F	clr	T	T	F
Server Cluster SwitchOver	asr5kStrgSrvrClusStateChange	asr5kStrgSrvrClusSwitchover	N	IManagedElement	F	F	F	0	F	critical	T	T	F
The threshold condition is now clear	asr5kThreshCDRFlowControl	asr5kThreshClearCDRFlowControl	N	IManagedElement	F	F	F	0	F	clr	F	T	F
Raid Recovered	asr5kRaidRecovered	asr5kRaidRecovered	N	IManagedElement	F	F	F	0	F	clr	T	T	F
Raid Degraded	asr5kRaidRecovered	asr5kRaidDegraded	N	IManagedElement	F	F	F	0	F	maj	T	T	F
Export Unacknowledged GCDRs from Backup DB	asr5kUnackedGcdrFileGen	asr5kUnackedGcdrFileGen	N	IManagedElement	F	F	F	0	F	clr	T	T	F
Unacknowledged GCDRs Volume Purge	asr5kUnackedGcdrFileGen	asr5kUnackedGcdrVolPurge	N	IManagedElement	F	F	F	0	F	critical	T	T	F
OSPF v3 Neighbour Full	asr5kOSPFv3NeighbourDown	asr5kOSPFv3NeighbourFull	N	IManagedElement	F	F	F	0	F	clr	T	T	F
The threshold condition is now clear	asr5kThreshLMASessions	asr5kThreshClearLMASessions	N	IManagedElement	F	F	F	0	F	clr	F	T	F
The total number of LMA sessions is above the configured threshold value	asr5kThreshLMASessions	asr5kThreshLMASessions	N	IManagedElement	F	F	F	0	F	warning	F	T	F
OSPF Neighbour Full	asr5kOSPFNeighbourDown	asr5kOSPFNeighbourFull	N	IManagedElement	F	F	F	0	F	clr	T	T	F

Table 16-30 Cisco ASR 5000 Series V2Trap Registry Parameters (continued)

Short Description	Event Type	Event Subtype	Expedites Polling	Event Source (IMO Name)	Activate Flow	Correlate	Is Correlation Allowed	Weight	Auto Clear	Severity	Is Ticketable	Auto Remove	Flapping
OSPF Neighbour Down	asr5kOSPFNeighbourDown	asr5kOSPFNeighbourDown	N	IManagedElement	F	F	F	0	F	minor	T	T	F
GPRS Sessions Threshold Cleared	asr5kThreshGPRSSessions	asr5kThreshClearGPRSSessions	N	IManagedElement	F	F	F	0	F	clr	F	T	F
The threshold condition is now clear	asr5kThreshMAGSessions	asr5kThreshClearMAGSessions	N	IManagedElement	F	F	F	0	F	clr	F	T	F
GPRS Sessions Threshold	asr5kThreshGPRSSessions	asr5kThreshGPRSSessions	N	IManagedElement	F	F	F	0	F	warning	F	T	F
The total number of MAG sessions is above the configured threshold value	asr5kThreshMAGSessions	asr5kThreshMAGSessions	N	IManagedElement	F	F	F	0	F	warning	F	T	F
Certificate is approaching its expiration	asr5kCertShortLifetime	asr5kCertShortLifetime	N	IManagedElement	F	F	F	0	F	warning	F	T	F
Cleared IP Pool Threshold Available	asr5kThreshIPPoolAvail	asr5kThreshClearIPPoolAvail	N	IManagedElement	F	F	F	0	F	clr	T	T	F
The NAT port chunks utilization of NAT pool is above the configured	asr5kThreshNAPTPortChunks	asr5kThreshNAPTPortChunks	N	IManagedElement	F	F	F	0	F	warning	F	T	F
IP Pool Threshold Available	asr5kThreshIPPoolAvail	asr5kThreshIPPoolAvail	N	IManagedElement	F	F	F	0	F	warning	T	T	F
Storage Utilization Threshold is now clear	asr5kThreshStorageUtilization	asr5kThreshClearStorageUtilization	N	IManagedElement	F	F	F	0	F	clr	F	T	F
Storage Utilization Reached Threshold	asr5kThreshStorageUtilization	asr5kThreshStorageUtilization	N	IManagedElement	F	F	F	0	F	warning	F	T	F

Table 16-30 Cisco ASR 5000 Series V2Trap Registry Parameters (continued)

Short Description	Event Type	Event Subtype	Expedites Polling	Event Source (IMO Name)	Activate Flow	Correlate	Is Correlation Allowed	Weight	Auto Clear	Severity	Is Ticketable	Auto Remove	Flapping
Number of GPRS sessions in a service is above the threshold	asr5kThreshPerServiceGPRSSessions	asr5kThreshPerServiceGPRSSessions	N	IManagedElement	F	F	F	0	F	warning	F	T	F
GPRS Pdp Sessions Threshold Cleared	asr5kThreshGPRSPdpSessions	asr5kThreshClearGPRSPdpSessions	N	IManagedElement	F	F	F	0	F	clr	F	T	F
GPRS Pdp Sessions Threshold	asr5kThreshGPRSPdpSessions	asr5kThreshGPRSPdpSessions	N	IManagedElement	F	F	F	0	F	warning	F	T	F
Number of GPRS PDP sessions in a service is above the threshold value	asr5kThreshPerServiceGPRSPdpSessions	asr5kThreshPerServiceGPRSPdpSessions	N	IManagedElement	F	F	F	0	F	warning	F	T	F
CPU Load Threshold Cleared	asr5kThreshCPULoad	asr5kThreshClearCPULoad	N	IManagedElement	F	F	F	0	F	clr	F	T	F
The threshold condition cleared	asr5kThreshPerServiceGPRSSessions	asr5kThreshClearPerServiceGPRSSessions	N	IManagedElement	F	F	F	0	F	clr	F	T	F
CPU Load Threshold	asr5kThreshCPULoad	asr5kThreshCPULoad	N	IManagedElement	F	F	F	0	F	warning	F	T	F
Number of PCC-Quota sessions is above the threshold value	asr5kThreshPCCQuotaSessions	asr5kThreshPCCQuotaSessions	N	IManagedElement	F	F	F	0	F	warning	F	T	F
The threshold condition cleared	asr5kThreshPerServicePCCPolicySessions	asr5kThreshClearPerServicePCCPolicySessions	N	IManagedElement	F	F	F	0	F	clr	F	T	F
System Startup	asr5kSystemStartup	asr5kSystemStartup	N	IManagedElement	F	F	F	0	F	info	F	T	F
The threshold condition cleared	asr5kThreshPCCQuotaSessions	asr5kThreshClearPCCQuotaSessions	N	IManagedElement	F	F	F	0	F	clr	F	T	F
Licence Expired	asr5kLicenseExpired	asr5kLicenseExpired	N	IManagedElement	F	F	F	0	F	warning	F	T	F

Table 16-30 Cisco ASR 5000 Series V2Trap Registry Parameters (continued)

Short Description	Event Type	Event Subtype	Expedites Polling	Event Source (IMO Name)	Activate Flow	Correlate	Is Correlation Allowed	Weight	Auto Clear	Severity	Is Ticketable	Auto Remove	Flapping
Number of PCC-Policy sessions is above the threshold value	asr5kThreshPCCPolicySessions	asr5kThreshPCCPolicySessions	N	IManagedElement	F	F	F	0	F	warning	F	T	F
PPP Setup FailRate Threshold Cleared	asr5kThreshPPPSetupFailRate	asr5kThreshClearPPPSetupFailRate	N	IManagedElement	F	F	F	0	F	clr	F	T	F
The threshold condition cleared	asr5kThreshPerServiceGPRSPdpSessions	asr5kThreshClearPerServiceGPRSPdpSessions	N	IManagedElement	F	F	F	0	F	clr	F	T	F
PPP Setup FailRate Threshold	asr5kThreshPPPSetupFailRate	asr5kThreshPPPSetupFailRate	N	IManagedElement	F	F	F	0	F	warning	F	T	F
Number of PCC-Policy sessions in a service is above the threshold value	asr5kThreshPerServicePCCPolicySessions	asr5kThreshPerServicePCCPolicySessions	N	IManagedElement	F	F	F	0	F	warning	F	T	F
CPU Memory Usage Threhold cleared	asr5kThreshCPUMemUsage	asr5kThreshClearCPUMemUsage	N	IManagedElement	F	F	F	0	F	clr	F	T	F
The threshold condition cleared	asr5kThreshPCCPolicySessions	asr5kThreshClearPCCPolicySessions	N	IManagedElement	F	F	F	0	F	clr	F	T	F
CPU Memory Usage Threhold reached	asr5kThreshCPUMemUsage	asr5kThreshCPUMemUsage	N	IManagedElement	F	F	F	0	F	warning	F	T	F
The threshold condition is now clear	asr5kThreshPacketsFilteredDropped	asr5kThreshClearPacketsFilteredDropped	N	IManagedElement	F	F	F	0	F	clr	F	T	F
The threshold condition is now clear	asr5kThreshCallRejectNoResource	asr5kThreshClearCallRejectNoResource	N	IManagedElement	F	F	F	0	F	clr	F	T	F

Table 16-30 Cisco ASR 5000 Series V2Trap Registry Parameters (continued)

Short Description	Event Type	Event Subtype	Expedites Polling	Event Source (IMO Name)	Activate Flow	Correlate	Is Correlation Allowed	Weight	Auto Clear	Severity	Is Ticketable	Auto Remove	Flapping
User data packets filtered has exceeded the configured threshold	asr5kThreshPacketsFilteredDropped	asr5kThreshPacketsFilteredDropped	N	IManagedElement	F	F	F	0	F	warning	F	T	F
System Reboot	asr5kSystemReboot	asr5kSystemReboot	N	IManagedElement	F	F	F	0	F	info	F	T	F
Card Temperature Threshold NearPowerOffLimit Cleared	asr5kThreshCardTemperatureNearPowerOffLimit	asr5kThreshClearCardTemperatureNearPowerOffLimit	N	IManagedElement	F	F	F	0	F	clr	T	T	F
Card Temperature Threshold NearPowerOffLimit	asr5kThreshCardTemperatureNearPowerOffLimit	asr5kThreshCardTemperatureNearPowerOffLimit	N	IManagedElement	F	F	F	0	F	maj	T	T	F
System Capacity Threshold Cleared	asr5kThreshSystemCapacity	asr5kThreshClearSystemCapacity	N	IManagedElement	F	F	F	0	F	clr	F	T	F
System Capacity Reached Threshold	asr5kThreshSystemCapacity	asr5kThreshSystemCapacity	N	IManagedElement	F	F	F	0	F	warning	F	T	F
The threshold condition is now clear.	asr5kThreshAAAAcctArchive	asr5kThreshClearAAAAcctArchive	N	IManagedElement	F	F	F	0	F	clr	F	T	F
The AAA accounting archive size has gone above the configured	asr5kThreshAAAAcctArchive	asr5kThreshAAAAcctArchive	N	IManagedElement	F	F	F	0	F	warning	F	T	F
The threshold condition is now clear.	asr5kThreshPerServiceHASessions	asr5kThreshClearPerServiceHASessions	N	IManagedElement	F	F	F	0	F	clr	F	T	F
Number of HA sessions in a service is above the configured threshold	asr5kThreshPerServiceHASessions	asr5kThreshPerServiceHASessions	N	IManagedElement	F	F	F	0	F	warning	F	T	F
The threshold condition is now clear	asr5kThreshDCCAProtocolErrors	asr5kThreshClearDCCAProtocolErrors	N	IManagedElement	F	F	F	0	F	clr	F	T	F

Table 16-30 Cisco ASR 5000 Series V2Trap Registry Parameters (continued)

Short Description	Event Type	Event Subtype	Expedites Polling	Event Source (IMO Name)	Activate Flow	Correlate	Is Correlation Allowed	Weight	Auto Clear	Severity	Is Ticketable	Auto Remove	Flapping
The number of DCCA Protocol Errors has exceeded the configured threshold	asr5kThreshDCCAProtocolErrors	asr5kThreshDCCAProtocolErrors	N	IManagedElement	F	F	F	0	F	warning	F	T	F
The threshold condition is now clear	asr5kThreshAAAMgrQueue	asr5kThreshClearAAAMgrQueue	N	IManagedElement	F	F	F	0	F	clr	F	T	F
The Per-AAA Manager internal request queue usage has gone above the configured threshold	asr5kThreshAAAMgrQueue	asr5kThreshAAAMgrQueue	N	IManagedElement	F	F	F	0	F	warning	F	T	F
The number of DCCA BadAnswers has exceeded the configured threshold	asr5kThreshDCCABadAnswers	asr5kThreshDCCABadAnswers	N	IManagedElement	F	F	F	0	F	warning	F	T	F
Power Filter Unit Unavailable	asr5kPowerFilterUnitAvail	asr5kPowerFilterUnitUnavail	N	IManagedElement	F	F	F	0	F	maj	T	T	F
The threshold condition is now clear	asr5kThreshDCCABadAnswers	asr5kThreshClearDCCABadAnswers	N	IManagedElement	F	F	F	0	F	clr	F	T	F
Power Filter Unit Available	asr5kPowerFilterUnitAvail	asr5kPowerFilterUnitAvail	N	IManagedElement	F	F	F	0	F	clr	T	T	F
NPU ARP Pool Exhausted	asr5kNPUARPPoolExhausted	asr5kNPUARPPoolExhausted	N	IManagedElement	F	F	F	0	F	maj	T	T	F
Power Filter Unit Failed	asr5kPowerFilterUnitAvail	asr5kPowerFilterUnitFailed	N	IManagedElement	F	F	F	0	F	maj	T	T	F
GGSN Service Start	asr5kGGSNServiceState	asr5kGGSNServiceStart	N	IManagedElement	F	F	F	0	F	clr	T	T	F

Table 16-30 Cisco ASR 5000 Series V2Trap Registry Parameters (continued)

Short Description	Event Type	Event Subtype	Expedites Polling	Event Source (IMO Name)	Activate Flow	Correlate	Is Correlation Allowed	Weight	Auto Clear	Severity	Is Ticketable	Auto Remove	Flapping
The number of DCCA UnknownRating Group has exceeded the configured threshold	asr5kThreshDCCAUnknownRatingGroup	asr5kThreshDCCAUnknownRatingGroup	N	IManagedElement	F	F	F	0	F	warning	F	T	F
The number of DCCA RatingFailed has exceeded the configured threshold	asr5kThreshDCCARatingFailed	asr5kThreshDCCARatingFailed	N	IManagedElement	F	F	F	0	F	warning	F	T	F
The threshold condition is now clear	asr5kThreshDCCAUnknownRatingGroup	asr5kThreshClearDCCAUnknownRatingGroup	N	IManagedElement	F	F	F	0	F	clr	F	T	F
The CDR file space usage is above the configured threshold percentage	asr5kThreshCDRFileSpace	asr5kThreshCDRFileSpace	N	IManagedElement	F	F	F	0	F	warning	F	T	F
The threshold condition is now clear	asr5kThreshDCCARatingFailed	asr5kThreshClearDCCARatingFailed	N	IManagedElement	F	F	F	0	F	clr	F	T	F
The EDR file space usage is above the configured threshold percentage	asr5kThreshEDRFileSpace	asr5kThreshEDRFileSpace	N	IManagedElement	F	F	F	0	F	warning	F	T	F
The threshold condition is now clear	asr5kThreshCDRFileSpac	asr5kThreshClearCDRFileSpace	N	IManagedElement	F	F	F	0	F	clr	F	T	F
The number of CDR records which have been discarded at an ACSMGR	asr5kThreshCDRFlowControl	asr5kThreshCDRFlowControl	N	IManagedElement	F	F	F	0	F	info	F	T	F
The threshold condition is now clear	asr5kThreshEDRFileSpace	asr5kThreshClearEDRFileSpace	N	IManagedElement	F	F	F	0	F	clr	F	T	F

Table 16-30 Cisco ASR 5000 Series V2Trap Registry Parameters (continued)

Short Description	Event Type	Event Subtype	Expedites Polling	Event Source (IMO Name)	Activate Flow	Correlate	Is Correlation Allowed	Weight	Auto Clear	Severity	Is Ticketable	Auto Remove	Flapping
AAA auth requests exceeded threshold	asr5kThreshAAAAuthFailRate	asr5kThreshAAAAuthFailRate	N	IManagedElement	F	F	F	0	F	warning	F	T	F
The threshold condition is cleared	asr5kThreshAAAAuthFailRate	asr5kThreshClearAAAAuthFailRate	N	IManagedElement	F	F	F	0	F	clr	F	T	F
Number of AAA authentication failures exceeded	asr5kThreshAAAAuthFail	asr5kThreshAAAAuthFail	N	IManagedElement	F	F	F	0	F	warning	F	T	F
The threshold condition is cleared	asr5kThreshAAAAuthFail	asr5kThreshClearAAAAuthFail	N	IManagedElement	F	F	F	0	F	clr	F	T	F
Number of subscribers above configured threshold value	asr5kThreshSubscriberTotal	asr5kThreshSubscriberTotal	N	IManagedElement	F	F	F	0	F	warning	F	T	F
The threshold condition is cleared	asr5kThreshSubscriberTotal	asr5kThreshClearSubscriberTotal	N	IManagedElement	F	F	F	0	F	clr	F	T	F
The IPCF Event Notification Interface peer cannot be reached	asr5kPCCNtfyIntfPeerUnreachable	asr5kPCCNtfyIntfPeerUnreachable	N	IManagedElement	F	F	F	0	F	maj	T	T	F
Original Lawful Intercept configured by Admin	asr5kLawfulInterceptChanged	asr5kLawfulInterceptChanged	N	IManagedElement	F	F	F	0	F	info	F	T	F
Number of TPO low compression gain is above the configured	asr5kThreshTpoLowCompressionGain	asr5kThreshTpoLowCompressionGain	N	IManagedElement	F	F	F	0	F	warning	F	T	F
The Notification Interface peer can be reached	asr5kPCCNtfyIntfPeerUnreachable	asr5kPCCNtfyIntfPeerReachable	N	IManagedElement	F	F	F	0	F	clr	T	T	F
CDRs purged	asr5kCdrPurged	asr5kCdrPurged	N	IManagedElement	F	F	F	0	F	warning	F	T	F

Table 16-30 Cisco ASR 5000 Series V2Trap Registry Parameters (continued)

Short Description	Event Type	Event Subtype	Expedites Polling	Event Source (IMO Name)	Activate Flow	Correlate	Is Correlation Allowed	Weight	Auto Clear	Severity	Is Ticketable	Auto Remove	Flapping
Capability negotiations has failed and connections are down	asr5kDiameterCapabilitiesExchangeFailure	asr5kDiameterCapabilitiesExchangeFailure	N	IManagedElement	F	F	F	0	F	maj	T	T	F
The threshold condition cleared	asr5kThreshTpoLowCompressionGain	asr5kThreshClearTpoLowCompressionGain	N	IManagedElement	F	F	F	0	F	clr	F	T	F
A diameter peer is down	asr5kDiameterIpv6PeerDown	asr5kDiameterIpv6PeerDown	N	IManagedElement	F	F	F	0	F	maj	T	T	F
A diameter server is up	asr5kDiameterCapabilitiesExchangeFailure	asr5kDiameterCapabilitiesExchangeSuccess	N	IManagedElement	F	F	F	0	F	clr	T	T	F
A diameter peer is up	asr5kDiameterIpv6PeerDown	asr5kDiameterIpv6PeerUp	N	IManagedElement	F	F	F	0	F	clr	T	T	F
The threshold condition is cleared.	asr5kThreshAAAAcctFail	asr5kThreshClearAAAAcctFail	N	IManagedElement	F	F	F	0	F	clr	F	T	F
AAA accounting exceeded threshold	asr5kThreshAAAAcctFail	asr5kThreshAAAAcctFail	N	IManagedElement	F	F	F	0	F	warning	F	T	F
The threshold condition is now clear	asr5kThreshAAAAcctFailRate	asr5kThreshClearAAAAcctFailRate	N	IManagedElement	F	F	F	0	F	clr	F	T	F
AAA accounting requests exceeded threshold	asr5kThreshAAAAcctFailRate	asr5kThreshAAAAcctFailRate	N	IManagedElement	F	F	F	0	F	warning	F	T	F
The threshold condition is now clear	asr5kThreshCallSetup	asr5kThreshClearCallSetup	N	IManagedElement	F	F	F	0	F	clr	F	T	F
Number of call setup operations exceeded threshold	asr5kThreshCallSetupFailure	asr5kThreshCallSetupFailure	N	IManagedElement	F	F	F	0	F	warning	F	T	F
The threshold condition is now clear	asr5kThreshCallSetupFailure	asr5kThreshClearCallSetupFailure	N	IManagedElement	F	F	F	0	F	clr	F	T	F

Table 16-30 Cisco ASR 5000 Series V2Trap Registry Parameters (continued)

Short Description	Event Type	Event Subtype	Expedites Polling	Event Source (IMO Name)	Activate Flow	Correlate	Is Correlation Allowed	Weight	Auto Clear	Severity	Is Ticketable	Auto Remove	Flapping
Number of call setup operations rejected due to a no resource condition exceeded threshold	asr5kThreshCallRejectNoResource	asr5kThreshCallRejectNoResource	N	IManagedElement	F	F	F	0	F	warning	F	T	F
AAA requests exceeded threshold	asr5kThreshAAARetryRate	asr5kThreshAAARetryRate	N	IManagedElement	F	F	F	0	F	warning	F	T	F
The threshold condition is now clear.	asr5kThreshAAARetryRate	asr5kThreshClearAAARetryRate	N	IManagedElement	F	F	F	0	F	clr	F	T	F
A diameter server is up	asr5kDiameterServerUnreachable	asr5kDiameterServerReachable	N	IManagedElement	F	F	F	0	F	clr	T	T	F
number of call setup operations has exceeded threshold	asr5kThreshCallSetup	asr5kThreshCallSetup	N	IManagedElement	F	F	F	0	F	warning	F	T	F
CDR file has been deleted from the system	asr5kCDRFileRemoved	asr5kCDRFileRemoved	N	IManagedElement	F	F	F	0	F	maj	T	T	F
A diameter peer is up	asr5kDiameterPeerDown	asr5kDiameterPeerUp	N	IManagedElement	F	F	F	0	F	clr	T	T	F
A diameter server is down	asr5kDiameterServerUnreachable	asr5kDiameterServerUnreachable	N	IManagedElement	F	F	F	0	F	maj	T	T	F
The Per-Sessmgr Archive queue usage is above the configured threshold percentage	asr5kThreshAAAAcctArchiveQueue-1	asr5kThreshAAAAcctArchiveQueue-1	N	IManagedElement	F	F	F	0	F	warning	F	T	F
The threshold condition cleared	asr5kThreshAAAAcctArchiveQueue-1	asr5kThreshClearAAAAcctArchiveQueue-1	N	IManagedElement	F	F	F	0	F	clr	F	T	F
A diameter peer is down	asr5kDiameterPeerDown	asr5kDiameterPeerDown	N	IManagedElement	F	F	F	0	F	maj	T	T	F

Table 16-30 Cisco ASR 5000 Series V2Trap Registry Parameters (continued)

Short Description	Event Type	Event Subtype	Expedites Polling	Event Source (IMO Name)	Activate Flow	Correlate	Is Correlation Allowed	Weight	Auto Clear	Severity	Is Ticketable	Auto Remove	Flapping
The Sessmgr Archive queue usage is above the configured threshold percentage	asr5kThreshAAAAcctArchiveQueue-2	asr5kThreshAAAAcctArchiveQueue-2	N	IManagedElement	F	F	F	0	F	warning	F	T	F
GTPP CGF Server Dead	asr5kCgfAlive	asr5kCgfDead	N	IManagedElement	F	F	F	0	F	maj	T	T	F
The threshold condition cleared	asr5kThreshAAAAcctArchiveQueue-2	asr5kThreshClearAAAAcctArchiveQueue-2	N	IManagedElement	F	F	F	0	F	clr	F	T	F
GTPC Path Failure	asr5kGtpcPathFailure	asr5kGtpcPathFailure	N	IManagedElement	F	F	F	0	F	maj	T	T	F
The Sessmgr Archive queue usage is above the configured threshold percentage	asr5kThreshAAAAcctArchiveQueue-3	asr5kThreshAAAAcctArchiveQueue-3	N	IManagedElement	F	F	F	0	F	warning	F	T	F
The threshold condition cleared	asr5kThreshAAAAcctArchiveQueue-3	asr5kThreshClearAAAAcctArchiveQueue-3	N	IManagedElement	F	F	F	0	F	clr	F	T	F
GTPP CGF Server Alive	asr5kCgfAlive	asr5kCgfAlive	N	IManagedElement	F	F	F	0	F	clr	T	T	F
Periodic SNMP heartbeat	asr5kHeartbeat	asr5kHeartbeat	N	IManagedElement	F	F	F	0	F	info	F	T	F
The AAA server has been misconfigured	asr5kAAAAccServerUnreachable	asr5kAAAAccServerMisconfigured	N	IManagedElement	F	F	F	0	F	maj	T	T	F
GTP Data Path Failure	asr5kGtpuPathFailure	asr5kGtpuPathFailure	N	IManagedElement	F	F	F	0	F	maj	T	T	F
Archive started	asr5kAAAArchiveStarted	asr5kAAAArchiveStarted	N	IManagedElement	F	F	F	0	F	info	F	T	F
Threshold GGSN sessions	asr5kThreshGGSNSessions	asr5kThreshGGSNSessions	N	IManagedElement	F	F	F	0	F	warning	T	T	F
Storage Server CPU Normal	asr5kStorageServerCPU	asr5kStorageServerCPUNormal	N	IManagedElement	F	F	F	0	F	clr	T	T	F

Table 16-30 Cisco ASR 5000 Series V2Trap Registry Parameters (continued)

Short Description	Event Type	Event Subtype	Expedites Polling	Event Source (IMO Name)	Activate Flow	Correlate	Is Correlation Allowed	Weight	Auto Clear	Severity	Is Ticketable	Auto Remove	Flapping
GGSN initiate update failed	asr5kGgsnInitiatedUpdtFailed	asr5kGgsnInitiatedUpdtFailed	N	IManagedElement	F	F	F	0	F	info	F	T	F
SGW sessions is above the configured threshold value.	asr5kThreshSGWSessions	asr5kThreshSGWSessions	N	IManagedElement	F	F	F	0	F	warning	T	T	F
PGW Service stopped	asr5kPGWServiceStart	asr5kPGWServiceStop	N	IManagedElement	F	F	F	0	F	maj	T	T	F
PGW Service started	asr5kPGWServiceStart	asr5kPGWServiceStart	N	IManagedElement	F	F	F	0	F	clr	T	T	F
PGW sessions threshold condition cleared	asr5kThreshPGWSessions	asr5kThreshClearPGWSessions	N	IManagedElement	F	F	F	0	F	clr	T	T	F
PGW sessions are above the configured threshold value	asr5kThreshPGWSessions	asr5kThreshPGWSessions	N	IManagedElement	F	F	F	0	F	warning	T	T	F
Threshold Per Service GGSN Sessions Cleared	asr5kThreshPerServiceGGSNSessions	asr5kThreshClearPerServiceGGSNSessions	N	IManagedElement	F	F	F	0	F	clr	T	T	F
Threshold Per Service GGSN Sessions	asr5kThreshPerServiceGGSNSessions	asr5kThreshPerServiceGGSNSessions	N	IManagedElement	F	F	F	0	F	warning	T	T	F
Threshold GGSN sessions cleared	asr5kThreshGGSNSessions	asr5kThreshClearGGSNSessions	N	IManagedElement	F	F	F	0	F	clr	T	T	F
Service Overload	asr5kOverloadService	asr5kOverloadService	N	IManagedElement	F	F	F	0	F	maj	T	T	F
System Overload Cleared	asr5kOverloadSystem	asr5kOverloadSystemClear	N	IManagedElement	F	F	F	0	F	clr	T	T	F
Storage Server CPU Busy	asr5kStorageServerCPU	asr5kStorageServerCPUBusy	N	IManagedElement	F	F	F	0	F	maj	T	T	F
Service Overload Cleared	asr5kOverloadService	asr5kOverloadServiceClear	N	IManagedElement	F	F	F	0	F	clr	T	T	F

Table 16-30 Cisco ASR 5000 Series V2Trap Registry Parameters (continued)

Short Description	Event Type	Event Subtype	Expedites Polling	Event Source (IMO Name)	Activate Flow	Correlate	Is Correlation Allowed	Weight	Auto Clear	Severity	Is Ticketable	Auto Remove	Flapping
System Overload	asr5kOverloadSystem	asr5kOverloadSystem	N	IManagedElement	F	F	F	0	F	maj	T	T	F
A MVG peer is up	asr5kMVGPeerDown	asr5kMVGPeerUp	N	IManagedElement	F	F	F	0	F	clr	T	T	F
Storage Server DiskSpace Low	asr5kStorageServerDiskSpaceLow	asr5kStorageServerDiskSpaceLow	N	IManagedElement	F	F	F	0	F	maj	T	T	F
Storage Server Low DiskSpace Cleared	asr5kStorageServerDiskSpaceLo	asr5kStorageServerDiskSpaceOk	N	IManagedElement	F	F	F	0	F	clr	T	T	F
A SGTP Service has started	asr5kSGTPServiceStop	asr5kSGTPServiceStart	N	IManagedElement	F	F	F	0	F	clr	T	T	F
Task Failed	asr5kTaskFailed	asr5kTaskFailed	N	IManagedElement	F	F	F	0	F	maj	T	T	F
A MVG peer is down	asr5kMVGPeerDown	asr5kMVGPeerDown	N	IManagedElement	F	F	F	0	F	maj	T	T	F
Task Restarted	asr5kTaskFailed	asr5kTaskRestart	N	IManagedElement	F	F	F	0	F	clr	T	T	F
AAA AuthServer Unreachable	asr5kAAAAuthServerUnreachable	asr5kAAAAuthServerUnreachable	N	IManagedElement	F	F	F	0	F	maj	T	T	F
AAA AuthServer Reachable	asr5kAAAAuthServerUnreachable	asr5kAAAAuthServerReachable	N	IManagedElement	F	F	F	0	F	clr	T	T	F
AAA AccServer Unreachable	asr5kAAAAccServerUnreachable	asr5kAAAAccServerUnreachable	N	IManagedElement	F	F	F	0	F	maj	T	T	F
AAA AccServer Reachable	asr5kAAAAccServerUnreachable	asr5kAAAAccServerReachable	N	IManagedElement	F	F	F	0	F	clr	T	T	F
A PCC-Policy Service has started	asr5kPCCPolicyServiceStop	asr5kPCCPolicyServiceStart	N	IManagedElement	F	F	F	0	F	clr	T	T	F
A PCC-Quota Service has stopped	asr5kPCCQuotaServiceStop	asr5kPCCQuotaServiceStop	N	IManagedElement	F	F	F	0	F	maj	T	T	F
A PCC-Policy Service has stopped	asr5kPCCPolicyServiceStop	asr5kPCCPolicyServiceStop	N	IManagedElement	F	F	F	0	F	maj	T	T	F

Table 16-30 Cisco ASR 5000 Series V2Trap Registry Parameters (continued)

Short Description	Event Type	Event Subtype	Expedites Polling	Event Source (IMO Name)	Activate Flow	Correlate	Is Correlation Allowed	Weight	Auto Clear	Severity	Is Ticketable	Auto Remove	Flapping
A PCC-AF Service has started	asr5kPCCAFServiceStop	asr5kPCCAFServiceStart	N	IManagedElement	F	F	F	0	F	clr	T	T	F
A SGTP Service has stopped	asr5kSGTPServiceStop	asr5kSGTPServiceStop	N	IManagedElement	F	F	F	0	F	maj	T	T	F
A PCC-Quota Service has started	asr5kPCCQuotaServiceStop	asr5kPCCQuotaServiceStart	N	IManagedElement	F	F	F	0	F	clr	T	T	F
A PCC-AF Service has stopped	asr5kPCCAFServiceStop	asr5kPCCAFServiceStop	N	IManagedElement	F	F	F	0	F	maj	T	T	F
GTPP Storage Server Memory Low	asr5kStrgSrvrClusMemOK	asr5kStrgSrvrClusMemLow	N	IManagedElement	F	F	F	0	F	critical	T	T	F
Valid Certificate Configured	asr5kCertValid	asr5kCertValid	N	IManagedElement	F	F	F	0	F	clr	T	T	F
GTPP Storage Server Memory Normal	asr5kStrgSrvrClusMemOK	asr5kStrgSrvrClusMemOK	N	IManagedElement	F	F	F	0	F	clr	T	T	F
GTPP Storage Server Cluster Disk Path Failure Restored to OK	asr5kStrgSrvrClusPathOK	asr5kStrgSrvrClusPathOK	N	IManagedElement	F	F	F	0	F	clr	T	T	F
EGTP Control Path Failure condition is no longer valid.	asr5kEgtpcPathFailure	asr5kEgtpcPathFailureClear	N	IManagedElement	F	F	F	0	F	clr	T	T	F
No response received for GTP-U ECHO requests	asr5kEgtpuPathFailure	asr5kEgtpuPathFailure	N	IManagedElement	F	F	F	0	F	warning	F	T	F
GTPP Storage Server Cluster Transport Path Failure	asr5kStrgSrvrClusIntercOK	asr5kStrgSrvrClusIntercFail	N	IManagedElement	F	F	F	0	F	critical	T	T	F
The data path to the peer EPC node which was down is now available	asr5kEgtpuPathFailure	asr5kEgtpuPathFailureClear	N	IManagedElement	F	F	F	0	F	clr	F	T	F

Table 16-30 Cisco ASR 5000 Series V2Trap Registry Parameters (continued)

Short Description	Event Type	Event Subtype	Expedites Polling	Event Source (IMO Name)	Activate Flow	Correlate	Is Correlation Allowed	Weight	Auto Clear	Severity	Is Ticketable	Auto Remove	Flapping
GTPP Storage Server is experiencing CDR Loss greater than the configured threshold value at the GSS	asr5kStorageServerCDRLoss	asr5kStorageServerCDRLoss	N	IManagedElement	F	F	F	0	F	maj	T	T	F
GTPP Storage Server Cluster Disk Path Failure	asr5kStrgSrvrClusPathOK	asr5kStrgSrvrClusPathFail	N	IManagedElement	F	F	F	0	F	critical	T	T	F
GTPP Storage Server Cluster GE Interface Failure Restored to OK	asr5kStrgSrvrClusIfOK	asr5kStrgSrvrClusIfOK	N	IManagedElement	F	F	F	0	F	clr	T	T	F
Certificate Expired	asr5kCertValid	asr5kCertExpired	N	IManagedElement	F	F	F	0	F	critical	T	T	F
GTPP Storage Server Cluster Transport Path Failure Restored to OK	asr5kStrgSrvrClusIntercOK	asr5kStrgSrvrClusIntercOK	N	IManagedElement	F	F	F	0	F	clr	T	T	F
GTPP Storage Server Cluster GE Interface Failure	asr5kStrgSrvrClusIfOK	asr5kStrgSrvrClusIfFail	N	IManagedElement	F	F	F	0	F	critical	T	T	F
An Evolved GPRS Tunneling Protocol (EGTP) Service has started	asr5kEGTPServiceStop	asr5kEGTPServiceStart	N	IManagedElement	F	F	F	0	F	clr	T	T	F
A Local Mobility Anchor (LMA) Service has stopped	asr5kLMAServiceStop	asr5kLMAServiceStop	N	IManagedElement	F	F	F	0	F	maj	T	T	F
A Local Mobility Anchor (LMA) Service has started	asr5kLMAServiceStop	asr5kLMAServiceStart	N	IManagedElement	F	F	F	0	F	clr	T	T	F
A MAG Service has stopped	asr5kMAGServiceStop	asr5kMAGServiceStop	N	IManagedElement	F	F	F	0	F	maj	T	T	F

Table 16-30 Cisco ASR 5000 Series V2Trap Registry Parameters (continued)

Short Description	Event Type	Event Subtype	Expedites Polling	Event Source (IMO Name)	Activate Flow	Correlate	Is Correlation Allowed	Weight	Auto Clear	Severity	Is Ticketable	Auto Remove	Flapping
NTP Sync Established	asr5kNTPSyncLost	asr5kNTPSyncEstablished	N	IManagedElement	F	F	F	0	F	clr	T	T	F
NTP Sync lost	asr5kNTPSyncLost	asr5kNTPSyncLost	N	IManagedElement	F	F	F	0	F	maj	T	T	F
NTP Peer Reachable	asr5kNTPPeerUnreachable	asr5kNTPPeerReachable	N	IManagedElement	F	F	F	0	F	clr	T	T	F
NTP Peer UnReachable	asr5kNTPPeerUnreachable	asr5kNTPPeerUnreachable	N	IManagedElement	F	F	F	0	F	maj	T	T	F
Config change	asr5kConfigurationUpdate	asr5kConfigurationUpdate	N	IManagedElement	F	F	F	0	F	min	F	T	F
Link Up	SNMPLinkDown	SNMPLinkUp	N	IManagedElement	F	F	F	0	F	clr	T	T	F
Link Down	SNMPLinkDown	SNMPLinkDown	N	IManagedElement	F	F	F	0	F	min	T	T	F
SGW Service stopped	asr5kSGWServiceStart	asr5kSGWServiceStop	N	IManagedElement	F	F	F	0	F	maj	T	T	F
NTP Sync lost	asr5kBGPPeerSessionUp	asr5kBGPPeerSessionUp	N	IManagedElement	F	F	F	0	F	clr	T	T	F
BGP Peer Session Down	asr5kBGPPeerSessionUp	asr5kBGPPeerSessionDown	N	IManagedElement	F	F	F	0	F	maj	T	T	F
PCCA threshold condition cleared	asr5kThreshPCCAFSessions	asr5kThreshClearPCCAFSessions	N	IManagedElement	F	F	F	0	F	clr	T	T	F
Number of PCC-AF sessions is above the threshold value	asr5kThreshPCCAFSessions	asr5kThreshPCCAFSessions	N	IManagedElement	F	F	F	0	F	warning	T	T	F
SGW Sessions threshold condition cleared	asr5kThreshSGWSessions	asr5kThreshClearSGWSessions	N	IManagedElement	F	F	F	0	F	clr	T	T	F
Dhcp Service Started	asr5kDhcpServiceStarted	asr5kDhcpServiceStarted	N	IManagedElement	F	F	F	0	F	clr	T	T	F

Table 16-30 Cisco ASR 5000 Series V2Trap Registry Parameters (continued)

Short Description	Event Type	Event Subtype	Expedites Polling	Event Source (IMO Name)	Activate Flow	Correlate	Is Correlation Allowed	Weight	Auto Clear	Severity	Is Ticketable	Auto Remove	Flapping
Number of PCC-Quota sessions threshold condition cleared	asr5kThreshPerServicePCCQuotaSessions	asr5kThreshClearPerServicePCCQuotaSessions	N	IManagedElement	F	F	F	0	F	clr	F	T	F
SGW Service started	asr5kSGWServiceStart	asr5kSGWServiceStart	N	IManagedElement	F	F	F	0	F	clr	T	T	F
Number of PCC-Quota sessions threshold condition cleared	asr5kThreshPerServicePCCQuotaSessions	asr5kThreshPerServicePCCQuotaSessions	N	IManagedElement	F	F	F	0	F	warning	F	T	F
The threshold condition cleared	asr5kThreshDiameterRetryRate	asr5kThreshClearDiameterRetryRate	N	IManagedElement	F	F	F	0	F	clr	T	T	F
DHCP Alive	asr5kDhcpDead	asr5kDhcpAlive	N	IManagedElement	F	F	F	0	F	clr	T	T	F
The percentage of Diameter requests which has to be retried has exceeded the configured threshold	asr5kThreshDiameterRetryRate	asr5kThreshDiameterRetryRate	N	IManagedElement	F	F	F	0	F	warning	F	T	F
Dhcp Service Stopped	asr5kDhcpServiceStarted	asr5kDhcpServiceStopped	N	IManagedElement	F	F	F	0	F	maj	T	T	F
The threshold condition cleared	asr5kThreshPerServicePCCAFSessions	asr5kThreshClearPerServicePCCAFSessions	N	IManagedElement	F	F	F	0	F	clr	F	T	F
Storage Server Alive	asr5kStorageServerDead	asr5kStorageServerAlive	N	IManagedElement	F	F	F	0	F	clr	T	T	F
The threshold condition cleared	asr5kThreshPerServicePCCAFSessions	asr5kThreshPerServicePCCAFSessions	N	IManagedElement	F	F	F	0	F	clr	N	T	F
DHCP Dead	asr5kDhcpDead	asr5kDhcpDead	N	IManagedElement	F	F	F	0	F	maj	T	T	F
Service Loss LC	asr5kServiceLossLC	asr5kServiceLossLC	N	IManagedElement	F	F	F	0	F	critical	T	T	F

Table 16-30 Cisco ASR 5000 Series V2Trap Registry Parameters (continued)

Short Description	Event Type	Event Subtype	Expedites Polling	Event Source (IMO Name)	Activate Flow	Correlate	Is Correlation Allowed	Weight	Auto Clear	Severity	Is Ticketable	Auto Remove	Flapping
Storage Server Dead	asr5kStorageServerDead	asr5kStorageServerDead	N	IManagedElement	F	F	F	0	F	critical	T	T	F
Number of TPO RTO timeouts is above the configured	asr5kThreshTpoRtoTimeout	asr5kThreshTpoRtoTimeout	N	IManagedElement	F	F	F	0	F	warning	F	T	F
NPU Utilization Threshold reached	asr5kThreshNPUUtilization	asr5kThreshClearNPUUtilization	N	IManagedElement	F	F	F	0	F	clr	T	T	F
The chassis-wide count of current HNBGW IU sessions has gone above the configured threshold	asr5kThreshHNBGWIuSess	asr5kThreshHNBGWIuSess	N	IManagedElement	F	F	F	0	F	warning	F	T	F
Service Loss PTACs	asr5kServiceLossPTACs	asr5kServiceLossPTACs	N	IManagedElement	F	F	F	0	F	critical	T	T	F
NPU Utilization Threshold reached	asr5kThreshNPUUtilization	asr5kThreshNPUUtilization	N	IManagedElement	F	F	F	0	F	major	T	T	F
CLISession End	asr5kCLISession	asr5kCLISessionEnd	N	IManagedElement	F	F	F	0	F	info	F	T	F
CLISession start	asr5kCLISession	asr5kCLISessionStart	N	IManagedElement	F	F	F	0	F	info	F	T	F
Number of TPO RTO timeouts is above the configured	asr5kThreshTpoRtoTimeout	asr5kThreshClearTpoRtoTimeout	N	IManagedElement	F	F	F	0	F	warning	F	T	F
Thresh CPU Orbs Critical Cleared	asr5kThreshCPUOrbsCritical	asr5kThreshClearCPUOrbsCritical	N	IManagedElement	F	F	F	0	F	clr	T	T	F
The threshold condition cleared	asr5kThreshTpoDnsFailure	asr5kThreshClearTpoDnsFailure	N	IManagedElement	F	F	F	0	F	clr	F	T	F
Thresh CPU Orbs Critical	asr5kThreshCPUOrbsCritical	asr5kThreshCPUOrbsCritical	N	IManagedElement	F	F	F	0	F	critical	T	T	F

Table 16-30 Cisco ASR 5000 Series V2Trap Registry Parameters (continued)

Short Description	Event Type	Event Subtype	Expedites Polling	Event Source (IMO Name)	Activate Flow	Correlate	Is Correlation Allowed	Weight	Auto Clear	Severity	Is Ticketable	Auto Remove	Flapping
Number of TPO DNS query failure is above the configured threshold value	asr5kThreshTpoDnsFailure	asr5kThreshTpoDnsFailure	N	IManagedElement	F	F	F	0	F	warning	F	T	F
An IPMS server is reachable	asr5kIPMSServerUnreachable	asr5kIPMSServerReachable	N	IManagedElement	F	F	F	0	F	clr	T	T	F
An IPMS server is unreachable	asr5kIPMSServerUnreachable	asr5kIPMSServerUnreachable	N	IManagedElement	F	F	F	0	F	minor	T	T	F
License Exceeded	asr5kLicenseExceeded	asr5kLicenseExceeded	N	IManagedElement	F	F	F	0	F	maj	T	T	F
SS7 Point code Congestion gets cleared	asr5kSS7PCCongested	asr5kSS7PCCongestionCleared	N	IManagedElement	F	F	F	0	F	clr	T	T	F
Card SPOF Alarm Cleared	asr5kCardSPOFAlarm	asr5kCardSPOFClear	N	IManagedElement	F	F	F	0	F	clr	T	T	F
SS7 Point code Congestion gets cleared	asr5kSS7PCCongested	asr5kSS7PCCongested	N	IManagedElement	F	F	F	0	F	clr	T	T	F
Card SPOF Alarm	asr5kCardSPOFAlarm	asr5kCardSPOFAlarm	N	IManagedElement	F	F	F	0	F	maj	T	T	F
A GPRS Service has started	asr5kGPRSServiceStop	asr5kGPRSServiceStart	N	IManagedElement	F	F	F	0	F	clr	T	T	F
A GPRS Service has stopped	asr5kGPRSServiceStop	asr5kGPRSServiceStop	N	IManagedElement	F	F	F	0	F	maj	T	T	F
Storage Failed	asr5kStorageFailed	asr5kStorageFailed	N	IManagedElement	F	F	F	0	F	maj	T	T	F
OSPF v3 Neighbour Down	asr5kOSPFv3NeighbourDown	asr5kOSPFv3NeighbourDown	N	IManagedElement	F	F	F	0	F	min	T	T	F
An Evolved GPRS Tunneling Protocol (EGTP) Service has started	asr5kEGTPServiceStop	asr5kEGTPServiceStop	N	IManagedElement	F	F	F	0	F	clr	T	T	F
SRP Connection Up	asr5kSRPConnDown	asr5kSRPConnUp	N	IManagedElement	F	F	F	0	F	clr	T	T	F
SRP Connection Down	asr5kSRPConnDown	asr5kSRPConnDown	N	IManagedElement	F	F	F	0	F	min	T	T	F

Table 16-30 Cisco ASR 5000 Series V2Trap Registry Parameters (continued)

Short Description	Event Type	Event Subtype	Expedites Polling	Event Source (IMO Name)	Activate Flow	Correlate	Is Correlation Allowed	Weight	Auto Clear	Severity	Is Ticketable	Auto Remove	Flapping
License UnderLimit	asr5kLicense Exceeded	asr5kLicense UnderLimit	N	IManagedElement	F	F	F	0	F	clr	T	T	F
Fan Inserted	asr5kFanFailure	asr5kFanInserted	N	IManagedElement	F	F	F	0	F	clr	T	T	F
Fan Failed	asr5kFanFailure	asr5kFanFailed	N	IManagedElement	F	F	F	0	F	maj	T	T	F
Fan Removed	asr5kFanFailure	asr5kFanRemoved	N	IManagedElement	F	F	F	0	F	maj	T	T	F
Port Up	asr5kPortDown	asr5kPortUp	N	IManagedElement	F	F	F	0	F	clr	T	T	F
Port Down	asr5kPortDown	asr5kPortDown	N	IManagedElement	F	F	F	0	F	maj	T	T	F
Alerts Enabled	asr5kAlertsDisabled	asr5kAlertsEnabled	N	IManagedElement	F	F	F	0	F	clr	F	T	F
Alerts Disabled	asr5kAlertsDisabled	asr5kAlertsDisabled	N	IManagedElement	F	F	F	0	F	min	F	T	F
Log Msg	asr5kLogMsg	asr5kLogMsg	N	IManagedElement	F	F	F	0	F	min	F	T	F
Card Active	asr5kCardActive	asr5kCardActive	N	IManagedElement	F	F	F	0	F	clr	T	T	F
Card Up	asr5kCardUp	asr5kCardDown	N	IManagedElement	F	F	F	0	F	clr	T	T	F
EGTP Control Path Failure	asr5kEgtpcPathFailure	asr5kEgtpcPathFailure	N	IManagedElement	F	F	F	0	F	maj	T	T	F
A Mobile Access Gateway (MAG) Service has started	asr5kMAGServiceStop	asr5kMAGServiceStart	N	IManagedElement	F	F	F	0	F	clr	T	T	F
PAC Card Migration Started	asr5KCardPACMigrateStart	asr5KCardPACMigrateStart	N	IModule	F	T	T	0	F	maj	T	T	F
Card Temperature Over Heat	asr5kCardTempOverheat	asr5kCardTempOverheat	N	IModule	F	T	T	0	F	critical	T	T	F
Card Temperature OK	asr5kCardTempOverheat	asr5kCardTempOK	N	IModule	F	T	T	0	F	clr	T	T	F
Card Up	asr5kCardUp	asr5kCardUp	N	IModule	F	T	T	0	F	clr	T	T	F

Table 16-30 Cisco ASR 5000 Series V2Trap Registry Parameters (continued)

Short Description	Event Type	Event Subtype	Expedites Polling	Event Source (IMO Name)	Activate Flow	Correlate	Is Correlation Allowed	Weight	Auto Clear	Severity	Is Ticketable	Auto Remove	Flapping
CPU Memory Low Clear	asr5kCpuMemoryLow	asr5kCpuMemoryLowClear	N	IModule	F	T	T	0	F	clr	T	T	F
CPU Busy Clear	asr5kCpuBusy	asr5kCpuBusyClear	N	IModule	F	T	T	0	F	clr	T	T	F
Critical Task Failed	asr5kCardUp	asr5kCritTaskFailed	N	IModule	F	T	T	0	F	critical	T	T	F
Card Boot Failed	asr5KCardBootFailed	asr5KCardBootFailed	N	IModule	F	T	T	0	F	maj	T	T	F
SPC Card SwitchOver Failed	asr5kCardUp	asr5KCardSPCSwitchoverFailed	N	IModule	F	T	T	0	F	critical	T	T	F
SPC Card Switchover Completed	asr5KCardSPCSwitchoverStart	asr5KCardSPCSwitchoverComplete	N	IModule	F	T	T	0	F	clr	T	T	F
SPC Card Switchover Started	asr5KCardSPCSwitchoverStart	asr5KCardSPCSwitchoverStart	N	IModule	F	T	T	0	F	maj	T	T	F
PAC Card Migration Failed	asr5kCardUp	asr5KCardPACMigrateFailed	N	IModule	F	T	T	0	F	maj	T	T	F
PAC Card Migration Completed	asr5KCardPACMigrateStart	asr5KCardPACMigrateComplete	N	IModule	F	T	T	0	F	clr	T	T	F
CPU WatchDog Expired	asr5kCardUp	asr5kCpuWatchDogExpired	N	IModule	F	T	T	0	F	critical	T	T	F
CPU Failed	asr5kCardUp	asr5kCpuFailed	N	IModule	F	T	T	0	F	critical	T	T	F
CPU Memory Failed	asr5kCardUp	asr5kCpuMemoryFailed	N	IModule	F	T	T	0	F	critical	T	T	F
CPU Memory Low	asr5kCpuMemoryLow	asr5kCpuMemoryLow	N	IModule	F	T	T	0	F	maj	T	T	F
CPU Busy	asr5kCpuBusy	asr5kCpuBusy	N	IModule	F	T	T	0	F	maj	T	T	F

Cisco Unified Computing System V2 Trap Registry Parameters

Table 16-31 lists the associated event types, event subtypes, and Prime Network registry parameters for the Cisco Unified Computing System V2 traps shown in Table 16-15.

Table 16-31 Cisco Unified Computing System V2 Trap Registry Parameters

Short Description	Event Type	Event Subtype	Expedites Polling	Event Source (IMO Name)	Activate Flow	Correlate	Is Correlation Allowed	Weight	Auto Clear	Severity	Is Ticketable	Auto Remove	Flapping
fltEquipmentPsuInoperable	fltEquipmentPsuInoperable	fltEquipmentPsuInoperable	N	IModule	F	T	F	0	T	maj	F	F	F
fltEquipmentPsuInoperable-cleared	fltEquipmentPsuInoperable	fltEquipmentPsuInoperable-cleared	N	IModule	F	F	F	0	T	clr	F	F	F
fltPortPIoFailed	fltPortPIoFailed	fltPortPIoFailed	N	IPortLayer1	F	T	F	0	T	maj	F	F	F
fltPortPIoFailed-cleared	fltPortPIoFailed	fltPortPIoFailed-cleared	N	IPortLayer1	F	F	F	0	T	clr	F	F	F
fltPortPIoHardware-failure	fltPortPIoHardware-failure	fltPortPIoHardware-failure	N	IPortLayer1	F	T	F	0	T	maj	F	F	F
fltPortPIoHardware-failure-cleared	fltPortPIoHardware-failure	fltPortPIoHardware-failure-cleared	N	IPortLayer1	F	F	F	0	T	clr	F	F	F
fltPortPIoInvalid-sfp	fltPortPIoInvalid-sfp	fltPortPIoInvalid-sfp	N	IPortLayer1	F	T	F	0	T	maj	F	F	F
fltPortPIoInvalid-sfp-cleared	fltPortPIoInvalid-sfp	fltPortPIoInvalid-sfp-cleared	N	IPortLayer1	F	F	F	0	T	clr	F	F	F
fltPortPIoLink-down	fltPortPIoLink-down	fltPortPIoLink-down	port-status	IPortLayer1	F	T	F	0	T	maj	F	F	T
fltPortPIoLink-down-cleared	fltPortPIoLink-down	fltPortPIoLink-down-cleared	port-status	IPortLayer1	F	F	F	0	T	clr	F	F	F
fltPortPIoSfp-not-present	fltPortPIoSfp-not-present	fltPortPIoSfp-not-present	N	IPortLayer1	F	T	F	0	T	info	F	F	F
fltPortPIoSfp-not-present-cleared	fltPortPIoSfp-not-present	fltPortPIoSfp-not-present-cleared	N	IPortLayer1	F	F	F	0	T	clr	F	F	F
fltEquipmentPsuIdentity	fltEquipmentPsuIdentity	fltEquipmentPsuIdentity	N	IModule	F	T	F	0	T	cri	F	F	F
fltEquipmentPsuIdentity-cleared	fltEquipmentPsuIdentity	fltEquipmentPsuIdentity-cleared	N	IModule	F	F	F	0	T	clr	F	F	F

Table 16-31 Cisco Unified Computing System V2 Trap Registry Parameters (continued)

Short Description	Event Type	Event Subtype	Expedites Polling	Event Source (IMO Name)	Activate Flow	Correlate	Is Correlation Allowed	Weight	Auto Clear	Severity	Is Ticketable	Auto Remove	Flapping
fltEquipmentPsuMissing	fltEquipmentPsuMissing	fltEquipmentPsuMissing	N	IModule	F	T	F	0	T	wrn	F	F	F
fltEquipmentPsuMissing-cleared	fltEquipmentPsuMissing	fltEquipmentPsuMissing-cleared	N	IModule	F	F	F	0	T	clr	F	F	F
fltEquipmentPsuOffline	fltEquipmentPsuOffline	fltEquipmentPsuOffline	N	IModule	F	T	F	0	T	wrn	F	F	F
fltEquipmentPsuOffline-cleared	fltEquipmentPsuOffline	fltEquipmentPsuOffline-cleared	N	IModule	F	F	F	0	T	clr	F	F	F
fltEquipmentPsuPerfThresholdCritical	fltEquipmentPsuPerfThresholdCritical	fltEquipmentPsuPerfThresholdCritical	N	IModule	F	T	F	0	T	maj	F	F	F
fltEquipmentPsuPerfThresholdCritical-cleared	fltEquipmentPsuPerfThresholdCritical	fltEquipmentPsuPerfThresholdCritical-cleared	N	IModule	F	F	F	0	T	clr	F	F	F
fltEquipmentPsuPerfThresholdNonCritical	fltEquipmentPsuPerfThresholdNonCritical	fltEquipmentPsuPerfThresholdNonCritical	N	IModule	F	T	F	0	T	min	F	F	F
fltEquipmentPsuPerfThresholdNonCritical-cleared	fltEquipmentPsuPerfThresholdNonCritical	fltEquipmentPsuPerfThresholdNonCritical-cleared	N	IModule	F	F	F	0	T	clr	F	F	F
fltEquipmentPsuInoperable	fltEquipmentPsuInoperable	fltEquipmentPsuInoperable	N	IModule	F	T	F	0	T	maj	F	F	F
fltEquipmentPsuPerfThresholdNonRecoverable	fltEquipmentPsuPerfThresholdNonRecoverable	fltEquipmentPsuPerfThresholdNonRecoverable	N	IModule	F	T	F	0	T	cri	F	F	F
fltEquipmentPsuPerfThresholdNonRecoverable-cleared	fltEquipmentPsuPerfThresholdNonRecoverable	fltEquipmentPsuPerfThresholdNonRecoverable-cleared	N	IModule	F	F	F	0	T	clr	F	F	F
fltEquipmentPsuPowerSupplyProblem	fltEquipmentPsuPowerSupplyProblem	fltEquipmentPsuPowerSupplyProblem	N	IModule	F	T	F	0	T	maj	F	F	F

Table 16-31 Cisco Unified Computing System V2 Trap Registry Parameters (continued)

Short Description	Event Type	Event Subtype	Expedites Polling	Event Source (IMO Name)	Activate Flow	Correlate	Is Correlation Allowed	Weight	Auto Clear	Severity	Is Ticketable	Auto Remove	Flapping
fltEquipmentPsuPowerSupplyProblem-cleared	fltEquipmentPsuPowerSupplyProblem	fltEquipmentPsuPowerSupplyProblem-cleared	N	IModule	F	F	F	0	T	clr	F	F	F
fltEquipmentPsuThermalThresholdCritical	fltEquipmentPsuThermalThresholdCritical	fltEquipmentPsuThermalThresholdCritical	N	IModule	F	T	F	0	T	maj	F	F	F
fltEquipmentPsuThermalThresholdCritical-cleared	fltEquipmentPsuThermalThresholdCritical	fltEquipmentPsuThermalThresholdCritical-cleared	N	IModule	F	F	F	0	T	clr	F	F	F
fltEquipmentPsuThermalThresholdNonCritical	fltEquipmentPsuThermalThresholdNonCritical	fltEquipmentPsuThermalThresholdNonCritical	N	IModule	F	T	F	0	T	min	F	F	F
fltEquipmentPsuThermalThresholdNonCritical-cleared	fltEquipmentPsuThermalThresholdNonCritical	fltEquipmentPsuThermalThresholdNonCritical-cleared	N	IModule	F	F	F	0	T	clr	F	F	F
fltEquipmentPsuThermalThresholdNonRecoverable	fltEquipmentPsuThermalThresholdNonRecoverable	fltEquipmentPsuThermalThresholdNonRecoverable	N	IModule	F	T	F	0	T	cri	F	F	F
fltEquipmentPsuThermalThresholdNonRecoverable-cleared	fltEquipmentPsuThermalThresholdNonRecoverable	fltEquipmentPsuThermalThresholdNonRecoverable-cleared	N	IModule	F	F	F	0	T	clr	F	F	F
fltEquipmentPsuVoltageThresholdCritical	fltEquipmentPsuVoltageThresholdCritical	fltEquipmentPsuVoltageThresholdCritical	N	IModule	F	T	F	0	T	maj	F	F	F
fltEquipmentPsuVoltageThresholdCritical-cleared	fltEquipmentPsuVoltageThresholdCritical	fltEquipmentPsuVoltageThresholdCritical-cleared	N	IModule	F	F	F	0	T	clr	F	F	F
fltEquipmentPsuVoltageThresholdNonCritical	fltEquipmentPsuVoltageThresholdNonCritical	fltEquipmentPsuVoltageThresholdNonCritical	N	IModule	F	T	F	0	T	min	F	F	F

Table 16-31 Cisco Unified Computing System V2 Trap Registry Parameters (continued)

Short Description	Event Type	Event Subtype	Expedites Polling	Event Source (IMO Name)	Activate Flow	Correlate	Is Correlation Allowed	Weight	Auto Clear	Severity	Is Ticketable	Auto Remove	Flapping
fltEquipmentPsuVoltageThresholdNonCritical-cleared	fltEquipmentPsuVoltageThresholdNonCritical	fltEquipmentPsuVoltageThresholdNonCritical-cleared	N	IModule	F	F	F	0	T	clr	F	F	F
fltEquipmentPsuVoltageThresholdNonRecoverable	fltEquipmentPsuVoltageThresholdNonRecoverable	fltEquipmentPsuVoltageThresholdNonRecoverable	N	IModule	F	T	F	0	T	cri	F	F	F
fltEquipmentPsuVoltageThresholdNonRecoverable-cleared	fltEquipmentPsuVoltageThresholdNonRecoverable	fltEquipmentPsuVoltageThresholdNonRecoverable-cleared	N	IModule	F	F	F	0	T	clr	F	F	F
fltEquipmentIOCardIdentity	fltEquipmentIOCardIdentity	fltEquipmentIOCardIdentity	N	IModule	F	T	F	0	T	cri	F	F	F
fltEquipmentIOCardIdentity-cleared	fltEquipmentIOCardIdentity	fltEquipmentIOCardIdentity-cleared	N	IModule	F	F	F	0	T	clr	F	F	F
fltEquipmentIOCardInaccessible	fltEquipmentIOCardInaccessible	fltEquipmentIOCardInaccessible	phyical-command	IModule	F	T	F	0	T	cri	F	F	F
fltEquipmentIOCardInaccessible-cleared	fltEquipmentIOCardInaccessible	fltEquipmentIOCardInaccessible-cleared	phyical-command	IModule	F	F	F	0	T	clr	F	F	F
fltEquipmentIOCardPeerDisconnected	fltEquipmentIOCardPeerDisconnected	fltEquipmentIOCardPeerDisconnected	N	IModule	F	T	F	0	T	war	F	F	F
fltEquipmentIOCardPeerDisconnected-cleared	fltEquipmentIOCardPeerDisconnected	fltEquipmentIOCardPeerDisconnected-cleared	N	IModule	F	F	F	0	T	clr	F	F	F
fltEquipmentIOCardPost-failure	fltEquipmentIOCardPost-failure	fltEquipmentIOCardPost-failure	N	IModule	F	T	F	0	T	maj	F	F	F
fltEquipmentIOCardPost-failure-cleared	fltEquipmentIOCardPost-failure	fltEquipmentIOCardPost-failure-cleared	N	IModule	F	F	F	0	T	clr	F	F	F

Table 16-31 Cisco Unified Computing System V2 Trap Registry Parameters (continued)

Short Description	Event Type	Event Subtype	Expedites Polling	Event Source (IMO Name)	Activate Flow	Correlate	Is Correlation Allowed	Weight	Auto Clear	Severity	Is Ticketable	Auto Remove	Flapping
fltEquipmentIOCardRemoved	fltEquipmentIOCardRemoved	fltEquipmentIOCardRemoved	physical-command	IModule	F	T	F	0	T	cri	F	F	F
fltEquipmentIOCardRemoved-cleared	fltEquipmentIOCardRemoved	fltEquipmentIOCardRemoved-cleared	physical-command	IModule	F	F	F	0	T	clr	F	F	F
fltEquipmentIOCardThermalProblem	fltEquipmentIOCardThermalProblem	fltEquipmentIOCardThermalProblem	N	IModule	F	T	F	0	T	maj	F	F	F
fltEquipmentIOCardThermalProblem-cleared	fltEquipmentIOCardThermalProblem	fltEquipmentIOCardThermalProblem-cleared	N	IModule	F	F	F	0	T	clr	F	F	F
fltEquipmentIOCardThermalThresholdCritical	fltEquipmentIOCardThermalThresholdCritical	fltEquipmentIOCardThermalThresholdCritical	N	IModule	F	T	F	0	T	maj	F	F	F
fltEquipmentIOCardThermalThresholdCritical-cleared	fltEquipmentIOCardThermalThresholdCritical	fltEquipmentIOCardThermalThresholdCritical-cleared	N	IModule	F	F	F	0	T	clr	F	F	F
fltEquipmentIOCardThermalThresholdNonCritical	fltEquipmentIOCardThermalThresholdNonCritical	fltEquipmentIOCardThermalThresholdNonCritical	N	IModule	F	T	F	0	T	min	F	F	F
fltEquipmentIOCardThermalThresholdNonCritical-cleared	fltEquipmentIOCardThermalThresholdNonCritical	fltEquipmentIOCardThermalThresholdNonCritical-cleared	N	IModule	F	F	F	0	T	clr	F	F	F
fltEquipmentIOCardThermalThresholdNonRecoverable	fltEquipmentIOCardThermalThresholdNonRecoverable	fltEquipmentIOCardThermalThresholdNonRecoverable	N	IModule	F	T	F	0	T	cri	F	F	F
fltEquipmentIOCardThermalThresholdNonRecoverable-cleared	fltEquipmentIOCardThermalThresholdNonRecoverable	fltEquipmentIOCardThermalThresholdNonRecoverable-cleared	N	IModule	F	F	F	0	T	clr	F	F	F

Table 16-31 Cisco Unified Computing System V2 Trap Registry Parameters (continued)

Short Description	Event Type	Event Subtype	Expedites Polling	Event Source (IMO Name)	Activate Flow	Correlate	Is Correlation Allowed	Weight	Auto Clear	Severity	Is Ticketable	Auto Remove	Flapping
fltEquipmentIOCardUnsupportedConnectivity	fltEquipmentIOCardUnsupportedConnectivity	fltEquipmentIOCardUnsupportedConnectivity	N	IModule	F	T	F	0	T	maj	F	F	F
fltEquipmentIOCardUnsupportedConnectivity-cleared	fltEquipmentIOCardUnsupportedConnectivity	fltEquipmentIOCardUnsupportedConnectivity-cleared	N	IModule	F	F	F	0	T	clr	F	F	F
fltEquipmentFanDegraded	fltEquipmentFanDegraded	fltEquipmentFanDegraded	N	IModule	F	T	F	0	T	min	F	F	F
fltEquipmentFanDegraded-cleared	fltEquipmentFanDegraded	fltEquipmentFanDegraded-cleared	N	IModule	F	F	F	0	T	clr	F	F	F
fltEquipmentFanInoperable	fltEquipmentFanInoperable	fltEquipmentFanInoperable	N	IModule	F	T	F	0	T	maj	F	F	F
fltEquipmentFanInoperable-cleared	fltEquipmentFanInoperable	fltEquipmentFanInoperable-cleared	N	IModule	F	F	F	0	T	clr	F	F	F
fltEquipmentFanMissing	fltEquipmentFanMissing	fltEquipmentFanMissing	N	IModule	F	T	F	0	T	war	F	F	F
fltEquipmentFanMissing-cleared	fltEquipmentFanMissing	fltEquipmentFanMissing-cleared	N	IModule	F	F	F	0	T	clr	F	F	F
fltEquipmentFanModuleDegraded	fltEquipmentFanModuleDegraded	fltEquipmentFanModuleDegraded	N	IModule	F	T	F	0	T	min	F	F	F
fltEquipmentFanModuleDegraded-cleared	fltEquipmentFanModuleDegraded	fltEquipmentFanModuleDegraded-cleared	N	IModule	F	F	F	0	T	clr	F	F	F
fltEquipmentFanModuleIdentity	fltEquipmentFanModuleIdentity	fltEquipmentFanModuleIdentity	N	IModule	F	T	F	0	T	cri	F	F	F
fltEquipmentFanModuleIdentity-cleared	fltEquipmentFanModuleIdentity	fltEquipmentFanModuleIdentity-cleared	N	IModule	F	F	F	0	T	clr	F	F	F

Table 16-31 Cisco Unified Computing System V2 Trap Registry Parameters (continued)

Short Description	Event Type	Event Subtype	Expedites Polling	Event Source (IMO Name)	Activate Flow	Correlate	Is Correlation Allowed	Weight	Auto Clear	Severity	Is Ticketable	Auto Remove	Flapping
fltEquipmentFanModuleInoperable	fltEquipmentFanModuleInoperable	fltEquipmentFanModuleInoperable	N	IModule	F	T	F	0	T	maj	F	F	F
fltEquipmentFanModuleInoperable-cleared	fltEquipmentFanModuleInoperable	fltEquipmentFanModuleInoperable-cleared	N	IModule	F	F	F	0	T	clr	F	F	F
fltEquipmentFanModuleMissing	fltEquipmentFanModuleMissing	fltEquipmentFanModuleMissing	N	IModule	F	T	F	0	T	wrn	F	F	F
fltEquipmentFanModuleMissing-cleared	fltEquipmentFanModuleMissing	fltEquipmentFanModuleMissing-cleared	N	IModule	F	F	F	0	T	clr	F	F	F
fltEquipmentFanModuleThermalThresholdCritical	fltEquipmentFanModuleThermalThresholdCritical	fltEquipmentFanModuleThermalThresholdCritical	N	IModule	F	T	F	0	T	maj	F	F	F
fltEquipmentFanModuleThermalThresholdCritical-cleared	fltEquipmentFanModuleThermalThresholdCritical	fltEquipmentFanModuleThermalThresholdCritical-cleared	N	IModule	F	F	F	0	T	clr	F	F	F
fltEquipmentFanModuleThermalThresholdNonCritical	fltEquipmentFanModuleThermalThresholdNonCritical	fltEquipmentFanModuleThermalThresholdNonCritical	N	IModule	F	T	F	0	T	min	F	F	F
fltEquipmentFanModuleThermalThresholdNonCritical-cleared	fltEquipmentFanModuleThermalThresholdNonCritical	fltEquipmentFanModuleThermalThresholdNonCritical-cleared	N	IModule	F	F	F	0	T	clr	F	F	F
fltEquipmentFanModuleThermalThresholdNonRecoverable	fltEquipmentFanModuleThermalThresholdNonRecoverable	fltEquipmentFanModuleThermalThresholdNonRecoverable	N	IModule	F	T	F	0	T	cri	F	F	F

Table 16-31 Cisco Unified Computing System V2 Trap Registry Parameters (continued)

Short Description	Event Type	Event Subtype	Expedites Polling	Event Source (IMO Name)	Activate Flow	Correlate	Is Correlation Allowed	Weight	Auto Clear	Severity	Is Ticketable	Auto Remove	Flapping
fltEquipmentFanModuleThermalThresholdNonRecoverable-cleared	fltEquipmentFanModuleThermalThresholdNonRecoverable	fltEquipmentFanModuleThermalThresholdNonRecoverable-cleared	N	IModule	F	F	F	0	T	clr	F	F	F
fltEquipmentFanPerfThresholdCritical	fltEquipmentFanPerfThresholdCritical	fltEquipmentFanPerfThresholdCritical	N	IModule	F	T	F	0	T	info	F	F	F
fltEquipmentFanPerfThresholdCritical-cleared	fltEquipmentFanPerfThresholdCritical	fltEquipmentFanPerfThresholdCritical-cleared	N	IModule	F	F	F	0	T	clr	F	F	F
fltEquipmentFanPerfThresholdLowerNonRecoverable	fltEquipmentFanPerfThresholdLowerNonRecoverable	fltEquipmentFanPerfThresholdLowerNonRecoverable	N	IModule	F	T	F	0	T	cri	F	F	F
fltEquipmentFanPerfThresholdLowerNonRecoverable-cleared	fltEquipmentFanPerfThresholdLowerNonRecoverable	fltEquipmentFanPerfThresholdLowerNonRecoverable-cleared	N	IModule	F	F	F	0	T	clr	F	F	F
fltEquipmentFanPerfThresholdNonCritical	fltEquipmentFanPerfThresholdNonCritical	fltEquipmentFanPerfThresholdNonCritical	N	IModule	F	T	F	0	T	info	F	F	F
fltEquipmentFanPerfThresholdNonCritical-cleared	fltEquipmentFanPerfThresholdNonCritical	fltEquipmentFanPerfThresholdNonCritical-cleared	N	IModule	F	F	F	0	T	clr	F	F	F
fltEquipmentFanPerfThresholdNonRecoverable	fltEquipmentFanPerfThresholdNonRecoverable	fltEquipmentFanPerfThresholdNonRecoverable	N	IModule	F	T	F	0	T	info	F	F	F
fltEquipmentFanPerfThresholdNonRecoverable-cleared	fltEquipmentFanPerfThresholdNonRecoverable	fltEquipmentFanPerfThresholdNonRecoverable-cleared	N	IModule	F	F	F	0	T	clr	F	F	F
fltExtmgmtIfMgmtifdown	fltExtmgmtIfMgmtifdown	fltExtmgmtIfMgmtifdown	N	IModule	F	T	F	0	T	maj	F	F	F

Table 16-31 Cisco Unified Computing System V2 Trap Registry Parameters (continued)

Short Description	Event Type	Event Subtype	Expedites Polling	Event Source (IMO Name)	Activate Flow	Correlate	Is Correlation Allowed	Weight	Auto Clear	Severity	Is Ticketable	Auto Remove	Flapping
fltExtmgmtIfMgmtifdown-cleared	fltExtmgmtIfMgmtifdown	fltExtmgmtIfMgmtifdown-cleared	N	IModule	F	F	F	0	T	clr	F	F	F
fltMgmtEntityDegraded	fltMgmtEntityDegraded	fltMgmtEntityDegraded	N	IModule	F	T	F	0	T	maj	F	F	F
fltMgmtEntityDegraded-cleared	fltMgmtEntityDegraded	fltMgmtEntityDegraded-cleared	N	IModule	F	F	F	0	T	clr	F	F	F
fltMgmtEntityDown	fltMgmtEntityDown	fltMgmtEntityDown	N	IModule	F	T	F	0	T	cri	F	F	F
fltMgmtEntityDown-cleared	fltMgmtEntityDown	fltMgmtEntityDown-cleared	N	IModule	F	F	F	0	T	clr	F	F	F
fltMgmtEntityElection-failure	fltMgmtEntityElection-failure	fltMgmtEntityElection-failure	N	IModule	F	T	F	0	T	cri	F	F	F
fltMgmtEntityElection-failure-cleared	fltMgmtEntityElection-failure	fltMgmtEntityElection-failure-cleared	N	IModule	F	F	F	0	T	clr	F	F	F
fltMgmtEntityVersion-incompatible	fltMgmtEntityVersion-incompatible	fltMgmtEntityVersion-incompatible	N	IModule	F	T	F	0	T	cri	F	F	F
fltMgmtEntityVersion-incompatible-cleared	fltMgmtEntityVersion-incompatible	fltMgmtEntityVersion-incompatible-cleared	N	IModule	F	F	F	0	T	clr	F	F	F
fltNetworkElementInoperable	fltNetworkElementInoperable	fltNetworkElementInoperable	N	IModule	F	T	F	0	T	cri	F	F	F
fltNetworkElementInoperable-cleared	fltNetworkElementInoperable	fltNetworkElementInoperable-cleared	N	IModule	F	F	F	0	T	clr	F	F	F
fltStorageItemCapacityExceeded	fltStorageItemCapacityExceeded	fltStorageItemCapacityExceeded	N	IModule	F	T	F	0	T	maj	F	F	F
fltStorageItemCapacityExceeded-cleared	fltStorageItemCapacityExceeded	fltStorageItemCapacityExceeded-cleared	N	IModule	F	F	F	0	T	clr	F	F	F

Table 16-31 Cisco Unified Computing System V2 Trap Registry Parameters (continued)

Short Description	Event Type	Event Subtype	Expedites Polling	Event Source (IMO Name)	Activate Flow	Correlate	Is Correlation Allowed	Weight	Auto Clear	Severity	Is Ticketable	Auto Remove	Flapping
fltStorageItemCapacityWarning	fltStorageItemCapacityWarning	fltStorageItemCapacityWarning	N	IModule	F	T	F	0	T	maj	F	F	F
fltStorageItemCapacityWarning-cleared	fltStorageItemCapacityWarning	fltStorageItemCapacityWarning-cleared	N	IModule	F	F	F	0	T	clr	F	F	F
fltEquipmentFexIdentity	fltEquipmentFexIdentity	fltEquipmentFexIdentity	N	IModule	F	T	F	0	T	cri	F	F	F
fltEquipmentFexIdentity-cleared	fltEquipmentFexIdentity	fltEquipmentFexIdentity-cleared	N	IModule	F	F	F	0	T	clr	F	F	F
fltEquipmentFexIdentity-unestablishable	fltEquipmentFexIdentity-unestablishable	fltEquipmentFexIdentity-unestablishable	N	IModule	F	T	F	0	T	maj	F	F	F
fltEquipmentFexIdentity-unestablishable-cleared	fltEquipmentFexIdentity-unestablishable	fltEquipmentFexIdentity-unestablishable-cleared	N	IModule	F	F	F	0	T	clr	F	F	F
fltEquipmentChassisIdentity	fltEquipmentChassisIdentity	fltEquipmentChassisIdentity	N	IManagedElement	F	T	F	0	T	cri	F	F	F
fltEquipmentChassisIdentity-cleared	fltEquipmentChassisIdentity	fltEquipmentChassisIdentity-cleared	N	IManagedElement	F	F	F	0	T	clr	F	F	F
fltEquipmentChassisIdentity-unestablishable	fltEquipmentChassisIdentity-unestablishable	fltEquipmentChassisIdentity-unestablishable	N	IManagedElement	F	T	F	0	T	maj	F	F	F
fltEquipmentChassisIdentity-unestablishable-cleared	fltEquipmentChassisIdentity-unestablishable	fltEquipmentChassisIdentity-unestablishable-cleared	N	IManagedElement	F	F	F	0	T	clr	F	F	F
fltEquipmentChassisInoperable	fltEquipmentChassisInoperable	fltEquipmentChassisInoperable	N	IManagedElement	F	T	F	0	T	cri	F	F	F
fltEquipmentChassisInoperable-cleared	fltEquipmentChassisInoperable	fltEquipmentChassisInoperable-cleared	N	IManagedElement	F	F	F	0	T	clr	F	F	F

Table 16-31 Cisco Unified Computing System V2 Trap Registry Parameters (continued)

Short Description	Event Type	Event Subtype	Expedites Polling	Event Source (IMO Name)	Activate Flow	Correlate	Is Correlation Allowed	Weight	Auto Clear	Severity	Is Ticketable	Auto Remove	Flapping
fltEquipmentChassisPowerProblem	fltEquipmentChassisPowerProblem	fltEquipmentChassisPowerProblem	N	IManagedElement	F	T	F	0	T	maj	F	F	F
fltEquipmentChassisPowerProblem-cleared	fltEquipmentChassisPowerProblem	fltEquipmentChassisPowerProblem-cleared	N	IManagedElement	F	F	F	0	T	clr	F	F	F
fltEquipmentChassisThermalThresholdCritical	fltEquipmentChassisThermalThresholdCritical	fltEquipmentChassisThermalThresholdCritical	N	IManagedElement	F	T	F	0	T	maj	F	F	F
fltEquipmentChassisThermalThresholdCritical-cleared	fltEquipmentChassisThermalThresholdCritical	fltEquipmentChassisThermalThresholdCritical-cleared	N	IManagedElement	F	F	F	0	T	clr	F	F	F
fltEquipmentChassisThermalThresholdNonCritical	fltEquipmentChassisThermalThresholdNonCritical	fltEquipmentChassisThermalThresholdNonCritical	N	IManagedElement	F	T	F	0	T	min	F	F	F
fltEquipmentChassisThermalThresholdNonCritical-cleared	fltEquipmentChassisThermalThresholdNonCritical	fltEquipmentChassisThermalThresholdNonCritical-cleared	N	IManagedElement	F	F	F	0	T	clr	F	F	F
fltEquipmentChassisThermalThresholdNonRecoverable	fltEquipmentChassisThermalThresholdNonRecoverable	fltEquipmentChassisThermalThresholdNonRecoverable	N	IManagedElement	F	T	F	0	T	cri	F	F	F
fltEquipmentChassisThermalThresholdNonRecoverable-cleared	fltEquipmentChassisThermalThresholdNonRecoverable	fltEquipmentChassisThermalThresholdNonRecoverable-cleared	N	IManagedElement	F	F	F	0	T	clr	F	F	F
fltEquipmentChassisUnacknowledged	fltEquipmentChassisUnacknowledged	fltEquipmentChassisUnacknowledged	N	IManagedElement	F	T	F	0	T	wrn	F	F	F
fltEquipmentChassisUnacknowledged-cleared	fltEquipmentChassisUnacknowledged	fltEquipmentChassisUnacknowledged-cleared	N	IManagedElement	F	F	F	0	T	clr	F	F	F

Table 16-31 Cisco Unified Computing System V2 Trap Registry Parameters (continued)

Short Description	Event Type	Event Subtype	Expedites Polling	Event Source (IMO Name)	Activate Flow	Correlate	Is Correlation Allowed	Weight	Auto Clear	Severity	Is Ticketable	Auto Remove	Flapping
fltEquipmentChassisUnsupportedConnectivity	fltEquipmentChassisUnsupportedConnectivity	fltEquipmentChassisUnsupportedConnectivity	N	IManagedElement	F	T	F	0	T	maj	F	F	F
fltEquipmentChassisUnsupportedConnectivity-cleared	fltEquipmentChassisUnsupportedConnectivity	fltEquipmentChassisUnsupportedConnectivity-cleared	N	IManagedElement	F	F	F	0	T	clr	F	F	F
fltFabricComputeSlotEpMisplacedInChassisSlot	fltFabricComputeSlotEpMisplacedInChassisSlot	fltFabricComputeSlotEpMisplacedInChassisSlot	N	IManagedElement	F	T	F	0	T	wrn	F	F	F
fltFabricComputeSlotEpMisplacedInChassisSlot-cleared	fltFabricComputeSlotEpMisplacedInChassisSlot	fltFabricComputeSlotEpMisplacedInChassisSlot-cleared	N	IManagedElement	F	F	F	0	T	clr	F	F	F
fltFabricComputeSlotEpServerIdentificationProblem	fltFabricComputeSlotEpServerIdentificationProblem	fltFabricComputeSlotEpServerIdentificationProblem	N	IManagedElement	F	T	F	0	T	wrn	F	F	F
fltFabricComputeSlotEpServerIdentificationProblem-cleared	fltFabricComputeSlotEpServerIdentificationProblem	fltFabricComputeSlotEpServerIdentificationProblem-cleared	N	IManagedElement	F	F	F	0	T	clr	F	F	F

Cisco ASR 1000 V2 Trap Registry Parameters

Table 16-32 lists the associated event types, event subtypes, and Prime Network registry parameters for the Cisco ASR 1000 V2 traps shown in Table 16-16.

Table 16-32 Cisco ASR 1000 V2 Trap Registry Parameters

Short Description	Event Type	Event Subtype	Expedites Polling	Event Source (IMO Name)	Activate Flow	Correlate	Is Correlation Allowed	Weight	Auto Clear	Severity	Is Ticketable	Auto Remove	Flapping
IPsec Phase-1 IKE Tunnel active trap	cisco ipsec tunnel state change trap	cisco ike tunnel start	N	IIPSecTunnel	F	F	F	0	F	clr	T	T	F
IPsec Phase-1 IKE Tunnel inactive trap	cisco ipsec tunnel state change trap	cisco ike tunnel stop	N	IIPSecTunnel	F	F	F	0	F	maj	T	T	F



CHAPTER 17

Syslogs

This chapter provides detailed information about the syslogs supported in Prime Network. Syslogs appear in the Prime Network Events Syslog tab. (For information about Prime Network Events, see the *Cisco Prime Network 3.9 User Guide*.) Syslog information is presented in two forms:

- **Syslog Tables:** A section devoted to the supported syslogs for each NOS platform (e.g., Cisco ASR 9000 Syslogs). Each of these sections contains a table listing the name of each supported syslog, along with a description, the raw format of the syslog string, and a short description. In the syslog tables in this Reference, each syslog's short description is also a link to its corresponding registry parameters.
- **Registry Parameter Tables:** A section devoted to the event types, event subtypes and Prime Network registry parameters for the supported syslogs. There is one parameter table for every syslog table (e.g., Cisco ASR 9000 Syslog Registry Parameters). Each syslog can have multiple event subtypes, or states. The parameter tables indicate when each state is generated, and how Prime Network processes them (such as their severity, whether they are ticketable, can be correlated, are autocleared, and so on).

Cisco Prime Network 3.9 users can enable an additional IP in the device for traps and syslogs other than the device management IP address. This new feature is called Multisource Events. When Prime Network 3.9 receives a trap or syslog from that device (from the new IP) it will still recognize the device.

This chapter includes the following sections:

- Cisco ASR 9000 Syslogs, page 17-2
- Cisco ASR 1000 Syslogs, page 17-4
- Cisco IOS Syslogs, page 17-4
- Cisco IOX Syslogs, page 17-21
- Cisco ACE Syslogs, page 17-35
- Cisco Nexus Syslogs, page 17-39
- Cisco ASR 9000 Syslog Registry Parameters, page 17-43
- Cisco ASR 1000 Registry Parameters, page 17-46
- Cisco IOS Syslog Registry Parameters, page 17-47
- Cisco IOX Syslog Registry Parameters, page 17-71
- Cisco ACE Syslog Registry Parameters, page 17-85
- Cisco Nexus Syslog Registry Parameters, page 17-89

Cisco ASR 9000 Syslogs

Table 17-1 lists the Cisco ASR 9000 Syslogs supported in Prime Network.

Table 17-1 Cisco ASR 9000 Syslogs

Syslog Name	Description	Raw Format	Short Description
PLATFORM-PWRMON-4-OIR	handle power supply syslog	%PLATFORM-PWRMON-4-OIR : Power-module 0/PM0/SP inserted	Power supply inserted syslog
PLATFORM-PWRMON-4-OIR	handle power supply syslog	%PLATFORM-PWRMON-4-OIR : Power-module 0/PM0/SP removed	Power supply removed syslog
IP-VRRP-6-INFO_STATECHANGE	handle VRRP state change syslog	%IP-VRRP-6-INFO_STATECHANGE : GigabitEthernet0_5_0_1 vrid 10: state Backup -> Master	Backup to Master change syslog
IP-VRRP-6-INFO_STATECHANGE	handle VRRP state change syslog	%IP-VRRP-6-INFO_STATECHANGE : GigabitEthernet0_5_0_1 vrid 10: state Master -> Backup	Master to Backup change syslog
L2-BFD-4-RATE_LIMIT_WARNING_HIGH_WATERMARK	BFD rate limit high warning syslog	%L2-BFD-4-RATE_LIMIT_WARNING_HIGH_WATERMARK BFD PPS allocation exceeds 90 percent of maximum.	BFD rate limit high warning syslog
ROUTING-RIP-3-ERR_PAK_AUTH	RIP Authentication Failure syslog	%ROUTING-RIP-3-ERR_PAK_AUTH Authentication failure for RIP [chars] packet in context [chars]: instance [chars]: error equals [chars]	RIP authentication failed syslog
ROUTING-RIP-3-ERR_CFG	RIP configuration error syslog	%ROUTING-RIP-3-ERR_CFG Error during configuration in context [chars]: error equals [chars]	RIP configuration error syslog
ROUTING-RIP-6-INFO_OOM	RIP out of memory event syslog	%ROUTING-RIP-6-INFO_OOM RIP out-of-memory event [chars]: new/current state equals [chars]: old state equals [chars]	RIP out of memory event syslog
ROUTING-ISIS-5-ADJCHANGE	handle ROUTING-ISIS-5-ADJCHANGE syslog	RP/0/RSP1/CPU0:Oct 19 19:48:32.212 : isis[240]: %ROUTING-ISIS-5-ADJCHANGE : Adjacency to AGS2a (Bundle-Ether1) (L1) Down, Interface state down	routing ISIS neighbor down syslog
ROUTING-ISIS-5-ADJCHANGE	handle ROUTING-ISIS-5-ADJCHANGE syslog	RP/0/RSP1/CPU0:Oct 19 19:48:32.212 : isis[240]: %ROUTING-ISIS-5-ADJCHANGE : Adjacency to AGS2a (Bundle-Ether1) (L1) Up, Interface state up	routing ISIS neighbor up syslog
L2-ELO-6-INTF_REMOTE_LOOPBACK	Ethernet OAM Remote loopback session started/stopped syslog	%L2-ELO-6-INTF_REMOTE_LOOPBACK : TenGigE0/2/0/3: OAM remote loopback has been stopped on the interface	Ethernet OAM Remote loopback session stopped Syslog

Table 17-1 Cisco ASR 9000 Syslogs (continued)

Syslog Name	Description	Raw Format	Short Description
L2-ELO-6-INTF_REMOTE_LOOPBACK	Ethernet OAM Remote loopback session started/stopped syslog	%L2-ELO-6-INTF_REMOTE_LOOPBACK : TenGigE0/2/0/3: OAM remote loopback has been started on the interface.	Ethernet OAM Remote loopback session started Syslog
L2-ELO-6-INTF_REMOTE_LOOPBACK	Ethernet OAM Remote loopback session started/stopped syslog	%L2-ELO-6-INTF_REMOTE_LOOPBACK : TenGigE0/2/0/3: OAM local loopback has been stopped on the interface.	Ethernet OAM Local loopback session stopped Syslog
L2-ELO-6-INTF_REMOTE_LOOPBACK	Ethernet OAM Remote loopback session started/stopped syslog	%L2-ELO-6-INTF_REMOTE_LOOPBACK : TenGigE0/2/0/3: OAM local loopback has been started on the interface	Ethernet OAM Local loopback session started Syslog
L2-ELO-6-INTF_SESSION_DOWN	Ethernet OAM session up/down syslog	%L2-ELO-6-INTF_SESSION_DOWN: TenGigE0/2/0/3: OAM session has gone down	Ethernet OAM Session down Syslog
L2-ELO-6-INTF_SESSION_DOWN	Ethernet OAM session up/down syslog	%L2-ELO-6-INTF_SESSION_UP : TenGigE0/2/0/3: OAM session has come up	Ethernet OAM Session up Syslog
L2-CFM-6-CC_ERROR	handle L2-CFM-6-CC_ERROR syslog	%L2-CFM-6-CC_ERROR : Peer MEP error change: error flags or remote interface state changed - domain ELAN, service elan10, local MEP ID 3991, local interface GigabitEthernet0/0/0/2.3010, peer MEP ID 3010, peer MAC address 001b.53ff.80d9, errors set: received CCM with RDI bit set; current: received CCM with RDI bit set;	CFM cc error syslog
L2-CFM-6-CC_ERROR	handle L2-CFM-6-CC_ERROR syslog	%L2-CFM-6-CC_ERROR : Peer MEP error change: error flags or remote interface state changed - domain ELAN, service elan10, local MEP ID 3991, local interface GigabitEthernet0/0/0/2.3010, peer MEP ID 3010, peer MAC address 001b.53ff.80d9, errors cleared: received CCM with RDI bit set; current: none	CFM cc error cleared syslog
MAC_TABLE_RESYNC_COMPLETE	handle MAC_TABLE_RESYNC_COMPLETE syslog	LC/0/0/CPU0:Jun 16 9:37:05.189 : l2fib[193]: %L2-L2FIB-5-MAC_TABLE_RESYNC_COMPLETE : The resynchronization of the MAC address table is complete 0/0/CPU0	Mac Table resync completed syslog

Cisco ASR 1000 Syslogs

Table 17-2 lists the Cisco ASR 1000 syslogs supported in Prime Network.

Table 17-2 Cisco ASR 1000 Syslogs

Syslog Name	Description	Raw Format	Short Description
CRYPTO-5-SESSION_STATUS_UP	crypto tunnel status syslog	%CRYPTO-5-SESSION_STATUS: Crypto tunnel is UP . Peer 20.0.149.203:500 Id: 20.0.149.203	Crypto session status up syslog
CRYPTO-5-SESSION_STATUS_DOWN	crypto tunnel status syslog	%CRYPTO-5-SESSION_STATUS: Crypto tunnel is DOWN. Peer 20.0.149.203:500 Id: 20.0.149.203	Crypto session status down syslog

Cisco IOS Syslogs

Table 17-3 lists the Cisco IOS syslogs supported in Prime Network.

Note If SNMP syslogs are disabled in a device, wrapped syslogs are enabled by Cisco Prime Network 3.9. Wrapped syslogs are SNMP traps that enclose the syslog information.

Table 17-3 Cisco IOS Syslogs

Syslog Name	Description	Raw Format	Short Description
LINK-5-CHANGED	handle link down syslog	%LINK-5-CHANGED: Interface Ethernet5/1, changed state to administratively up	Link down syslog
LINK-5-CHANGED	handle link down syslog	%LINK-5-CHANGED: Interface Ethernet5/1, changed state to administratively down	Link up syslog
FR-5-DLCICHANGE	handle dlci change syslog	%FR-5-DLCICHANGE: Interface Serial3/0/0:1 - DLCI 105 state changed to INACTIVE	FR DLCI down syslog
FR-5-DLCICHANGE	handle dlci change syslog	%FR-5-DLCICHANGE: Interface Serial3/0/0:1 - DLCI 105 state changed to ACTIVE	FR DLCI up syslog
STANDBY-6-STATECHANGE	handle hsrp syslog	%STANDBY-6-STATECHANGE: Standby: 1: Ethernet1 state Active -> Standby	HSRP group change syslog
STANDBY-6-STATECHANGE	handle hsrp syslog	%STANDBY-6-STATECHANGE: Standby: 1: Ethernet1 state Active -> Speak	HSRP group restored syslog

Table 17-3 Cisco IOS Syslogs (continued)

Syslog Name	Description	Raw Format	Short Description
SNMP-5-SNMPAUTHFAIL	This message indicates that the switch has received an SNMP message that was not properly authenticated	%SNMP-5-SNMPAUTHFAIL: Authentication failed for message from 192.168.1.2	SNMP message has not properly authenticated
SYS-2-MALLOCFAIL	The requested memory allocation is not available from the specified memory pool	%SYS-2-MALLOCFAIL: Memory allocation of 1028 bytes failed from 0x6015EC84, Pool Processor, alignment 0	Memory allocation is not available
SYS-3-CPUHOG	The indicated process ran too long without relinquishing the processor	%SYS-3-CPUHOG: Task ran for 2148 msec (20/13), Process = IP Input, PC = 3199482 -Traceback= 314B5E6 319948A	process ran too long
SCHED-3-STUCKMTMR	A process can register to be notified when various events occur in the router. This message indicates that a registered timer is expired and its value is unchanged after the process has executed two successive times	%SCHED-3-STUCKMTMR: Sleep with expired managed timer 1C7410, time 0x1063F9C52 (00:00:00 ago).	registered timer is expired
DUAL-3-SIA	The EIGRP router has not received a reply to a query from one or more neighbors within the time allotted, so it clears the neighbors that did not send a reply	%DUAL-3-SIA: Route 10.1.2.0/24 stuck-in-active state in IP-EIGRP 1. Cleaning up	EIGRP router query to neighbors timeouted syslog
LANCE-3-BADCABLE	The Ethernet cable is not connected	%LANCE-3-BADCABLE: msgtxt_badcable	Ethernet cable is not connected
LAPB-4-CTRLBAD	A received FRMR has reported a frame with an invalid control code	%LAPB-4-CTRLBAD: Interface Ethernet0, Invalid control field	frame with an invalid control code
DTP-5-NONTRUNKPORTON	The interface changed to non trunk	%DTP-5- ONTRUNKPORTON:Port 8/1 has become trunk	Interface changed to non trunk
LINEPROTO-5-UPDOWN	Handle line syslog	%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet1/0/1, changed state to down	Line down syslog
LINEPROTO-5-UPDOWN	Handle line syslog	%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet1/0/1, changed state to up	Line up syslog

Table 17-3 Cisco IOS Syslogs (continued)

Syslog Name	Description	Raw Format	Short Description
IPX-3-BADIGRPSAP	A hardware or software error occurred	%IPX-3-BADIGRPSAP: Cannot send incremental SAP update to peer on interface Ethernet0. Increasing output-sap-delay may help	Cannot send incremental SAP update to peer
LANCE-5-COLL	An Ethernet cable is broken or unterminated, or the transceiver is unplugged	%LANCE-5-COLL: Unit 1, excessive collisions. TDR=10	An Ethernet cable is broken or unterminated
LANCE-5-LATECOLL	An Ethernet transceiver is unplugged or defective	%LANCE-5-LATECOLL: Unit 1, late collision error	An Ethernet transceiver is unplugged or defective
SYS-5-CONFIG_I	The configuration of the router was changed	%SYS-5-CONFIG_I: Configured from console by console	Device configuration changed
AT-6-NODEWRONG	An AppleTalk node sent a GetNet Info request to this router specifying an invalid network number for the source of the GetNet Info request	%AT-6-NODEWRONG: XX: AppleTalk node 192.168.2.0 misconfigured; reply has been broadcast	AppleTalk invalid network number
SECURITY-1-PORTSHUTDOWN	This message indicates that a port has been shut down due to an insecure host sourcing a packet into that port	%Security-1-PORTSHUTDOWN: Port 0/1 shutdown due to security violation	security port shut down
SPANTREE-2-RX_PORTFAST	A BPDU that has spanning-tree portfast enabled was received on the specified interface	%SPANTREE-2-RX_PORTFAST:Received BPDU on PortFast enabled port. Disabling 2/1	BPDU spanning-tree portfast enabled
UDLD-3-DISABLE	This message indicates that a fault has been detected in a fiber Ethernet port connection and that the port has been disabled to prevent other protocols from malfunctioning	%UDLD-3-DISABLE: Unidirectional link detected on port 1/2. Port disabled	Fault has been detected in a fiber Ethernet port connection
UDLD-3-DISABLEFAIL	This message indicates that a fault was detected in the wiring on a fiber Ethernet port, but UDLD could not disable the port	%UDLD-3-DISABLEFAIL: Unidirectional link detected on port 1/2, failed to disable port	Unidirectional link detected

Table 17-3 Cisco IOS Syslogs (continued)

Syslog Name	Description	Raw Format	Short Description
UDLD-4-ONEWAYPATH	This message indicates that a fault has been detected in a fiber Ethernet connection in a shared media environment and that the connection may cause a possible malfunction	%UDLD-4-ONEWAYPATH: A unidirectional link from port 1/2 to port 1/2 of device abc was detected	Fault has been detected in a fiber Ethernet connection
OSPF-5-ADJCHG	Handle ospf syslog	%OSPF-5-ADJCHG: Process 1, Nbr 10.100.12.6 on FastEthernet1/0 from Up to DOWN, Loading Done	OSPF neighbor down syslog
OSPF-5-ADJCHG	Handle ospf syslog	%OSPF-5-ADJCHG: Process 1, Nbr 10.100.12.6 on FastEthernet1/0 from LOADING to FULL, Loading Done	OSPF neighbor up syslog
SPANTREE-2-LOOPGUARDBLOCK	When the loop guard blocks an inconsistent port, the following message is logged	%SPANTREE-2-LOOPGUARDBLOCK: No BPDUs were received on port 3/2 in vlan 3. Moved to loop-inconsistent state	No BPDUs were received on port
SPANTREE-2-LOOPGUARDUNBLOCK	After the recovery, the following message is logged	%SPANTREE-2-LOOPGUARDUNBLOCK: port 3/2 restored in vlan 3	BPDUs were received on port
AMDP2_FE-5-COLL	Ethernet or Fast Ethernet is seeing multiple collisions. This problem may occur under heavy loads	%AMDP2_FE-5-COLL: AMDP2/FE Ethernet1/1, Excessive collisions, TDR=1, TRC=1	Ethernet is seeing multiple collisions
DEC21140-5-COLL	A Fast Ethernet packet has been dropped because too many attempts to transmit it were stopped by collisions	%DEC21140-5-COLL: unit 0, excessive collisions	Fast Ethernet packet has been dropped
ILACC-5-COLL	An Ethernet cable is broken or is not terminated, or the transceiver is unplugged	%ILACC-5-COLL: Unit 0, excessive collisions. TDR=0.12	An Ethernet cable is broken
PQUICC-5-COLL	PQUICC-5-COLL : An Ethernet cable is broken or is not terminated	%PQUICC-5-COLL: Unit 1, excessive collisions. Retry limit 12 exceeded	pquicc 5 coll syslog: An Ethernet cable is broken

Table 17-3 Cisco IOS Syslogs (continued)

Syslog Name	Description	Raw Format	Short Description
PQUICC_ETHER-5-COLL	PQUICC_ETHER-5-COLL : An Ethernet cable is broken or is not terminated	%PQUICC_ETHER-5-COLL: Unit 1, excessive collisions. Retry limit 2 exceeded	pquicc ether 5 coll syslog: An Ethernet cable is broken
PQUICC_FE-5-COLL	Ethernet or Fast Ethernet is detecting multiple collisions	%PQUICC_FE-5-COLL: PQUICC/FE(0/1), Excessive collisions, TDR=10, TRC=10.	Ethernet is detecting multiple collisions
QUICC_ETHER-5-COLL	An Ethernet cable is broken or unterminated	%PQUICC_ETHER-5-COLL: Unit 1, excessive collisions. Retry limit 2 exceeded	quicc ether 5 coll syslog: An Ethernet cable is broken
AMDP2_FE-5-LATECOLL	Late collisions have occurred on the Ethernet or Fast Ethernet	%AMDP2_FE-5-LATECOLL: Ethernet1/1 transmit error	Late collisions have occurred
CLNS-5-ADJCHANGE	Handle IS-IS syslog	%CLNS-5-ADJCHANGE: ISIS: Adjacency to edge-02(POS0/0) Down, hold time expired	IS-IS neighbor down syslog
CLNS-5-ADJCHANGE	Handle IS-IS syslog	%CLNS-5-ADJCHANGE: ISIS: Adjacency to edge-02(POS0/0) Up, hold time expired	IS-IS neighbor up syslog
DEC21140-5-LATECOLL	Late collisions are collisions that occur after transmitting the preamble	%DEC21140-5-LATECOLL: FastEthernet0/0 transmit error	Late collisions have occurred
ILACC-5-LATECOLL	An Ethernet transceiver is malfunctioning, the Ethernet is overloaded, or the Ethernet cable is too long	%ILACC-5-LATECOLL: Unit 0, late collision error	ilacc 5 late coll syslog: Late collisions have occurred
PQUICC-5-LATECOLL	pquicc 5 late coll syslog	%PQUICC-5-LATECOLL: Unit 1, late collision error	pquicc 5 late coll syslog: Late collisions have occurred
PQUICC_ETHER-5-LATECOLL	PQUICC_ETHER-5-LATECOLL : A new network may not have been engineered properly or adding a regenerator to an existing network may have changed the network specifications	%PQUICC_ETHER-5-LATECOLL: Unit 0, late collision error	A new network may not have been engineered properly
PQUICC_FE-5-LATECOLL	Late collisions have occurred on the Ethernet or Fast Ethernet interface	%PQUICC_FE-5-LATECOLL: PQUICC/FE(0/1), Late collision	pquicc fe 5 late coll syslog: Late collisions have occurred

Table 17-3 Cisco IOS Syslogs (continued)

Syslog Name	Description	Raw Format	Short Description
QUICC_ETHER-5-LATECOLL	QUICC_ETHER-5-LATECOLL : A software or hardware error occurred	%QUICC_ETHER-5-LATECOLL: Unit 0, late collision error	quicc ether 5 late coll syslog: Late collisions have occurred
SNMP-5-LINKTRAP	This message indicates the type of Link Trap	%SNMP-5-LINKTRAP: Link down Trap -- ifName=sc0	Link trap down has occurred
SNMP-5-LINKTRAP	This message indicates the type of Link Trap	%SNMP-5-LINKTRAP: Link up Trap -- ifName=sc0	Link trap up has occurred
SNMP-5-TOPOTRAP	This message indicates that a configured port changed from the learning state to the forwarding state, or from the forwarding state to the blocking state	%SNMP-5-TOPOTRAP: Topology Change Trap for VLAN 1	configured port changed state from learning to forwarding
DUAL-5-NBRCHANGE	Handle eigrp syslog	%DUAL-5-NBRCHANGE: IP-EIGRP 1: Neighbor 10.1.4.3 (Serial0) is down: stuck in active	DUAL 5 neighbor down syslog
DUAL-5-NBRCHANGE	Handle eigrp syslog	%DUAL-5-NBRCHANGE: IP-EIGRP 1: Neighbor 10.1.4.3 (Serial0) is up: stuck in active	DUAL 5 neighbor up syslog
LINK-3-UPDOWN	Handle link down syslog	%LINK-3-UPDOWN: Interface ATM2/0, changed state to down	Link down syslog
LINK-3-UPDOWN	Handle link down syslog	%LINK-3-UPDOWN: Interface ATM2/0, changed state to up	Link up syslog
BGP-5-ADJCHANGE-vrf	Handle BGP 5 syslog from vrf. make sure it is before the "BGP-5-ADJCHANGE" pattern	%BGP-5-ADJCHANGE: neighbor 10.1.2.3 vpn vrf inet Down	BGP neighbor down syslog
BGP-5-ADJCHANGE-vrf	Handle BGP 5 syslog from vrf. make sure it is before the "BGP-5-ADJCHANGE" pattern	%BGP-5-ADJCHANGE: neighbor 10.1.2.3 vpn vrf inet Up	BGP neighbor up syslog
BGP-5-ADJCHANGE	Handle BGP 5 syslog	%BGP-5-ADJCHANGE: neighbor 161.10.11.1 Down	BGP neighbor down syslog
BGP-5-ADJCHANGE	Handle BGP 5 syslog	%BGP-5-ADJCHANGE: neighbor 161.10.11.1 Up	BGP neighbor up syslog
OIR-6-(REM|INS)CARD	Handle module out syslog	%OIR-6-INSCARD: Card inserted from slot 4, interfaces disabled	card in syslog
OIR-6-(REM|INS)CARD	Handle module out syslog	%OIR-6-REMCARD: Card removed from slot 4, interfaces disabled	card out syslog

Table 17-3 Cisco IOS Syslogs (continued)

Syslog Name	Description	Raw Format	Short Description
OIR-SP-3-PWRCYCLE	Card being power cycled	%OIR-SP-3-PWRCYCLE: Card in module x, is being power-cycled off (Module not responding to Keep Alive polling)	oir sp 3 power cycle syslog
SYS-5-RELOAD	Syslog for reloading the device	%SYS-5-RELOAD: Reload requested	Reloading device syslog
SYS-5-RESTART	Syslog for restarting the device	%SYS-5-RESTART: System restarted --	System restart
DTP-5-TRUNKPORTON	The interface returned to be a trunk	%DTP-5-TRUNKPORTON:Port 7/2 has become interface trunk	Interface changed to non trunk
DTP-5-TRUNKPORTON	The interface returned to be a trunk	%DTP-5-TRUNKPORTON:Port 7/2 has become dot1q trunk	Interface changed to trunk
ISDN-6-CONNECT	handle ISDN connect syslog	%ISDN-6-CONNECT: Interface BRI0/0:1 is now connected to 5772223	ISDN connect syslog
ISDN-6-CONNECT	handle ISDN connect syslog	%ISDN-6-CONNECT: Interface BRI0/0:1 is now connected to 5772223	ISDN disconnect syslog
ISDN-6-DISCONNECT	handle ISDN connect syslog	%ISDN-6-DISCONNECT: Interface BRI0:1? disconnected from 8130 traxbol, call lasted 60 seconds	ISDN connect syslog
ISDN-6-DISCONNECT	handle ISDN connect syslog	%ISDN-6-DISCONNECT: Interface BRI0:1? disconnected from 8130 traxbol, call lasted 60 seconds	ISDN disconnect syslog
CDP-4-DUPLEX_MISMATCH	This messages indicates a duplex mismatch problem (IOS)	%CDP-4-DUPLEX_MISMATCH: duplex mismatch discovered on FastEthernet6/2 (not half duplex), with TBA04251336 3/2 (half duplex)	Duplex mismatch discovered
ISDN-6-CONNECT-2	handle ISDN connect syslog2	%ISDN-6-LAYER2UP: Layer 2 for Interface FastEthernet2/1, TEI 0 changed to up	ISDN connect syslog
ISDN-6-CONNECT-2	handle ISDN connect syslog2	%ISDN-6-DISCONNECT: Interface FastEthernet0/1 disconnected from 71017 , call lasted 22 seconds	ISDN disconnect syslog
ISDN-6-DISCONNECT-2	handle ISDN disconnect syslog2	%ISDN-6-LAYER2UP: Layer 2 for Interface FastEthernet2/1, TEI 0 changed to up	ISDN connect syslog
ISDN-6-DISCONNECT-2	handle ISDN disconnect syslog2	%ISDN-6-LAYER2DOWN: Layer 2 for Interface FastEthernet0/1, TEI 0 changed to down	ISDN disconnect syslog
LDP-5-NBRCHG-TDP	handle LDP Neighbor change syslog	%LDP-5-NBRCHG: TDP Neighbor 10.12.12.12:0 is DOWN (TCP connection closed by peer)	TDP neighbor down syslog
LDP-5-NBRCHG-TDP	handle LDP Neighbor change syslog	%LDP-5-NBRCHG: TDP Neighbor 10.12.12.12:0 is UP (TCP connection closed by peer)	TDP neighbor up syslog

Table 17-3 Cisco IOS Syslogs (continued)

Syslog Name	Description	Raw Format	Short Description
LDP-5-NBRCHG-LDP	handle LDP Neighbor change syslog	%LDP-5-NBRCHG: LDP Neighbor 10.12.12.12:0 is DOWN	LDP neighbor down syslog
LDP-5-NBRCHG-LDP	handle LDP Neighbor change syslog	%LDP-5-NBRCHG: LDP Neighbor 10.12.12.12:0 is UP	LDP neighbor up syslog
MPLS_TE-5-TUN_reoptimize	handle tunnel reoptimization syslog	%MPLS_TE-5-TUN: Tun1002: installed LSP 1002_33 (popt 10) for 1002_32 (popt 20), reopt. LSP is up	MPSL-TE tunnel reoptimized/rerouted syslog
MPLS_TE-5-TUN_up	handle tunnel up syslog	%MPLS_TE-5-TUN: Tun0: installed LSP 0_26 (popt 5) for nil, got 1st feasible path opt	MPLS TE tunnel down syslog
MPLS_TE-5-TUN_up	handle tunnel up syslog	%MPLS_TE-5-TUN: Tun0: installed LSP 0_26 (popt 5) for nil, got 1st feasible path opt	MPLS TE tunnel up syslog
MPLS_TE-5-TUN_down	handle tunnel down syslog	%MPLS_TE-5-TUN: Tun1001: installed LSP nil for 1001_92 (popt 1), path verification failed	MPLS TE tunnel down syslog
MPLS_TE-5-TUN_down	handle tunnel down syslog	%MPLS_TE-5-TUN: Tun1001: installed LSP nil for 1001_92 (popt 1), path verification failed	MPLS TE tunnel up syslog
ENV_MON-2-SUPPLY	Power supply is not working or has not been turned on	%ENV_MON-2-SUPPLY : [chars] Power Supply is Operation or Non-Operational	A power supply is not working or has not been turned on
SYS-SP-STDBY-5-RESTART	restarting the device	%SYS-SP-STDBY-5-RESTART: System restarted -- Cisco IOS Software (c7600s72033-ADVENTERPRISEK9_WAN_MZ), Version 12.2 Copyright (c) 1986-2006 by Cisco Systems, Inc.Compiled Thu 26-Oct-06 03:49 by	System restart
UDLD-SP-4-UDLD_PORT_DISABLED	aggressive mode failure detected	%UDLD-SP-4-UDLD_PORT_DISABLED: UDLD disabled interface FastEthernet2/1, FastEthernet2/1	Aggressive Mode Failure Detected
FABRIC-SP-5-FABRIC_MODULE_BACKUP	clear block option	%FABRIC-SP-5-FABRIC_MODULE_BACKUP: The Switch Fabric Module in slot 6 became standby	fabric sp 5 clear block down syslog
FABRIC-SP-5-FABRIC_MODULE_BACKUP	clear block option	%FABRIC-SP-5-FABRIC_MODULE_BACKUP: The Switch Fabric Module in slot 6 became standby	fabric sp 5 clear block up syslog
C6KENV-SP-4-FANTRAYFAILED	fan tray failed	%C6KENV-SP-4-FANTRAYFAILED: fan tray 2 failed	c6kenv sp 4 fan tray fail syslog
PFREDUN-SP-4-BOOTSTRING_INVALID	bootstring invalid	PFREDUN-SP-4-BOOTSTRING_INVALID: The bootfile slavebootflash:image_name is not present in standby	pfredun sp 4 bootstring invalid syslog

Table 17-3 Cisco IOS Syslogs (continued)

Syslog Name	Description	Raw Format	Short Description
SYS-5-POWER-SUPPLY	Power supply failure notification	Power supply [dec] failed	Power supply failed syslog
SYS-5-POWER-SUPPLY	Power supply failure notification	Power supply [dec] okay	Power supply okay syslog
PM-SP-STDBY-4-ERR_DISABLE	err disable state	%PM-SP-STDBY-4-ERR_DISABLE: bpduguard error detected on Gi2/5, putting Gi2/5 in err-disable state	pm sp stdby 4 err disable syslog
HSRP-6-STATECHANGE	handle hsrp syslog	%HSRP-6-STATECHANGE:FastEthernet 0/0 Grp 1 state Init	HSRP group change syslog
HSRP-6-STATECHANGE	handle hsrp syslog	%HSRP-6-STATECHANGE:FastEthernet 0/0 Grp 1 state Standby	HSRP group restored syslog
BGP-3-NOTIFICATION	handle BGP 3 syslog	%BGP-3-NOTIFICATION: sent to neighbor 10.10.10.254 4/0 (hold time expired) 0 bytes	BGP notification syslog
NEW-INTERFACE-FOR-VSL-CONNECTION	new interface for the VSL connection syslog (one of the ether channel interfaces)	%VSL-5-VSL_CNTRL_LINK: New VSL Control Link 8/4	new ethernet channel interface for VSL connection
VSL-LINK-UP	VSL link up syslog	%VSLP-5-VSL_UP: Ready for Role Resolution with Switch=1, MAC=0014.1bc6.1c00 over 8/4	VSL link up syslog
VSL-LINK-DOWN	VSL link down syslog	%VSLP-SW1_SP-2-VSL_DOWN: Last VSL interface Te1/6/4 went down	VSL link down syslog
VSL-LINK-UP	VSL link up syslog and active switch is #1	%VSLP-SW1_SP-5-VSL_UP: Ready for Role Resolution with Switch=2, MAC=0013a.30e1.6800 over Te1/5/5	VSL link up syslog: active switch is #1
VSL-LINK-UP	VSL link up syslog and active switch is #2	%VSLP-SW2_SP-5-VSL_UP: Ready for Role Resolution with Switch=2, MAC=0013a.30e1.6800 over Te1/5/5	VSL link up syslog: active switch is #2
VSL-ROLE-MISMATCH-RESOLVED	role mismatch resolved syslog, sent from active switch #1	%VSLP-SW1_SP-5-RRP_ROLE_RESOLVED: Role resolved as ACTIVE by VSLP	role mismatch resolved syslog, sent from active switch #1
VSL-ROLE-MISMATCH-RESOLVED	role mismatch resolved syslog, sent from active switch #2	%VSLP-SW2_SP-5-RRP_ROLE_RESOLVED: Role resolved as ACTIVE by VSLP	role mismatch resolved syslog, sent from active switch #2
ENV-SP-4-FANTRAYFAILED	fan tray failed	%C7600_ENV-SP-4-FANTRAYFAILED: fan tray 2 failed	env sp 4 fan tray fail syslog
PWR-SP-2-PSFAIL	power supply failed	%C7600_PWR-SP-2-PSFAIL: power supply 1 output failed.	pwr sp 2 power supply fail syslog
BGP-5-ADJCHANGE-bfd	handle BGP 5 syslogs for BFD	%BGP-5-ADJCHANGE: neighbor 192.168.20.1 Down BFD adjacency down	BGP neighbor down syslog
BGP-5-ADJCHANGE-bfd	handle BGP 5 syslogs for BFD	%BGP-5-ADJCHANGE: neighbor 192.168.20.1 UP BFD adjacency up	BGP neighbor up syslog

Table 17-3 Cisco IOS Syslogs (continued)

Syslog Name	Description	Raw Format	Short Description
VRRP-6-STATECHANGE	Virtual Router Redundancy Protocol (VRRP) message: The VRRP router has changed state.	%VRRP-6-STATECHANGE: Fa0/1 Grp 1 state Backup -> Master	VRRP State Changed syslog
ATM_AIM-5-ACTIVE_LINK_(DOWN|UP)	The specified link in the specified IMA group has become inactive/active	%ATM_AIM-5-ACTIVE_LINK_DOWN: Interface ATM1/0 of IMA Group ATM0/IMA2 is now inactive	Ima Link Status Change Down Syslog
ATM_AIM-5-ACTIVE_LINK_(DOWN|UP)	The specified link in the specified IMA group has become inactive/active	%ATM_AIM-5-ACTIVE_LINK_UP: Interface ATM1/0 of IMA Group ATM0/IMA2 is now active	Ima Link Status Change Up Syslog
ATM_AIM-5-ACTIVE_LINK_CHANGE	Active links were added to or removed from the group, changing the bandwidth of the group	%ATM_AIM-5-ACTIVE_LINK_CHANGE : IMA Group ATM3/1/ima0 now has 2 active links	IMA Active Link Change Syslog
CDP-4-NATIVE_VLAN_MISMATCH	Native VLAN mismatch discovered	%CDP-4-NATIVE_VLAN_MISMATCH: Native VLAN mismatch discovered on GigabitEthernet1/1 (12), with 3750E-24TD-AGG3 FastEthernet0/2 (1)	Native VLAN mismatch discovered
TOP_MODULE-6-CLK_STATUS_CHANGE	Clock status change	Mar 19 15:26:54.371: %TOP_MODULE-6-CLK_STATUS_CHANGE: PLL clock changed to LOCKED	Clock status change syslog
TOP_MODULE-6-CLK_SOURCE_CHANGE	Clock source change	Mar 19 15:15:40.523: %TOP_MODULE-6-CLK_SOURCE_CHANGE: Changing clock reference source to Seconary TDM 8KHZ	Clock source change syslog
L2-L2VPN_PW-3-UPDOWN	The L2VPN Pseudowire went down	%L2-L2VPN_PW-3-UPDOWN : Pseudowire with address 2.2.2.2, id 140, state is Down	pseudo wire tunnel down syslog
L2-L2VPN_PW-3-UPDOWN	The L2VPN Pseudowire went up	%L2-L2VPN_PW-3-UPDOWN : Pseudowire with address 2.2.2.2, id 140, state is Up	pseudo wire tunnel up syslog
ETHER_SERVICE-6-ERR_DISABLED	Service instance shutdown due to errdisable.	%ETHER_SERVICE-6-ERR_DISABLED : Mac security violation - shutdown service instance 900 on interface GigabitEthernet10/0/12	EFP service error disabled syslog
ETHER_SERVICE-6-UPDOWN	Service instance shutdown Syslog	%ETHER_SERVICE-6-UPDOWN: Service instance 111 on interface GigabitEthernet10/0/3 changed to down	EFP down syslog
ETHER_SERVICE-6-UPDOWN	Service instance up Syslog	%ETHER_SERVICE-6-UPDOWN: Service instance 111 on interface GigabitEthernet10/0/3 changed to up	EFP up syslog

Table 17-3 Cisco IOS Syslogs (continued)

Syslog Name	Description	Raw Format	Short Description
REP-SP-4-LINKSTATUS	The Resilient Ethernet Protocol (REP) link status has changed.	<188>950: *Aug 28 05:07:26.987: %REP-SP-4-LINKSTATUS: GigabitEthernet5/11 (segment 1) is non-operational due to neighbor not responding	REP link not operational syslog
REP-SP-4-LINKSTATUS	The Resilient Ethernet Protocol (REP) link status has changed.	<188>949:*Aug 28 05:04:40.690: %REP-SP-4-LINKSTATUS: GigabitEthernet5/11 (segment 1) is operational	REP link operational syslog
OSPFv3-5-ADJCHG	An OSPFv3 neighbor has changed state. The message describes the change and the reason for it. This message appears only if the log-adjacency-changes command is configured for the OSPF process.	%OSPFv3-5-ADJCHG : Process 1, Nbr 192.168.1.1 on Mg0/5/CPU0/1 from FULL to DOWN, Neighbor Down: Interface down or detached	OSPFv3 neighbor down syslog
OSPFv3-5-ADJCHG	An OSPFv3 neighbor has changed state. The message describes the change and the reason for it. This message appears only if the log-adjacency-changes command is configured for the OSPF process.	%OSPFv3-5-ADJCHG : Process 1, Nbr 192.168.1.1 on Mg0/5/CPU0/1 from LOADING to FULL, Neighbor Down: Interface down or detached	OSPFv3 neighbor up syslog
ETHER_CFM-6-ENTER_AIS	handle CFM AIS defect syslog	%ETHER_CFM-6-ENTER_AIS: local mep with mpid 101 level 4 id 7 dir I Interface Ethernet0/0 enters AIS defect condition	CFM enter AIS defect syslog
ETHER_CFM-6-EXIT_AIS	handle CFM AIS defect syslog	%ETHER_CFM-6-EXIT_AIS: local mep with mpid 101 level 4 id 7 dir I Interface Ethernet0/0 enters AIS defect condition	CFM exit AIS defect syslog
E_CFM-6-ENTER_AIS	handle CFM AIS defect syslog	%E_CFM-6-ENTER_AIS: local mep with mpid 7606 level 4 BD/VLAN 22 dir D Interface Gi5/1 enters AIS defect condition	CFM enter AIS defect syslog
E_CFM-6-EXIT_AIS	handle CFM AIS defect syslog	%E_CFM-6-EXIT_AIS: local mep with mpid 7606 level 4 BD/VLAN 22 dir D Interface Gi5/1 enters AIS defect condition	CFM exit AIS defect syslog
ETHER_CFM-6-ENTER_AIS_INT	handle CFM interface AIS defect syslog	%ETHER_CFM-6-ENTER_AIS_INT: Interface Ethernet0/0 enters AIS defect condition for outward direction	CFM interface enter AIS defect syslog

Table 17-3 Cisco IOS Syslogs (continued)

Syslog Name	Description	Raw Format	Short Description
ETHER_CFM-6-EXIT_AIS_INT	handle CFM interface AIS defect syslog	%ETHER_CFM-6-EXIT_AIS_INT: Interface Ethernet0/0 enters AIS defect condition for outward direction	CFM interface exit AIS defect syslog
E_CFM-6-ENTER_AIS_INT	handle CFM interface AIS defect syslog	%E_CFM-6-ENTER_AIS_INT: Interface GigabitEthernet5/1 enters AIS defect condition for Down direction	CFM interface enter AIS defect syslog
E_CFM-6-EXIT_AIS_INT	handle CFM interface AIS defect syslog	%E_CFM-6-EXIT_AIS_INT: Interface GigabitEthernet5/1 enters AIS defect condition for Down direction	CFM interface exit AIS defect syslog
E_CFM-6-ENTER_LCK	handle CFM AIS defect syslog	%E_CFM-6-ENTER_LCK: local mep with mpid 7606 level 4 BD/VLAN 22 dir D Interface Gi5/1 enters LCK defect condition	CFM enter LCK defect syslog
E_CFM-6-EXIT_LCK	handle CFM AIS defect syslog	%E_CFM-6-EXIT_LCK: local mep with mpid 7606 level 4 BD/VLAN 22 dir D Interface Gi5/1 exited LCK defect condition	CFM exit LCK defect syslog
E_CFM-6-ENTER_LCK_INT	CFM interface enter LCK defect syslog	%E_CFM-6-ENTER_LCK_INT: Interface GigabitEthernet5/1 enters LCK defect condition for Down direction	CFM interface enter LCK syslog
E_CFM-6-EXIT_LCK_INT	CFM interface exit LCK defect syslog	%E_CFM-6-EXIT_LCK_INT: Interface GigabitEthernet5/1 exited LCK defect condition for Down direction	CFM interface exit LCK syslog
E_CFM-3-REMOTE_MEP_DOWN	handle Remote MEP syslog	%E_CFM-3-REMOTE_MEP_DOWN: Remote MEP mpid 1911 evc DemoAugEVC vlan 911 MA name DemoAugMA in domain DemoAugDA changed state to down with event code TimeOut.	CFM Mep Down syslog
E_CFM-3-REMOTE_MEP_UP	handle Remote MEP syslog	%E_CFM-6-REMOTE_MEP_UP: Continuity Check message is received from a remote MEP with mpid 755 evc EVC_S4_22 vlan 22 MA name S4_22 domain L4 interface status Up event code Returning.	CFM Mep Up syslog
ETHER_CFM-3-REMOTE_MEP_DOWN	handle Remote MEP syslog	%ETHER_CFM-3-REMOTE_MEP_DOWN: Remote MEP mpid 537 vlan 555 CSIID S4_sw in domain D4_sw changed state to down with event code lastGasp.	CFM Mep Down syslog
ETHER_CFM-3-REMOTE_MEP_UP	handle Remote MEP syslog	%ETHER_CFM-3-REMOTE_MEP_UP: Remote MEP mpid 537 vlan 555 CSIID S4_sw in domain D4_sw changed state to up with event code lastGasp.	CFM Mep Up syslog

Table 17-3 Cisco IOS Syslogs (continued)

Syslog Name	Description	Raw Format	Short Description
E_CFM-6-REMOTE_MEP_DOWN	handle Remote MEP syslog	%E_CFM-6-REMOTE_MEP_DOWN: Continuity Check message is received from a remote MEP with mpid 755 evc EVC_S4_22 vlan 22 MA name S4_22 domain L4 interface status Down event code Returning.	CFM Mep Down syslog
E_CFM-6-REMOTE_MEP_UP	handle Remote MEP syslog	%E_CFM-6-REMOTE_MEP_UP: Continuity Check message is received from a remote MEP with mpid 755 evc EVC_S4_22 vlan 22 MA name S4_22 domain L4 interface status Up event code Returning.	CFM Mep Up syslog
TOP_MODULE-5-APPL_UPDOWN	Timing over packet application syslog	%TOP_MODULE-5-APPL_UPDOWN: Timing over packet application is down	Timing over packet application down syslog
TOP_MODULE-5-APPL_UPDOWN	Timing over packet application syslog	%TOP_MODULE-5-APPL_UPDOWN: Timing over packet application is up	Timing over packet application up syslog
HSRP-5-STATECHANGE	handle hsrp 5 syslog	%HSRP-5-STATECHANGE: GigabitEthernet0/1.555 Grp 55 state Active -> Init	HSRP group change syslog
HSRP-5-STATECHANGE	handle hsrp 5 syslog	%HSRP-5-STATECHANGE: GigabitEthernet0/1.555 Grp 55 state Active -> Standby	HSRP group restored syslog
DWDM-4-G709ALARM	The specified G709 Alarm has been declared	%DWDM-4-G709ALARM : DWDM 2/0/0 : LOS declared	Layer2 G709 alarm syslog
DWDM-4-G709ALARM	The specified G709 Alarm has been cleared	%DWDM-4-G709ALARM : DWDM 2/0/0 : LOS cleared	Layer2 G709 clear syslog
ETHERNET_OAM-3-LOOPBACK_ERROR	Loopback operation on interface has encountered the specified error	%ETHERNET_OAM-3-LOOPBACK_ERROR: Loopback operation on interface Gi1/1/1 has encountered an error(remote client failed to enter the loopback session)	Ethernet OAM Loopback Error syslog
ETHERNET_OAM-5-LINK_MONITOR	A monitored error has been detected to have crossed user-specified threshold	%ETHERNET_OAM-5-LINK_MONITOR: 0 frame errors detected over the last 10x100 milliseconds on interface Gi1/1/1	Ethernet OAM Link Monitor syslog
ETHERNET_OAM-5-LINK_MONITOR_HT_CROSS	A monitored error has been detected to have crossed user-specified (High threshold) threshold	%ETHERNET_OAM-5-LINK_MONITOR_HT_CROSS: High threshold was crossed on Port Channel [chars]'s last operational member port [chars]. Interface [chars] is kept online	Ethernet OAM Link Monitor high threshold syslog
ETHERNET_OAM-6-(ENTER|EXIT)_SESSION	Ethernet OAM Enter/Exit session syslog	%ETHERNET_OAM-6-EXIT_SESSION: The client on interface Gi1/1/1 has left the OAM session	Ethernet OAM exited the session

Table 17-3 Cisco IOS Syslogs (continued)

Syslog Name	Description	Raw Format	Short Description
ETHERNET_OAM-6-(ENTER|EXIT)_SESSION	Ethernet OAM Enter/Exit session syslog	%ETHERNET_OAM-6-ENTER_SESSION: The client on interface Gi1/1/1 has entered the OAM session	Ethernet OAM entered the session
ETHERNET_OAM-6-LINK_TIMEOUT	Ethernet OAM Link timeout Syslog	%ETHERNET_OAM-6-LINK_TIMEOUT: The client on interface Gi1/1/1 has timed out and exited the OAM session	Ethernet OAM Link timeout Syslog
VRRP-6-STATECHANGE	VRRP state change syslog	%VRRP-6-STATECHANGE: Vl1 Grp 1 state Backup -> Master	VRRP backup to master syslog
VRRP-6-STATECHANGE	VRRP state change syslog	%VRRP-6-STATECHANGE: Vl2 Grp 2 state Master -> Backup	VRRP master to backup syslog
ETHER_LMI-6-MISMATCHED_VLAN_(CONFIGURED|NOT_CONFIGURED)	ELMI VLAN not-Configured/Configured Syslog	%ETHER_LMI-6-MISMATCHED_VLAN_CONFIGURED: VLAN 1300 configured but not in VLAN mapping for UNI GigabitEthernet0/0 Interface	ELMI Vlan configured syslog
ETHER_LMI-6-MISMATCHED_VLAN_(CONFIGURED|NOT_CONFIGURED)	ELMI VLAN not-Configured/Configured Syslog	%ETHER_LMI-6-MISMATCHED_VLAN_NOT_CONFIGURED: VLAN 100 not Configured but in VLAN mapping for UNI FastEthernet1/0/23	ELMI Vlan not configured syslog
PM-4-ERR_(DISABLE|RECOVER)_VP	ELMI VLAN enabled/disabled Syslog	%PM-4-ERR_DISABLE_VP: elmi evc down error detected on Gi0/14, vlan 666. Putting in err-disable state	ELMI Vlan disabled syslog
PM-4-ERR_(DISABLE|RECOVER)_VP	ELMI VLAN enabled/disabled Syslog	%PM-4-ERR_RECOVER_VP: Attempting to recover from elmi evc down err-disable state on Gi0/14, vlan 666	ELMI Vlan enabled syslog
ETHERNET_OAM-6-RFI-Dyinggasp	RFI Dying Gasp Failure Events	%ETHERNET_OAM-6-RFI: The client on interface Et0/0 has received a remote failure indication from its remote peer(failure reason = remote client down action = none)	EOAM RFI dying gasp syslog - admin shutdown on peer
ETHERNET_OAM-6-RFI-Dyinggasp	RFI Dying Gasp Failure Events	%ETHERNET_OAM-6-RFI: The client on interface Gi1/1/1 has received a remote failure indication from its remote peer(failure reason = remote client administratively turned off action = none)	EOAM RFI dying gasp syslog - no ethernet oam
ETHERNET_OAM-6-RFI-Dyinggasp	RFI Dying Gasp Failure Events	%ETHERNET_OAM-6-RFI: The client on interface Gi1/1/1 has received a remote failure indication from its remote peer(failure reason = remote client reloaded action = error-disable)	EOAM RFI dying gasp syslog - admin reload on peer
ETHERNET_OAM-6-RFI-Dyinggasp	RFI Dying Gasp Failure Events	%ETHERNET_OAM-6-RFI: The client on interface Gi1/1/1 has received a remote failure indication from its remote peer(failure reason = dying gasp)	EOAM RFI dying gasp syslog - no org specific TLV

Table 17-3 Cisco IOS Syslogs (continued)

Syslog Name	Description	Raw Format	Short Description
ETHERNET_OAM-6-RFI_CLEAR-Dyinggasp	RFI Dying Gasp clear Event	%ETHERNET_OAM-6-RFI_CLEAR: The client on interface Et0/0 has received a clear of remote failure indication from its remote peer(failure reason = dying gasp action = none)	Eoam RFI dying gasp clear syslog
ETHERNET_OAM-6-RFI-linkfault	RFI link fault event	%ETHERNET_OAM-6-RFI: The client on interface Et0/0 has received a remote failure indication from its remote peer(failure reason = link fault action = none)	EOAM RFI link fault syslog
ETHERNET_OAM-6-RFI_CLEAR-linkfault	link fault clear event	%ETHERNET_OAM-6-RFI_CLEAR: The client on interface Et0/0 has received a clear of remote failure indication from its remote peer(failure reason = link fault action = none)	EOAM RFI link fault clear syslog
PM-4-ERR_(DISABLE|RECOVER)	PM Error disable/recover syslog	%PM-4-ERR_DISABLE: oam-remote-failure error detected on Gi0/1, putting Gi0/1 in err-disable state	PM Error disable syslog
PM-4-ERR_(DISABLE|RECOVER)	PM Error disable/recover syslog	%PM-4-ERR_RECOVER: Attempting to recover from link-flap err-disable state on Fa0/28	PM Error recover syslog
PM-SP-4-ERR_(DISABLE|RECOVER)	PM SP Error disable/recover syslog	%PM-SP-4-ERR_DISABLE: oam-remote-failure-dying-gasp error detected on Gi1/13, putting Gi1/13 in err-disable state	PM SP Error disable syslog
ETHERNET_OAM-6-LOOPBACK	Link loopback OAM Event	%ETHERNET_OAM-6-LOOPBACK: Interface Fa1/3 has entered the master loopback mode	Eoam entered master loopback mode syslog
ETHERNET_OAM-6-LOOPBACK	Link loopback OAM Event	%ETHERNET_OAM-6-LOOPBACK: Interface Gi1/1 has exited the master loopback mode.	Eoam exited master loopback mode syslog
ETHERNET_OAM-6-LOOPBACK	Link loopback OAM Event	%ETHERNET_OAM-6-LOOPBACK: Interface Gi1/1/1 has entered the slave loopback mode.	Eoam entered slave loopback mode syslog
ETHERNET_OAM-6-LOOPBACK	Link loopback OAM Event	%ETHERNET_OAM-6-LOOPBACK: Interface Gi1/1/1 has exited the slave loopback mode.	Eoam exited slave loopback mode syslog
TRANSCEIVER-DFC-6-INSERTED	Transceiver inserted syslog	%TRANSCEIVER-DFC3-6-INSERTED: transceiver module inserted in GigabitEthernet3/18	Transceiver inserted syslog
TRANSCEIVER-DFC-6-REMOVED	Transceiver removed syslog	%TRANSCEIVER-DFC3-6-REMOVED: Transceiver module removed from GigabitEthernet3/1	Transceiver removed syslog
OIR-SP-6-INSCARD	handle card remove syslog	%OIR-SP-6-INSCARD: Card removed from slot 3, interfaces up	card in syslog

Table 17-3 Cisco IOS Syslogs (continued)

Syslog Name	Description	Raw Format	Short Description
OIR-SP-6-REMCARD	handle card remove syslog	%OIR-SP-6-REMCARD: Card removed from slot 3, interfaces disabled	card out syslog
MPLS_TE-5-LSP: Sub-LSP	Handled MPLS TE Tunnel sub LSP Up syslog	%MPLS_TE-5-LSP: Sub-LSP 10.10.20.4[336:1]->10.10.20.1_101: UP	MPLS-TE tunnel lsp up syslog
MPLS_TE-5-LSP: Sub-LSP	Handled MPLS TE Tunnel sub LSP Down syslog	MPLS_TE-5-LSP: Sub-LSP 10.10.20.4[336:1]->10.10.20.1_101: DOWN: sub-LSP teardown	MPLS-TE tunnel lsp down syslog
ETHERNET_MLACP-3-PEER_ICCP_VERSION_INCOMPATIBLE		%ETHERNET_MLACP-3-PEER_ICCP_VERSION_INCOMPATIBLE: Peer ICCP version 0 is incompatible with local ICCP version 2	mLACP ICCP Version Incompatible syslog
ETHERNET_MLACP-3-SYS_CFG_DUPL_ID		%ETHERNET_MLACP-3-SYS_CFG_DUPL_ID : Remote mLACP peer has duplicate mLACP node-id 7	mLACP duplicate node-id syslog
ETHERNET_MLACP-3-SYS_CFG_INVALID_ID		%ETHERNET_MLACP-3-SYS_CFG_INVALID_ID : Received invalid mLACP node-id 40 from peer	mLACP invalid node-id syslog
ETHERNET_MLACP-4-CORE_ISOLATION		%ETHERNET_MLACP-4-CORE_ISOLATION : mLACP Core isolation failure: Attempting to failover 10 LAGs in redundancy group 60	mLACP Core isolation failure syslog
ETHERNET_MLACP-4-CORE_CONNECTED		%ETHERNET_MLACP-4-CORE_CONNECTED : mLACP has recovered from a core isolation failure. Attempting to recover 6 LAGs in redundancy group 60	mLACP Core isolation recover syslog
ETHERNET_MLACP-4-PEER_DOWN		%ETHERNET_MLACP-4-PEER_DOWN: mLACP Peer down failure: Attempting to make 0 local LAGs active in redundancy group 60	mLACP Peer down syslog
ETHERNET_MLACP-4-PEER_UP		%ETHERNET_MLACP-4-PEER_DOWN: mLACP Peer down failure: Attempting to make 0 local LAGs active in redundancy group 60	mLACP Peer up syslog
ETHERNET_MLACP-4-PEER_DISCONNECT		%ETHERNET_MLACP-4-PEER_DISCONNECT: An mLACP peer has disconnected from redundancy group 60, attempting to reconnect	mLACP Peer disconnect syslog
ETHERNET_MLACP-6-PEER_CONNECT		%ETHERNET_MLACP-6-PEER_CONNECT: mLACP peer is now connected in redundancy group 60	mLACP Peer connected syslog
MPLS_TP_TUNNEL_UPDOWN	Handle MPLS TP tunnel up syslog	%MPLS-TP-3-UPDOWN: Tunnel-tp10, changed state to up	MPLS TP Tunnel up syslog
MPLS_TP_TUNNEL_UPDOWN	Handle MPLS TP tunnel down syslog	%MPLS-TP-3-UPDOWN: Tunnel-tp10, changed state to Down.	MPLS TP Tunnel down syslog

Table 17-3 Cisco IOS Syslogs (continued)

Syslog Name	Description	Raw Format	Short Description
MPLS_TP_WORKING_PROTECTING_LSP_UPDOWN	Handle MPLS TP LSP down syslog	%LSP-3-UPDOWN: Working LSP 11::1.1.1.1::10::22::2.2.2.2::20::0 is Down: LDI:3.3.3.3::10	MPLS TP Lsp down syslog
MPLS_TP_WORKING_PROTECTING_LSP_UPDOWN	Handle MPLS TP LSP up syslog	%LSP-3-UPDOWN: Working LSP 11::1.1.1.1::10::22::2.2.2.2::20::0 is Up	MPLS TP Lsp Up syslog
MPLS_TP_TUNNEL_SWITCHOVER	MPLS TP tunnel switchover syslog	%MPLS-TP-5-REDUNDANCY: Tunnel-tp10 Switched from Working to Protect	MPLS TP tunnel switched from working to protect
MPLS_TP_TUNNEL_SWITCHOVER	MPLS TP tunnel switchover syslog	%MPLS-TP-5-REDUNDANCY: Tunnel-tp10 Switched from Protect to Working	MPLS TP tunnel switched from protect to working
MPLS_TP_WORKING_PROTECTING_LSP_LOCKDOWN	Lsp entering lockdown syslog	%MPLS-TP-5-LOCKOUT: Working LSP 11::1.1.1.1::10::22::2.2.2.2::20::0 Entering Lock Down State	MPLS TP Lsp enter lockdown syslog
MPLS_TP_WORKING_PROTECTING_LSP_LOCKDOWN	Lsp exiting lockdown syslog	%MPLS-TP-5-LOCKOUT: Working LSP 11::1.1.1.1::10::22::2.2.2.2::20::0 Exiting Lock Down State	MPLS TP Lsp exit lockdown syslog
MPLS_TP_ENDPOINT_CREATED_UPDATED	Tunnel tp endpoint created syslog	%MPLS_TP-5-CONFIG_CHANGED: Tunnel-tp10 is Added	MPLS TP tunnel added syslog
MPLS_TP_ENDPOINT_CREATED_UPDATED	Tunnel tp endpoint updated syslog	%MPLS_TP-5-CONFIG_CHANGED: Tunnel-tp10 is Updated	MPLS TP tunnel updated syslog
MPLS_TP_ENDPOINT_CREATED_UPDATED	Tunnel tp endpoint deleted syslog	%MPLS_TP-5-CONFIG_CHANGED: Tunnel-tp10 is deleted	MPLS TP tunnel deleted syslog
MPLS_TP_MIDPOINT_CREATED_UPDATED	Tunnel tp midpoint created syslog	%LSP-5-CONFIG-CHANGED: LSP 11::1.1.1.1::10::22::2.2.2.2::20::0 is Added	MPLS TP lsp added syslog
MPLS_TP_MIDPOINT_CREATED_UPDATED	Tunnel tp midpoint updated syslog	%LSP-5-CONFIG-CHANGED: LSP 11::1.1.1.1::10::22::2.2.2.2::20::0 is Updated	MPLS TP lsp updated syslog
MPLS_TP_MIDPOINT_CREATED_UPDATED	Tunnel tp midpoint deleted syslog	%LSP-5-CONFIG-CHANGED: LSP 11::1.1.1.1::10::22::2.2.2.2::20::0 is deleted	MPLS TP lsp deleted syslog
MPLS_TP_LINK_CREATED_UPDATED	Mpls tp link created syslog	%MPLS-TP-LINK-5-CONFIG-CHANGED: Link 1, Interface GigabitEthernet0/2/1, NextHop 10.10.10.2 Added	MPLS TP link added syslog
MPLS_TP_LINK_CREATED_UPDATED	Mpls tp link updated syslog	%MPLS-TP-LINK-5-CONFIG-CHANGED: Link 1, Interface GigabitEthernet0/2/1, NextHop 10.10.10.2 Updated	MPLS TP link updated syslog
MPLS_TP_LINK_CREATED_UPDATED	Mpls tp link deleted syslog	%MPLS-TP-LINK-5-CONFIG-CHANGED: Link 1, Interface GigabitEthernet0/2/1, NextHop 10.10.10.2 deleted	MPLS TP link deleted syslog
MPLS_LABEL_RANGE_UPDATED	MPLS static label range updated syslog	%MPLS-LABEL-5-CHANGED: Static Min/Max Label: 500/51000	MPLS TP static label range changed syslog

Table 17-3 Cisco IOS Syslogs (continued)

Syslog Name	Description	Raw Format	Short Description
MPLS_LABEL_RANGE_UPDATED	MPLS dynamic label range updated syslog	%MPLS-LABEL-5-CHANGED: dynamic Min/Max Label: 500/51000	MPLS TP dynamic label range changed syslog
OIR-6-(REM|INS)CARD	handle module out syslog	%OIR-6-INSCARD: Card inserted from slot 4, interfaces disabled	Fan module in syslog
OIR-6-(REM|INS)CARD	handle module out syslog	%OIR-6-REMCARD: Card removed from slot 4, interfaces disabled	Fan module out syslog
OIR-6-(REM|INS)CARD	handle module out syslog	%OIR-6-INSCARD: Card inserted from slot 4, interfaces disabled	Power module in syslog
OIR-6-(REM|INS)CARD	handle module out syslog	%OIR-6-REMCARD: Card removed from slot 4, interfaces disabled	Power module out syslog

Cisco IOX Syslogs

Table 17-4 lists the Cisco IOX Syslogs supported in Prime Network.

Table 17-4 Cisco IOX Syslogs

Syslog Name	Description	Raw Format	Short Description
LINK-3-UPDOWN	The interface hardware has gone either down or up.	%LINK-3-UPDOWN: Interface ATM2/0, changed state to down	Link down syslog
LINK-3-UPDOWN	The interface hardware has gone either down or up.	%LINK-3-UPDOWN: Interface ATM2/0, changed state to up	Link up syslog
LINK-5-CHANGED	The interface has changed state.	%LINK-5-CHANGED: Interface Ethernet5/1, changed state to administratively up	Link down syslog
LINK-5-CHANGED	The interface has changed state.	%LINK-5-CHANGED: Interface Ethernet5/1, changed state to administratively down	Link up syslog
LINEPROTO-5-UPDOWN	The data link level line protocol changed state.	%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet1/0/1, changed state to up	Line down syslog
LINEPROTO-5-UPDOWN	The data link level line protocol changed state.	%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet1/0/1, changed state to up	Line up syslog

Table 17-4 Cisco IOX Syslogs (continued)

Syslog Name	Description	Raw Format	Short Description
OSPF-5-ADJCHG	An OSPF neighbor has changed state. The message describes the change and the reason for it. This message appears only if the log-adjacency-changes command is configured for the OSPF process	%OSPF-5-ADJCHG: Process 1, Nbr 192.168.100.100 on POS1/0 from FULL to DOWN, Neighbor Down: Interface down or detached	OSPF neighbor down syslog
OSPF-5-ADJCHG	An OSPF neighbor has changed state. The message describes the change and the reason for it. This message appears only if the log-adjacency-changes command is configured for the OSPF process	%OSPF-5-ADJCHG: Process 1, Nbr 192.168.100.100 on POS1/0 from FULL to DOWN, Neighbor Down: Interface down or detached	OSPF neighbor up syslog
ENVMON-ADDITIVE-POWER-OVERBUDGET	The power calculated in use by the chassis exceeds that available by the powershelf. This condition could result in an outage of the chassis if action is not immediately taken	PLATFORM-ENVMON-2-POWERSUPPLY_CURRENT: 1 current has reached high level at 1 A	envmon powersupply syslog
ENVMON-ENV-CONDITION	One or more environmental conditions exist on the specified slot. If left untended, they could result in loss of service or even hardware damage	PLATFORM-ENVMON-2-ENV_CONDITION : An environmental condition exists on slot 1	envmon condition syslog
ENVMON-ENV-CONDITION	One or more environmental conditions exist on the specified slot. If left untended, they could result in loss of service or even hardware damage	PLATFORM-ENVMON-2-ENV_CONDITION_CLEAR : The environmental condition on slot 1 has cleared	envmon condition clear syslog
ENVMON-FAN	The fan array specified has reached a warning or critical level and is approaching or approached a condition that is outside the acceptable range	PLATFORM-ENVMON-2-FAN : The fan array 1 has reached high level.	envmon fan syslog
ENVMON-FAN	The fan array specified has reached a warning or critical level and is approaching or approached a condition that is outside the acceptable range	PLATFORM-ENVMON-2-FAN_CLEAR : The fan array 1 has reached high level.	envmon fan clear syslog
ENVMON-LOW-FAN-SPEED-WARNING	Indicates that the fan is spinning very slow	PLATFORM-ENVMON-5-LOW_FAN_SPEED_WARNING : 1 is spinning slow - speed is dRPM (register value = 0xx)	envmon fan syslog

Table 17-4 Cisco IOX Syslogs (continued)

Syslog Name	Description	Raw Format	Short Description
ENVMON-OVERTEMP	The temperature sensor specified has reached a warning or critical level and is approaching or approached a condition that is outside the acceptable range	PLATFORM-ENVMON-2-OVERTEMP : 1 temperature has reached high level	envmon tempretaure syslog
ENVMON-OVERTEMP	The temperature sensor specified has reached a warning or critical level and is approaching or approached a condition that is outside the acceptable range	PLATFORM-ENVMON-2-OVERTEMP_CLEAR : 1 temperature has returned to a normal level	envmon tempretaure clear syslog
ENVMON-PEM-REMOVE	The power entry module specified was detected as removed	PLATFORM-ENVMON-5-PEM_REMOVE : 2 removed from slot 2	card out syslog
ENVMON-PEM-REMOVE	The power entry module specified was detected as removed	PLATFORM-ENVMON-5-PEM_INSERT : 2 inserted into slot 2	card in syslog
ENVMON-POWERSUPPLY-CURRENT	handle envmon powersupply current syslog	PLATFORM-ENVMON-2-POWERSUPPLY_CURRENT: 1 current has reached high level at 1 A	envmon powersupply syslog
ENVMON-POWERSUPPLY-CURRENT	The current supply specified has reached a critical level and is now out of specification	PLATFORM-ENVMON-2-POWERSUPPLY_CURRENT_CLEAR : 1 current has returned to a normal level at d	envmon powersupply clear syslog
ENVMON-POWERSUPPLY-NONOP	The power supply specified has become non operational	PLATFORM-ENVMON-2-POWERSUPPLY_NONOP : Powersupply1 is Non-Operational	envmon powersupply syslog
ENVMON-POWERSUPPLY-NONOP	The power supply specified has become non operational	PLATFORM-ENVMON-2-POWERSUPPLY_NONOP_CLEAR : Powersupply1 has become operational	envmon powersupply clear syslog
ENVMON-POWERSUPPLY-VOLTAGE	The voltage supply specified has reached a critical level and is now out of specification	PLATFORM-ENVMON-2-POWERSUPPLY_VOLTAGE : Powersupply1 voltage has reached high level at 11 V	envmon powersupply syslog
ENVMON-POWERSUPPLY-VOLTAGE	The voltage supply specified has reached a critical level and is now out of specification	PLATFORM-ENVMON-2-POWERSUPPLY_VOLTAGE_CLEAR : Powersupply1 voltage has returned to a normal level at d V	envmon powersupply clear syslog
ENVMON-TEMP	The temperature sensor specified has reached a warning or critical level and is approaching or approached a condition that is outside the acceptable range	PLATFORM-ENVMON-2-OVERTEMP : 1 temperature has reached high level	envmon tempretaure syslog

Table 17-4 Cisco IOX Syslogs (continued)

Syslog Name	Description	Raw Format	Short Description
ENVMON-TEMP	The temperature sensor specified has reached a warning or critical level and is approaching or approached a condition that is outside the acceptable range	PLATFORM-ENVMON-2-OVERTEMP_CLEAR : 1 temperature has returned to a normal level	envmon tempretaure clear syslog
ENVMON-VOLTAGE	The voltage supply specified has reached a critical level and is now out of specification	PLATFORM-ENVMON-2-POWERSUPPLY_VOLTAGE : Powersupply1 voltage has reached high level at 11 V	envmon powersupply syslog
ENVMON-VOLTAGE	The voltage supply specified has reached a critical level and is now out of specification	PLATFORM-ENVMON-2-POWERSUPPLY_VOLTAGE_CLEAR : Powersupply1 voltage has returned to a normal level at d V	envmon powersupply clear syslog
FIA-FIAHW-LOS	This error indicates a problem (Loss of Sync) in the interface between the card reporting error and the switch fabric card in the indicated slot. This error is traffic affecting. Error recovery is triggered by this error	ENVMON-3-FIAHW_LOS : Persistent LOS on serial link (from slot 2)	fabric hardware syslog
FIA-FIAHW-LOS	This error indicates a problem (Loss of Sync) in the interface between the card reporting error and the switch fabric card in the indicated slot. This error is traffic affecting. Error recovery is triggered by this error	ENVMON-3-FIAHW_LOS_CLEAR LOS : cleared on serial link (from slot 2)	fabric hardware clear syslog
FLASH-CARD-REMOVAL	handle flash card insertion or removal syslog	libpcmcia_ide-1-CARD_UNAVAILABLE : flash1: Can not access flash device	flash card removed syslog
FLASH-CARD-REMOVAL	handle flash card insertion or removal syslog	libpcmcia_ide-1-CARD_SWAPPED : flash1: The flash card has been swapped (OIR)	flash card inserted syslog
LIBPARSER-ERR-MEMALLOC	handle memory allocation in syslog	MGBL-LIBPARSER-3-ERR_MEM_ALLOC : s: memory allocation routine failed.	Memory allocation is not available
NODE-RELOAD	handle node reload syslog by sysldr	PLATFORM-SHELFMGR-3-SHUTDOWN_RESET : Node 0/SM2/* is reset due to admin shut shut request	Module reset syslog
NODE-STATE-CHANGE	Indicates a change in the card oper status	PLATFORM-INVMGR-6-NODE_STATE_CHANGE : Node: 0/RP0/*, state: BRINGDOWN	Card oper status changed

Table 17-4 Cisco IOX Syslogs (continued)

Syslog Name	Description	Raw Format	Short Description
NODE-STATE-CHANGE	Indicates a change in the card oper status	PLATFORM-INVMGR-6-NODE_STATE_CHANGE : Node: 0/0/CPU0, state: IOS XR RUN	Card oper status changed
OIROUT	handle module out syslog	%PLATFORM-INV-6-OIROUT : OIR: Node 0/0/CPU0 removed	card out syslog
OIROUT	handle module out syslog	%PLATFORM-INV-6-OIRIN : OIR: Node 0/0/CPU0 inserted	card in syslog
OIROUT-on-CPU0	handle module out syslog	%PLATFORM-INV-6-OIROUT : OIR: Node 0/0/CPU0 removed	card out syslog
OIROUT-on-CPU0	handle module out syslog	%PLATFORM-INV-6-OIRIN : OIR: Node 0/0/CPU0 inserted	card in syslog
PIM-5-NBRCHG	handle pim neighbor syslog	PIM-5-NBRCHG: neighbor 172.72.73.1 DOWN on MgmtEth0/RSP0/CPU0/1	pim neighbor loss syslog
PIM-5-NBRCHG	handle pim neighbor syslog	PIM-5-NBRCHG: neighbor 192.168.2.1 UP on MgmtEth0/RSP0/CPU0/1	pim neighbor up syslog
PIM-5-UPDOWN	handle pim interface syslog	ROUTING-IPV4_PIM-5-INTCHG : PIM interface GigabitEthernet0/3/0/0 DOWN	pim interface down syslog
PIM-5-UPDOWN	handle pim interface syslog	ROUTING-IPV4_PIM-5-INTCHG : PIM interface GigabitEthernet0/3/0/0 UP	pim interface up syslog
PIM-INVALID-JOIN	handle pim invlid join in syslog	ROUTING-IPV4_PIM-5-INVALID_JP : PIM invalid POS0/2/0/0 J/P message from POS0/2/0/0 with RP address 1.1.1.1	pim invalid join syslog
POWERDOWN-RESET	Indicates that the node will be reset because the user has administratively ‘power disable’ or ‘no power disable’ the node	PLATFORM-SHELFMGR-3-POWERDOWN_RESET : Node 0/0/CPU0 is powered off due to admin power off request	Card oper status changed
POWERDOWN-RESET	Indicates that the node will be reset because the user has administratively ‘power disable’ or ‘no power disable’ the node	PLATFORM-SHELFMGR-3-POWERDOWN_RESET : Node 0/0/CPU0 is powered on due to admin power on request	Card oper status changed

Table 17-4 Cisco IOX Syslogs (continued)

Syslog Name	Description	Raw Format	Short Description
SONET-LOCAL-4-ALARM	The specified SONET Alarm has been declared or released	SONET_LOCAL-4-ALARM : Interface SONET/2/0/0: changed SLOS	Line down syslog
SONET-LOCAL-4-ALARM	The specified SONET Alarm has been declared or released	SONET_LOCAL-4-ALARM : Interface SONET/2/0/0: changed SLOS cleared	Line up syslog
SPA-OIROUT	handle invmgr node state change syslog	<SourceID>LC/0/0/CPU0</SourceID> L2-SPA-5-OIR_REMOVED : SPA removed from bay 0	card out syslog
SPA-OIROUT	handle invmgr node state change syslog	<SourceID>LC/0/0/CPU0</SourceID> L2-SPA-5-OIR_INSERTED : SPA discovered in bay 0	card in syslog
ROUTING-LDP-5-NBR_CHANGE	A LDP neighbor has changed state (up/down). If neighbor has went down, then a reason for session going down is also displayed. This message appears only if the log neighbor command is configured for the LDP process.	ROUTING-LDP-5-NBR_CHANGE : Neighbor 7.7.7.7:0, DOWN	LDP neighbor down syslog
ROUTING-LDP-5-NBR_CHANGE	A LDP neighbor has changed state (up/down). If neighbor has went down, then a reason for session going down is also displayed. This message appears only if the log neighbor command is configured for the LDP process.	gRP/0/RP0/CPU0:Sep 25 14:22:35.329 : mpls_ldp[274]: ROUTING-LDP-5-NBR_CHANGE : Neighbor 7.7.7.7:0, UP	LDP neighbor up syslog
BGP-5-ADJCHANGE	The adjacent BGP neighbor was lost	BGP-5-ADJCHANGE : neighbor 172.23.95.15 Down - BGP Notification received: configuration change	BGP neighbor down syslog
BGP-5-ADJCHANGE	The adjacent BGP neighbor was lost	BGP-5-ADJCHANGE : neighbor 172.23.95.15 Up - BGP Notification received: configuration change	BGP neighbor up syslog
SECURITY-4-AUTHEN_FAILED	The user login authentication failed	SECURITY-login-4-AUTHEN_FAILED. : Failed authentication attempt by user 'user_A' from '161.44.192.231'	Login authentication failed syslog

Table 17-4 Cisco IOX Syslogs (continued)

Syslog Name	Description	Raw Format	Short Description
MGBL-INVENTORY-6-PORTS	Sent by the XR device after a card-in event has occured and the If and Entity tables are in sync. Once Prime Network receives the syslog, it will expedite the physical command instead of the card-in syslogs doing the expedite, so that the polling is done only after the tables are synchronized.	%MGBL-INVENTORY-6-PORTS : ifTable INSYNC for card:0/PL7/* entPhysicalIndex:239	If-Table in sync syslog
L2-BFD-6-SESSION_STATE_DOWN	The bfd session is down	%L2-BFD-6-SESSION_STATE_DOWN : BFD session to neighbor 23.1.1.1 on interface GigabitEthernet0/2/0/0 has gone down. Reason: Echo function failed	bfd session down syslog
L2-BFD-6-SESSION_REMOVED	The bfd session has been removed	%L2-BFD-6-SESSION_REMOVED : BFD session to neighbor 23.1.1.1 on interface GigabitEthernet0/2/0/0 has gone down. Reason: Echo function failed	bfd session removed syslog
L2-BFD-6-SESSION_STATE_UP	The bfd session is up	%L2-BFD-6-SESSION_STATE_UP : BFD session to neighbor 23.1.1.1 on interface GigabitEthernet0/2/0/0 has gone down. Reason: Echo function failed	bfd session up syslog
L2-G709-4-ALARM	The specified G709 Alarm has been declared or released	LC/0/0/CPU0:Feb 16 05:36:25.553 : plim_4p_10ge_dwdm[204]: %L2-G709-4-ALARM : DWDM0/0/0/0: LOS	Layer2 G709 alarm syslog
L2-G709-4-ALARM-CLEARED	The specified G709 Alarm has been declared or released	LC/0/0/CPU0:Feb 16 05:36:25.553 : plim_4p_10ge_dwdm[204]: %L2-G709-4-ALARM : DWDM0/0/0/0: LOS cleared	Layer2 G709 clear syslog
L2-DWDM-3-INFO	The DWDM encountered an error that would lead to degraded service	LC/0/0/CPU0:Feb 16 05:36:25.553 : plim_4p_10ge_dwdm[204]: %L2-DWDM-3-INFO dwdm: service degrading error, reason equals ERROR	Layer2 dwdm info syslog

Table 17-4 Cisco IOX Syslogs (continued)

Syslog Name	Description	Raw Format	Short Description
L1-PMENGINE-4-TCA	The specified PM TCA has been declared	%L1-PMENGINE-4-TCA Port [chars] reports [chars] [chars]([chars]) PM TCA with current value [unsigned long long int], threshold [unsigned long long int] in current [chars] interval window	Layer1 PM TCA syslog
L2-SPA-3-POWER_FAILURE	SPA_OK and PWR_OK signals are asserted after the SPA is powered on by LC. These signals are deasserted when there is a power failure on the SPA and this failure indicates that it is an SPA hardware issue. The SPA is put into FAILED state.	%L2-SPA-3-POWER_FAILURE SPA_OK and PWR_OK signal is deasserted on subslot [unsigned int]	Layer2 SPA failure syslog
ROUTING-OSPF-5-ADJCHG	An OSPF routing neighbor has changed state. The message describes the change and the reason for it.	%ROUTING-OSPF-5-ADJCHG : Process 1, Nbr 2.2.2.2 on MgmtEth0/7/CPU0/2 in area 0 from FULL to DOWN, Loading Done,vrf default vrfid 0x60000000	OSPF routing neighbor down syslog
ROUTING-OSPF-5-ADJCHG	An OSPF routing neighbor has changed state. The message describes the change and the reason for it.	%ROUTING-OSPF-5-ADJCHG : Process 1, Nbr 2.2.2.2 on MgmtEth0/7/CPU0/2 in area 0 from LOADING to FULL, Loading Done,vrf default vrfid 0x60000000	OSPF routing neighbor up syslog
OSPFv3-5-ADJCHG	An OSPFv3 neighbor has changed state. The message describes the change and the reason for it. This message appears only if the log-adjacency-changes command is configured for the OSPF process.	%OSPFv3-5-ADJCHG : Process 1, Nbr 192.168.1.1 on Mg0/5/CPU0/1 from FULL to DOWN, Neighbor Down: Interface down or detached	OSPFv3 neighbor down syslog
OSPFv3-5-ADJCHG	An OSPFv3 neighbor has changed state. The message describes the change and the reason for it. This message appears only if the log-adjacency-changes command is configured for the OSPF process.	%OSPFv3-5-ADJCHG : Process 1, Nbr 192.168.1.1 on Mg0/5/CPU0/1 from LOADING to FULL, Neighbor Down: Interface down or detached	OSPFv3 neighbor up syslog
ROUTING-OSPFv3-5-ADJCHG	An IPv6 OSPFv3 neighbor has changed state. The message describes the change and the reason for it. This message appears only if the log-adjacency-changes command is configured for the OSPF process.	%ROUTING-OSPFv3-5-ADJCHG : Process 1, Nbr 192.168.1.1 on Mg0/5/CPU0/1 from FULL to DOWN, Neighbor Down: Interface down or detached	OSPFv3 routing neighbor down syslog

Table 17-4 Cisco IOX Syslogs (continued)

Syslog Name	Description	Raw Format	Short Description
ROUTING-OSPFv3-5-ADJCHG	An IPv6 OSPFv3 neighbor has changed state. The message describes the change and the reason for it. This message appears only if the log-adjacency-changes command is configured for the OSPF process.	%ROUTING-OSPFv3-5-ADJCHG : Process 1, Nbr 192.168.1.1 on Mg0/5/CPU0/1 from LOADING to FULL, Neighbor Down: Interface down or detached	OSPFv3 routing neighbor up syslog
ROUTING-BGP-5-ADJCHANGE	The adjacent BGP neighbor was lost	%ROUTING-BGP-5-ADJCHANGE : neighbor 3.3.3.3 down (VRF: default) %ROUTING-BGP-5-ADJCHANGE : neighbor 2001:210:10:1::1 Down - User clear requested	Routing BGP neighbor down syslog
ROUTING-BGP-5-ADJCHANGE	The adjacent BGP neighbor was lost	%ROUTING-BGP-5-ADJCHANGE : neighbor 3.3.3.3 Up (VRF: default) %ROUTING-BGP-5-ADJCHANGE : neighbor 2001:210:10:1::1 Up	Routing BGP neighbor up syslog
ROUTING-BGP-5-ADJCHANGE	The IPv6 adjacent BGP neighbor was lost	%ROUTING-BGP-5-ADJCHANGE : neighbor 3.3.3.3 down (VRF: default) %ROUTING-BGP-5-ADJCHANGE : neighbor 2001:210:10:1::1 Down - User clear requested	IPv6 Routing BGP neighbor down syslog
ROUTING-BGP-5-ADJCHANGE	The IPv6 adjacent BGP neighbor was lost	%ROUTING-BGP-5-ADJCHANGE : neighbor 3.3.3.3 Up (VRF: default) %ROUTING-BGP-5-ADJCHANGE : neighbor 2001:210:10:1::1 Up	IPv6 Routing BGP neighbor up syslog
L2-L2VPN_PW-3-UPDOWN	The L2VPN Pseudowire went down	%L2-L2VPN_PW-3-UPDOWN : Pseudowire with address 2.2.2.2, id 140, state is Down	pseudo wire tunnel down syslog
L2-L2VPN_PW-3-UPDOWN	The L2VPN Pseudowire went up	%L2-L2VPN_PW-3-UPDOWN : Pseudowire with address 2.2.2.2, id 140, state is Up	pseudo wire tunnel up syslog
ETHER_SERVICE-6-ERR_DISABLED	Service instance shutdown due to errdisable.	%ETHER_SERVICE-6-ERR_DISABLED: Mac security violation - shutdown service instance 900 on interface GigabitEthernet10/0/12	EFP service error disabled syslog

Table 17-4 Cisco IOX Syslogs (continued)

Syslog Name	Description	Raw Format	Short Description
L2-DWDM-3-NOT_YET_IMPLEMENTED	handle L2-DWDM-3-NOT_YET_IMPLEMENTED syslog	%L2-DWDM-3-NOT_YET_IMPLEMENTED dwdm: this function [chars] is not yet implemented	DWDM feature not implemented yet
L2-DWDM-3-FATAL_2	handle L2-DWDM-3-FATAL_2 syslog	%L2-DWDM-3-FATAL_2 dwdm: fatal error encountered, reason equals [chars], errno equals 1	DWDM fatal error with reason and error number
L2-DWDM-3-FATAL	handle L2-DWDM-3-FATAL syslog	%L2-DWDM-3-FATAL dwdm: fatal error encountered, reason equals 1	DWDM fatal error with reason
L2-PLIM-2-EIO_TRAIN	handle L2-PLIM-2-EIO_TRAIN syslog	%L2-PLIM-2-EIO_TRAIN PLA: [chars], [chars]	PLIM EIO training errors syslog
L2-PLIM-3-CHK_ERR	handle L2-PLIM-3-CHK_ERR syslog	%L2-PLIM-3-CHK_ERR PLA: [chars], [chars]	PLIM Checkpoint Initialization Failure syslog
L2-PLIM-3-HW_ERR	handle L2-PLIM-3-HW_ERR syslog	%L2-PLIM-3-HW_ERR asic error: [chars]	PLIM ASIC error syslog
L2-PLIM-3-MEM_ERR	handle L2-PLIM-3-MEM_ERR syslog	%L2-PLIM-3-MEM_ERR [chars]	PLIM memory error syslog
L2-PLIM-3-SQUID_ERR	handle L2-PLIM-3-SQUID_ERR syslog	%L2-PLIM-3-SQUID_ERR [chars]	PLIM squid error syslog
L2-PLIM-7-ERR	handle L2-PLIM-7-ERR syslog	%L2-PLIM-7-ERR [chars]	PLIM 7 error syslog
L2-PLIM_OC768-3-CRITICAL_ERROR	handle L2-PLIM_OC768-3-CRITICAL_ERROR syslog	%L2-PLIM_OC768-3-CRITICAL_ERROR [chars]: [chars]: [hex]	PLIM OC768 critical error syslog
L2-PLIM_OC768-6-INFO	handle L2-PLIM_OC768-6-INFO syslog	%L2-PLIM_OC768-6-INFO [chars]: [chars]	PLIM OC768 INFO syslog
L2-PLIM_OC768-7-DEBUG_MSG	handle L2-PLIM_OC768-7-DEBUG_MSG syslog	%L2-PLIM_OC768-7-DEBUG_MSG Debug: [chars]: [chars] errno 1	PLIM OC768 debug syslog
BGP-3-NOTIFICATION	handle BGP 3 syslog	%BGP-3-NOTIFICATION: sent to neighbor 10.10.10.254 4/0 (hold time expired) 0 bytes	BGP notification syslog
BGP-3-NOTIFICATION	handle BGP 3 syslog	%BGP-3-NOTIFICATION: sent to neighbor 10.10.10.254 4/0 (hold time expired) 0 bytes	BGP notification syslog
ROUTING-ISIS-4-ADJCHANGE	handle ROUTING-ISIS-4-ADJCHANGE syslog	RP/0/RSP1/CPU0:Oct 19 19:48:32.212 : isis[240]: %ROUTING-ISIS-4-ADJCHANGE : Adjacency to AGS2a (Bundle-Ether1) (L1) Down, Interface state down	routing ISIS neighbor down syslog

Table 17-4 Cisco IOX Syslogs (continued)

Syslog Name	Description	Raw Format	Short Description
ROUTING-ISIS-4-ADJCHANGE	handle ROUTING-ISIS-4-ADJCHANGE syslog	RP/0/RSP1/CPU0:Oct 19 19:48:32.212 : isis[240]: %ROUTING-ISIS-4-ADJCHANGE : Adjacency to AGS2a (Bundle-Ether1) (L1) Up, Interface state up	routing ISIS neighbor up syslog
IP-VRRP-6-INFO_STATECHANGE	handle VRRP state change syslog	%IP-VRRP-6-INFO_STATECHANGE : GigabitEthernet0_5_0_1 vrid 10: state Backup\t -> Master	Backup to Master change syslog
IP-VRRP-6-INFO_STATECHANGE	handle VRRP state change syslog	%IP-VRRP-6-INFO_STATECHANGE : GigabitEthernet0_5_0_1 vrid 10: state Master\t -> Backup	Master to Backup change syslog
IP-STANDBY-6-INFO_STATECHANGE	IP STANDBY 6 INFO STATECHANGE Syslog	%IP-STANDBY-6-INFO_STATECHANGE : SB81: GigabitEthernet0/4/1/3: state Active -> Init	IP standby state change syslog
IP-STANDBY-6-INFO_STATECHANGE	IP STANDBY 6 INFO STATECHANGE Syslog	%IP-STANDBY-6-INFO_STATECHANGE : SB81: GigabitEthernet0/4/1/3: state Standby -> Active	IP standby state restored syslog
L2-DWDM-5-SRLG_OVERFLOW	CTC has more than 100 values to configure, it indicates this situation by configuring the 101st value with a positive integer	%L2-DWDM-5-SRLG_OVERFLOW DWDM: 15: 150, Overflow of SRLGs: 105	DWDM5 SRLG OVERFLOW syslog
L2-SONET_APS-6-UPDOWN	handle L2-SONET_APS-6-UPDOWN syslog	%L2-SONET_APS-6-UPDOWN : SONET0_0_3_0 Group 1 Channel 0 Disabled	L2 SONET APS Disabled syslog
L2-SONET_APS-6-UPDOWN	handle L2-SONET_APS-6-UPDOWN syslog	%L2-SONET_APS-6-UPDOWN : SONET0_0_3_0 Group 1 Channel 0 Enabled	L2 SONET APS enabled syslog
L2-BFD-6-SESSION_REMOVED	The member link bfd session is down	bfd_agent[125]: %L2-BFD-6-SESSION_STATE_DOWN : BFD session to neighbor 23.1.1.1 on interface GigabitEthernet0/2/0/0 has gone down. Reason: Echo function failed	Bfd per member link session down syslog
L2-BFD-6-SESSION_STATE_UP	The member link bfd session is up	bfd_agent[125]: %L2-BFD-6-SESSION_STATE_UP : BFD session to neighbor 199.109.10.2 on interface GigabitEthernet0/1/0/0 is up	Bfd per member link session up syslog

Table 17-4 Cisco IOX Syslogs (continued)

Syslog Name	Description	Raw Format	Short Description
L2-BFD-6-SESSION_STATE_DOWN	The bundle link bfd session is down	RP/0/RP0/CPU0:Sep 17 09:48:53 : bfd[133]: %L2-BFD-6-SESSION_STATE_DOWN : BFD session to neighbor 199.109.10.2 on interface Bundle-Ether999 has gone down. Reason: None	Bfd session state down syslog
L2-BFD-6-SESSION_STATE_UP	The bundle link bfd session is up	RP/0/RP0/CPU0:Sep 17 10:00:29 : bfd[133]: %L2-BFD-6-SESSION_STATE_UP : BFD session to neighbor 199.109.10.2 on interface Bundle-Ether999 is up	Bfd session state up syslog
L2-BM-6-ACTIVE	bundle manager inactive syslog	RP/0/RP0/CPU0:Sep 17 09:48:53 : BM-DISTRIB[1115]: %L2-BM-6-ACTIVE : GigabitEthernet0/1/0/0 is no longer Active as part of Bundle-Ether999 (Bundle has been shut down)	Bundle manager inactive syslog
L2-BM-6-ACTIVE	bundle manager active syslog	RP/0/RP0/CPU0:Sep 17 10:00:32 : BM-DISTRIB[1115]: %L2-BM-6-MBR_BFD_SESSION_UP : The BFD session on link GigabitEthernet0/1/0/1 in Bundle-Ether999 has gone UP	Bundle manager active syslog
L2-BM-6-MBR_BFD_STARTING	bundle manager bfd starting syslog	RP/0/RP0/CPU0:Sep 17 10:00:14 : BM-DISTRIB[1115]: %L2-BM-6-MBR_BFD_STARTING : The BFD session on link GigabitEthernet0/1/0/0 in Bundle-Ether999 is starting. Waiting for 30 seconds for peer to establish session.	Bundle manager bfd session starting syslog
L2-BM-6-MBR_BFD_SESSION_UP	bundle manager bfd session up syslog	RP/0/RP0/CPU0:Sep 17 10:00:32 : BM-DISTRIB[1115]: %L2-BM-6-MBR_BFD_SESSION_UP : The BFD session on link GigabitEthernet0/1/0/1 in Bundle-Ether999 has gone UP	Bundle manager bfd session up syslog

Table 17-4 Cisco IOX Syslogs (continued)

Syslog Name	Description	Raw Format	Short Description
ROUTING-MPLS_TE-4-WARN	Bfd MPLS TE warning syslog	RP/0/RP0/CPU0:Sep 28 07:02:25.636 : te_control[1120]: %ROUTING-MPLS_TE-4-WARN : TE-BFD not configured on intf Bundle-Ether1.1, FRR or Path Protection triggered to be consistent with forwarding	Bfd MPLS TE warning syslog
L2-BFD-6-SESSION_INHERIT	Bfd session inherit off syslog	RP/0/RP0/CPU0:Dec 8 14:17:17.316 : bfd[134]: %L2-BFD-6-SESSION_INHERIT_OFF : BFD session to neighbor 192.168.88.2 on interface Bundle-Ether1.1 is not inheriting state from session over Bundle-Ether1	Bfd session inherit off syslog
L2-BFD-6-SESSION_INHERIT	Bfd session inherit on syslog	RP/0/RP0/CPU0:Sep 28 07:04:40.408 : bfd[133]: %L2-BFD-6-SESSION_INHERIT_ON : BFD session to neighbor 198.108.10.1 on interface Bundle-Ether1.1 is inheriting state from session over Bundle-Ether1	Bfd session inherit on syslog
MAC_TABLE_RESYNC_COMPLETE	Resynchronization of the MAC address table is complete	"LC/0/0/CPU0:Jun 16 9:37:05.189 : l2fib[193]: %L2-L2FIB-5-MAC_TABLE_RESYNC_COMPLETE : The resynchronization of the MAC address table is complete 0/0/CPU0"	Resynchronization of the MAC address table is complete
NODE-STATE-CHANGE	Indicates a change in the card oper status	PLATFORM-INVMGR-6-NODE_STATE_CHANGE : Node: 0/RP0/*, state: BRINGDOWN	Fan module oper status changed
NODE-STATE-CHANGE	Indicates a change in the card oper status	PLATFORM-INVMGR-6-NODE_STATE_CHANGE : Node: 0/0/CPU0, state: IOS XR RUN	Fan module oper status changed
OIROUT	handle module out syslog	%PLATFORM-INV-6-OIROUT : OIR: Node 0/0/CPU0 removed	Fan module out syslog
OIROUT	handle module out syslog	%PLATFORM-INV-6-OIRIN : OIR: Node 0/0/CPU0 inserted	Fan module in syslog

Table 17-4 Cisco IOX Syslogs (continued)

Syslog Name	Description	Raw Format	Short Description
NODE-STATE-CHANGE	Indicates a change in the card oper status	PLATFORM-INVMGR-6-NODE_STATE_CHANGE : Node: 0/RP0/*, state: BRINGDOWN	Power module oper status changed
NODE-STATE-CHANGE	Indicates a change in the card oper status	PLATFORM-INVMGR-6-NODE_STATE_CHANGE : Node: 0/0/CPU0, state: IOS XR RUN	Power module oper status changed
OIROUT	handle module out syslog	%PLATFORM-INV-6-OIROUT : OIR: Node 0/0/CPU0 removed	Power module out syslog
OIROUT	handle module out syslog	%PLATFORM-INV-6-OIRIN : OIR: Node 0/0/CPU0 inserted	Power module in syslog
L2-SONET_APS-6-K1K2_INFO	handle L2-SONET_APS-6-K1K2_INFO	%L2-SONET_APS-6-K1K2_INFO : Group 10: Tx K1K2 0x21 0x15 , Rx K1K2 0x81 0x15	L2 Sonet APS 6 K1K2 info syslog
L2-SONET_APS-6-CONTACT	handle L2-SONET_APS-6-CONTACT	%L2-SONET_APS-6-CONTACT : PGP Link Up Group 10 Channel 1 Contacted	L2 Sonet APS 6 Contact syslog
L2-T3E3-4-UPDOWN-INFO	handle t3e3 syslog line state UP	.*%L2-T3E3-4-UPDOWN.*:\s*(\S+):\s*LINESTATE\s*(\S+).*	L2 T3E3 line state up syslog
L2-T3E3-4-UPDOWN-INFO	handle t3e3 syslog line state DOWN	.*%L2-T3E3-4-UPDOWN.*:\s*(\S+):\s*LINESTATE\s*(\S+).*	L2 T3E3 line state down syslog
SONET-LOCAL-4-ALARM	handle SONET Line AIS cleared syslog	.*SONET_LOCAL-4-ALARM.*:\s(\S+):\s*(\S+)*\s*	SONET Line AIS cleared syslog
SONET-LOCAL-4-ALARM	handle SONET PATH AIS cleared syslog	.*SONET_LOCAL-4-ALARM.*:\s(\S+):\s*(\S+)*\s*	SONET PATH AIS cleared syslog
SONET-LOCAL-4-ALARM-UP	handle SONET Line AIS syslog	.*SONET_LOCAL-4-ALARM.*:\s(\S+):\s*(\S+)*\s*(\S+)*\s.*(cleared)\s*	SONET Line AIS syslog
SONET-LOCAL-4-ALARM-UP	handle SONET PATH AIS syslog	.*SONET_LOCAL-4-ALARM.*:\s(\S+):\s*(\S+)*\s*(\S+)*\s.*(cleared)\s*	SONET PATH AIS syslog

Cisco ACE Syslogs

Table 17-5 lists the Cisco ACE Syslogs supported in Prime Network.

Table 17-5 Cisco ACE Syslogs

Syslog Name	Description	Raw Format	Short Description
LINK-5-CHANGED	handle link down syslog	%LINK-5-CHANGED: Interface Ethernet5/1, changed state to administratively up	Link down syslog
LINK-5-CHANGED	handle link down syslog	%LINK-5-CHANGED: Interface Ethernet5/1, changed state to administratively down	Link up syslog
LINK-3-UPDOWN	handle link down syslog	%LINK-3-UPDOWN: Interface ATM2/0, changed state to down	Link down syslog
LINK-3-UPDOWN	handle link down syslog	%LINK-3-UPDOWN: Interface ATM2/0, changed state to up	Link up syslog
ACE-1-106021	Deny protocol reverse path check.	%ACE-1-106021: Deny protocol 0 reverse path check from 11.1.13.110 to 11.1.11.110 on interface vlan12	Deny protocol reverse path check
ACE-1-106028	Access rule memory exhausted.	%ACE-1-106028: WARNING: Unknown error while processing merged list. Incomplete rule is currently applied on interface vlan31. Manual roll back to a previous access rule configuration on this interface is needed	Access rule memory exhausted
ACE-1-444006	License manager exiting.	%ACE-1-444006: License manager exiting: reason	License manager exiting
ACE-1-456029	The ACE attempted to start or set up the application acceleration core daemon process.	%ACE-1-456029: Error creating ACC core process. [reason]	The ACE attempted to start or set up the application acceleration core daemon process
ACE-1-456078	Critical shared memory setup failure.	%ACE-1-456078: Critical shared memory setup failure. [reason]	Critical shared memory setup failure
ACE-1-456080	Critical Semaphore related errors.	%ACE-1-456080: Critical Semaphore related errors. [reason]	Critical Semaphore related errors
ACE-1-456085	A generic alert-level message.	%ACE-1-456085: Message.	A generic alert-level message
ACE-1-456086	The ACE initialization has failed.	%ACE-1-456086: Error initializing the ACE. [reason]	The ACE initialization has failed
ACE-1-727001	Peer IP address is not reachable.	lbm050b/Admin# Jul 31 2009 09:07:09 Admin: %ACE-1-727001: HA: Peer 172.21.5.65 is not reachable. Error: Heartbeat stopped. No alternate interface configured	Peer IP address is not reachable
ACE-1-727002	Peer device is not reachable on an FT Interface.	%ACE-1-727002: HA: FT interface 0 to reach peer 172.28.0.221 is down. Error: Heartbeat stopped. Peer is reachable via alternate interface	Peer device is not reachable on an FT Interface

Table 17-5 Cisco ACE Syslogs (continued)

Syslog Name	Description	Raw Format	Short Description
ACE-1-727003	Mismatch in context names detected for FT group.	%ACE-1-727003: hostname: HA: Mismatch in context names detected for FT	Mismatch incontext names detected for FTgroup
ACE-1-727004	Both devices were detected to be Active for the same FT group.	%ACE-1-727004: HA: Two actives have been detected for FT group 5.	Both devices were detected to be Active for the same FT group
ACE-1-727005	Configuration could not be synced to the peer device.	Dec 13 2006 12:56:16 6K-1_ACE1: %ACE-1-727005: HA: Configuration Replication failed for context SH-Gold. Error : Running configuration sync has completed to peer Jun 19 2007 20:59:09 slot4: %ACE-1-727005: HA: Configuration Replication failed for context user-1. Error : script file not configured	Configuration could not be synced to the peer device
ACE-1-727006	Peer is incompatible.	%ACE-1-727006: HA: Peer 1 is incompatible due to SRG Compatibility Mismatch. Cannot be Redundant.	Peer is incompatible
ACE-1-727007	Module Initialization failure.	%ACE-1-727007: hostname: HA: Module Initialization failure - Error Error str.	Module Initialization failure
ACE-1-727008	Failed to send heartbeats to peer.	34(Nov9 2008 04:46:36): from "KERN" ACE-1-727008:HA: Failed to send heartbeats to peer. Internal error: Failed to communicate to IXP	Failed to send heartbeats to peer
ACE-1-728001	Initialization failure - general.	ACE-1-728001: Initialization failure (general) type variable1.	Initialization failure - general
ACE-1-728002	Initialization failure - sticky.	ACE-1-728002: Initialization failure (sticky) type variable1.	Initialization failure - sticky
ACE-1-728003	Initialization failure - sticky hash.	ACE-1-728003: Initialization failure (sticky hash) variable1 entries, variable2 min, variable3 max type variable4.	Initialization failure - sticky hash
ACE-2-100001	The CLI end of line (EOL) function.	%ACE-2-100001: EOL function chars from library chars exited due to Signal dec	The CLI end of line (EOL) function
ACE-2-199006	Reload started .	6K-1_ACE2-1 login: admApr 4 2008 08:28:56 Admin: %ACE-2-199006: Orderly reload started at Fri Apr 4 08:28:55 2008 by System. Reload reason: Service "cfgmgr"	Reload started
ACE-2-212007	SNMPD initialization failed.	%ACE-2-212007: SNMPD initialization failed while Variable1	SNMPD initialization failed
ACE-2-313006	ICMP Manager Initialization Failed.	%ACE-2-313006: ICMP Manager Initialization Failed. Reason : Variable1	ICMP Manager Initialization Failed

Table 17-5 Cisco ACE Syslogs (continued)

Syslog Name	Description	Raw Format	Short Description
ACE-2-443001	System experienced fatal failure.	Nov 21 18:14:31 172.27.15.69 Nov 21 2007 18:14:30 : %ACE-2-443001: System experienced fatal failure.Service name:ifmgr(910) has terminated on receiving signal 10,reloading system	System experienced fatal failure
ACE-2-444001	License checkout failure.	%ACE-2-444001: License checkout failure for feature ACE-AP-C-UP1: Cannot read data from license server system.	License checkout failure
ACE-2-444004	Evaluation license expired.	%ACE-2-444004: Evaluation license expired for feature ACE-VIRT-050	Evaluation license expired
ACE-2-456014	Invalid stream.	%ACE-2-456014: Invalid stream. [reason]	Invalid stream
ACE-2-456090	Critical error parsing ACC module configuration.	%ACE-2-456090: Critical error parsing ACC module configuration config_directive reason.	Critical error parsing ACC module configuration
ACE-2-727009	Communication failure.	%ACE-2-727009: hostname: HA: Communication failure for Peer Peer id Event: error str.	Communication failure
ACE-2-727010	Data replication failed and not synced to the peer device.	%ACE-2-727010: hostname: HA: Data replication failed for context ctx name. Error code error str.	Data replication failed and not synced to the peer device
ACE-2-727011	Configuration synchronization does not occur.	%ACE-2-727011: HA: FT Group 2 changed state to FSM_FT_STATE_ELECT. Event: FSM_FT_EV_PEER_COMP	Configuration synchronization does not occurred

Table 17-5 Cisco ACE Syslogs (continued)

Syslog Name	Description	Raw Format	Short Description
ACE-2-727012	The state transitions made by an HA state device for a context.	Dec 21 2006 06:04:16 6kbACE: %ACE-2-727012: HA: FT Group 2 changed state to FSM_FT_STATE_STANDBY_BULK. Event: FSM_FT_EV_CFG_SYNC_STATUS Dec 21 2006 06:04:36 6kbACE: %ACE-2-727012: HA: FT Group 1 changed state to FSM_FT_STATE_STANDBY_HOT. Event: FSM_FT_EV_BULK_SYNC_STATUS Dec 21 2006 06:05:19 6kbACE: %ACE-2-727012: HA: FT Group 101 changed state to FSM_FT_STATE_STANDBY_COLD. Event: FSM_FT_EV_CFG_SYNC_STATUS Dec 21 2006 06:05:24 6kbACE: %ACE-2-727012: HA: FT Group 1 changed state to FSM_FT_STATE_STANDBY_COLD. Event: FSM_FT_EV_MAINT_MODE_SBY_COLD	The state transitions made by an HA state device for a context.
ACE-2-727013	The peer is now reachable.	%ACE-2-727013: hostname: HA: Peer Peer # is UP and reachable.	The peer is now reachable
ACE-2-727014	The redundancy heartbeats from a peer have become unidirectional.	%ACE-2-727014: hostname: HA: Heartbeats from Peer Peer id have become unidirectional.	The redundancy heartbeats from a peer have become unidirectional
ACE-2-727015	Detected mismatch in heartbeat interval from the peer.	%ACE-2-727015: hostname: HA: Detected mismatch in heartbeat interval from Peer peer id. Modified interval to interval.	Detected mismatch in heartbeat interval from the peer
ACE-2-727016	The replication is being carried out to a peer.	%ACE-2-727016: hostname: HA: Replication for context ctx name has started. Status - status.	The replication is being carried out to a peer
ACE-2-727017	ACE FT Track UP syslog	%ACE-2-727017: hostname: HA: FT Track track type track name is UP.	ACE FT Track UP syslog
ACE-2-727018	ACE FT Track DOWN syslog	%ACE-2-727018: hostname: HA: FT Track track type track name is DOWN.	ACE FT Track DOWN syslog
ACE-LB_General-2-728033	Drop connection as Application Acceleration Maximum.	%ACE-LB_General-2-728033: Drop connection as Application Acceleration Maximum concurrent connection is x (maximum was x connections)	Drop connection as Application Acceleration Maximum

Table 17-5 Cisco ACE Syslogs (continued)

Syslog Name	Description	Raw Format	Short Description
ACE-LB_General-2-728035	Disabled Web Application Acceleration	%ACE-LB_General-2-728035: Disabled Web Application Acceleration: Maximum configured concurrent connections limit (<count>) reached, sending connections to real servers	Disabled Web Application Acceleration
ACE-LB_General-2-728036	Enabled Web Application Acceleration.	%ACE-LB_General-2-728036: Enabled Web Application Acceleration: New connections will be sent for Optimization.(concurrent connections count <count>)	Enabled Web Application Acceleration

Cisco Nexus Syslogs

Table 17-6 lists the Cisco Nexus Syslogs supported in Prime Network.

Table 17-6 Cisco Nexus Syslogs

Syslog Name	Description	Raw Format	Short Description
HSRP_ENGINE-6-STATECHANGE	handle HSRP_ENGINE-6-STATECHANGE syslog	2009 Dec 15 07:32:14 MCS2-COREDP-NX-MCS2-DP-NX %HSRP_ENGINE-6-STATECHANGE: Vlan279 Grp 279 state move to Init	HSRP group change syslog
HSRP_ENGINE-6-STATECHANGE	handle HSRP_ENGINE-6-STATECHANGE syslog	2009 Dec 15 07:32:13 MCS2-COREDP-NX-MCS2-DP-NX %HSRP_ENGINE-6-STATECHANGE: Vlan279 Grp 279 state move to Active	HSRP group restored syslog
BGP-5-ADJCHANGE	handle BGP 5 syslog	2009 Sep 23 13:54:50 NEXUS-TRUE-CORE-1 %BGP-5-ADJCHANGE: bgp-7470 [4713] (default) neighbor 61.91.210.49 Down - session closed	BGP neighbor down syslog
BGP-5-ADJCHANGE	handle BGP 5 syslog	2009 Sep 23 13:54:50 NEXUS-TRUE-CORE-1 %BGP-5-ADJCHANGE: bgp-7470 [4713] (default) neighbor 61.91.210.49 Up - session closed	BGP neighbor up syslog
OSPF-5-ADJCHANGE	handle OSPF-5-ADJCHANGE syslog	2009 Mar 4 22:21:45 NEXUS-TRUE-CORE-1 %OSPF-5-ADJCHANGE: ospf-100 [4324] Nbr 203.144.143.114 on Vlan48 went DOWN	OSPF neighbor down syslog
OSPF-5-ADJCHANGE	handle OSPF-5-ADJCHANGE syslog	2009 Mar 4 22:21:45 NEXUS-TRUE-CORE-1 %OSPF-5-ADJCHANGE: ospf-100 [4324] Nbr 203.144.143.114 on Vlan48 went DOWN	OSPF neighbor up syslog

Table 17-6 Cisco Nexus Syslogs (continued)

Syslog Name	Description	Raw Format	Short Description
OSPF-5-NBRSTATE	handle OSPF-5-NBRSTATE syslog	OSPF-5-NBRSTATE Format: Process %s, Nbr %s on %s from %s to %s, %s	OSPF neighbor down syslog
OSPF-5-NBRSTATE	handle OSPF-5-NBRSTATE syslog	OSPF-5-NBRSTATE Format: Process %s, Nbr %s on %s from %s to %s, %s	OSPF neighbor up syslog
PORT-5-IF_DOWN_ADMIN_DOWN	PORT-5-IF_DOWN Syslogs	PORT-5-IF_DOWN_ADMIN_DOWN: Interface [chars] is down (Administratively down)	Interface is down syslog
PORT-5-IF_DOWN_BIT_ERR_RT_THRES_EXCEEDED	PORT-5-IF_DOWN Syslogs	PORT-5-IF_DOWN_BIT_ERR_RT_THRES_EXCEEDED: Interface [chars] is down (Error disabled - bit error rate too high).	Configuration error has occurred syslog
PORT-5-IF_DOWN_BUNDLE_MISCFG	PORT-5-IF_DOWN Syslogs	PORT-5-IF_DOWN_BUNDLE_MISCFG: Interface [chars] is down (Isolation due to channel mis-configuration on local or remote switch)	Configuration error has occurred syslog
PORT-5-IF_DOWN_CHANNEL_ADMIN_DOWN	PORT-5-IF_DOWN Syslogs	PORT-5-IF_DOWN_CHANNEL_ADMIN_DOWN: Interface [chars] is down (Channel admin down)	Interface is down syslog
PORT-5-IF_DOWN_DENIED_DUE_TO_PORT_BINDING	PORT-5-IF_DOWN Syslogs	PORT-5-IF_DOWN_DENIED_DUE_TO_PORT_BINDING: Interface [chars] is down(Suspended due to port binding)	Configuration error has occurred syslog
PORT-5-IF_DOWN_DOMAIN_ADDR_ASSIGN_FAILURE_ISOLATION	PORT-5-IF_DOWN Syslogs	PORT-5-IF_DOWN_DOMAIN_ADDR_ASSIGN_FAILURE_ISOLATION: Interface [chars] is down (Isolation due to domain id assignment failure)	Configuration error has occurred syslog
PORT-5-IF_DOWN_DOMAIN_INVALID_RCF_RECEIVED	PORT-5-IF_DOWN Syslogs	PORT-5-IF_DOWN_DOMAIN_INVALID_RCF_RECEIVED: Interface [chars] is down (Isolation due to invalid fabric reconfiguration)	Configuration error has occurred syslog
PORT-5-IF_DOWN_DOMAIN_MANAGER_DISABLED	PORT-5-IF_DOWN Syslogs	PORT-5-IF_DOWN_DOMAIN_MANAGER_DISABLED: Interface [chars] is down (Isolation due to domain manager disabled)	Configuration error has occurred syslog
PORT-5-IF_DOWN_DOMAIN_MAX_RETRANSMISSION_FAILURE	PORT-5-IF_DOWN Syslogs	PORT-5-IF_DOWN_DOMAIN_MAX_RETRANSMISSION_FAILURE: Interface [chars] is down (Isolation due to domain manager other side not responding)	Configuration error has occurred syslog
PORT-5-IF_DOWN_DOMAIN_NOT_ALLOWED_ISOLATION	PORT-5-IF_DOWN Syslogs	PORT-5-IF_DOWN_DOMAIN_NOT_ALLOWED_ISOLATION: Interface [chars] is isolated (domain not allowed)	Configuration error has occurred syslog

Table 17-6 Cisco Nexus Syslogs (continued)

Syslog Name	Description	Raw Format	Short Description
PORT-5-IF_DOWN_DOMAIN_OTHER_SIDE_EPORT_ISOLATED	PORT-5-IF_DOWN Syslogs	PORT-5-IF_DOWN_DOMAIN_OTHER_SIDE_EPORT_ISOLATED: Interface [chars] is down (Isolation due to domain other side eport isolated)	Configuration error has occurred syslog
PORT-5-IF_DOWN_DOMAIN_OVERLAP_ISOLATION	PORT-5-IF_DOWN Syslogs	PORT-5-IF_DOWN_DOMAIN_OVERLAP_ISOLATION: Interface [chars] is down (Isolation due to domain overlap)	Configuration error has occurred syslog
PORT-5-IF_DOWN_EPP_FAILURE	PORT-5-IF_DOWN Syslogs	PORT-5-IF_DOWN_EPP_FAILURE: Interface [chars] is down (Error Disabled - EPP Failure)	Configuration error has occurred syslog
PORT-5-IF_DOWN_FABRIC_BIND_FAILURE	PORT-5-IF_DOWN Syslogs	PORT-5-IF_DOWN_FABRIC_BIND_FAILURE: Interface [chars] is down(Isolation due to fabric bind failure)	Configuration error has occurred syslog
PORT-5-IF_DOWN_INCOMPATIBLE_ADMIN_RXBUFSIZE	PORT-5-IF_DOWN Syslogs	PORT-5-IF_DOWN_INCOMPATIBLE_ADMIN_RXBUFSIZE: Interface [chars] is down (Error disabled - Incompatible admin port rxbufsize)	Configuration error has occurred syslog
PORT-5-IF_DOWN_INCOMPATIBLE_ADMIN_SPEED	PORT-5-IF_DOWN Syslogs	PORT-5-IF_DOWN_INCOMPATIBLE_ADMIN_SPEED: Interface [chars] is down (Error disabled - Incompatible admin port speed)	Configuration error has occurred syslog
PORT-5-IF_DOWN_INTERFACE_REMOVED	PORT-5-IF_DOWN Syslogs	PORT-5-IF_DOWN_INTERFACE_REMOVED: Interface [chars] is down (Interface removed)	Interface is removed syslog
PORT-5-IF_DOWN_INVALID_CONFIG	PORT-5-IF_DOWN Syslogs	PORT-5-IF_DOWN_INVALID_CONFIG: Interface [chars] is down(Error disabled - Possible PortChannel misconfiguration)	Configuration error has occurred syslog
PORT-5-IF_DOWN_INVALID_FABRIC_BINDING	PORT-5-IF_DOWN Syslogs	PORT-5-IF_DOWN_INVALID_FABRIC_BINDING: Interface [chars] is down(Invalid fabric binding exchange)	Configuration error has occurred syslog
PORT-5-IF_DOWN_LINK_FAILURE	PORT-5-IF_DOWN Syslogs	PORT-5-IF_DOWN_LINK_FAILURE: Interface [chars] is down (Link failure)	Link down syslog
PORT-5-IF_DOWN_LOOPBACK_DIAG_FAILURE	PORT-5-IF_DOWN Syslogs	PORT-5-IF_DOWN_LOOPBACK_DIAG_FAILURE: Interface [chars] is down (Diag failure)	Configuration error has occurred syslog
PORT-5-IF_DOWN_LOOPBACK_ISOLATION	PORT-5-IF_DOWN Syslogs	PORT-5-IF_DOWN_LOOPBACK_ISOLATION: Interface [chars] is down (Isolation due to port loopback to same switch)	Configuration error has occurred syslog
PORT-5-IF_DOWN_MODULE_REMOVED	PORT-5-IF_DOWN Syslogs	PORT-5-IF_DOWN_MODULE_REMOVED: Interface [chars] is down (module removed)	Interface down due to module syslog

Table 17-6 Cisco Nexus Syslogs (continued)

Syslog Name	Description	Raw Format	Short Description
PORT-5-IF_DOWN_NONE	PORT-5-IF_DOWN Syslogs	PORT-5-IF_DOWN_NONE: Interface [chars] is down (None)	Interface is down syslog
PORT-5-IF_DOWN_NOS_RCVD	PORT-5-IF_DOWN Syslogs	PORT-5-IF_DOWN_NOS_RCVD: Interface [chars] is down (NOS received)	Link down syslog
PORT-5-IF_DOWN_OFFLINE	PORT-5-IF_DOWN Syslogs	PORT-5-IF_DOWN_OFFLINE: Interface [chars] is down (Offline)	Interface is down syslog
PORT-5-IF_DOWN_OHMS_EXTERNAL_LB_TEST	PORT-5-IF_DOWN Syslogs	PORT-5-IF_DOWN_OHMS_EXTERNAL_LB_TEST: Interface [chars] is down(Loopback test)	Interface is down syslog
PORT-5-IF_DOWN_OLS_RCVD	PORT-5-IF_DOWN Syslogs	PORT-5-IF_DOWN_OLS_RCVD: Interface [chars] is down (OLS received)	Link down syslog
PORT-5-IF_DOWN_PARENT_ADMIN_DOWN	PORT-5-IF_DOWN Syslogs	PORT-5-IF_DOWN_PARENT_ADMIN_DOWN: Interface [chars] is down (Parent interface down)	Interface is down syslog
PORT-5-IF_DOWN_PORT_CHANNEL_MEMBERS_DOWN	PORT-5-IF_DOWN Syslogs	PORT-5-IF_DOWN_PORT_CHANNEL_MEMBERS_DOWN: Interface [chars] is down (No operational members)	Interface is down syslog
PORT-5-IF_DOWN_SUSPENDED	PORT-5-IF_DOWN Syslogs	PORT-5-IF_DOWN_SUSPENDED: Interface [chars] is down (Suspended)	Configuration error has occurred syslog
PORT-5-IF_DOWN_SUSPENDED_BY_MODE	PORT-5-IF_DOWN Syslogs	PORT-5-IF_DOWN_SUSPENDED_BY_MODE: Interface [chars] is down (Suspended due to incompatible mode)	Configuration error has occurred syslog
PORT-5-IF_DOWN_SUSPENDED_BY_SPEED	PORT-5-IF_DOWN Syslogs	PORT-5-IF_DOWN_SUSPENDED_BY_SPEED: Interface [chars] is down (Suspended due to incompatible speed)	Configuration error has occurred syslog
PORT-5-IF_DOWN_SUSPENDED_BY_WWN	PORT-5-IF_DOWN Syslogs	PORT-5-IF_DOWN_SUSPENDED_BY_WWN: Interface [chars] is down (Suspended due to incompatible remote switch WWN)	Configuration error has occurred syslog
PORT-5-IF_DOWN_UPGRADE_IN_PROGRESS	PORT-5-IF_DOWN Syslogs	PORT-5-IF_DOWN_UPGRADE_IN_PROGRESS: Interface [chars] is down (Linecard upgrade in progress)	Interface is removed syslog
PORT-5-IF_UP	PORT-5-IF_UP syslog	PORT-5-IF_UP: Interface [chars] is up [chars].	Interface is up syslog
IPV6-6-CONFIG_EVENT	IPV6_config_event	IPV6-6-CONFIG_EVENT: IP Configuration Msg: [chars]	IPV6 configuration changed syslog
IPV6-6-INTERFACE_DELETED	IPV6_interface_deleted	IPV6-6-INTERFACE_DELETED: The interface [chars] has been deleted	IPV6 interface deleted syslog

Table 17-6 Cisco Nexus Syslogs (continued)

Syslog Name	Description	Raw Format	Short Description
IPV6-6-INTERFACE_EVENT	IPV6_interface_event	IPV6-6-INTERFACE_EVENT: IP address [chars] [chars] on interface [chars]	IPV6 interface changed syslog
IPv6-6-IPV6_STATS_ERROR	IPV6_stats_error	IPv6-6-IPV6_STATS_ERROR Format: Failed to get hardware statistics for interface %s, reason %s	IPV6 stats error syslog
IPV6-6-ROUTE_NOT_ACTIVE	IPV6_route_not_active	IPV6-6-ROUTE_NOT_ACTIVE: The [chars] is not active	IPV6 route not active syslog
IPV6-6-STARTING	IPV6_starting	IPV6-6-STARTING: IP configuration Manager started	IPV6 configuration manager started
IPv6-6-v6_REG_SEND_MSG	IPV6_register_send_message	IPv6-6-v6_REG_SEND_MSG Format: Suppress PIM6 Data Register for (%s, %s) due to suppression-timer	IPV6 PIM6 Data Register suppressed syslog

Cisco ASR 9000 Syslog Registry Parameters

Table 17-7 lists the associated event types, event subtypes, and Prime Network registry parameters for the Cisco ASR 9000 syslogs shown in Table 17-1.

Table 17-7 Cisco ASR 9000 Syslog Registry Parameters

Short Description	Event Type	Event Subtype	Subtype Value	Expedites Polling	Event Source (IMO Name)	Activate	Correlate	Is Correlation Allowed	Weight	Auto Clear	Severity	Is Ticketable	Auto Remove	Flapping
Power supply inserted syslog	power supply removed syslog	power supply inserted syslog	inserted	N	IModule	F	F	F	0	T	clr	F	T	F
Power supply removed syslog	power supply removed syslog	power supply removed syslog	removed	N	IModule	F	F	F	0	F	maj	T	T	F
Backup to Master change syslog	Backup to Master syslog	Backup to Master syslog	Backup	N	IIPInterface	F	F	F	0	F	info	T	T	F
Master to Backup change syslog	Backup to Master syslog	Master to Backup syslog	Master	N	IIPInterface	F	F	F	0	F	info	T	T	F

Table 17-7 Cisco ASR 9000 Syslog Registry Parameters (continued)

Short Description	Event Type	Event Subtype	Subtype Value	Expedites Polling	Event Source (IMO Name)	Activate	Correlate	Is Correlation Allowed	Weight	Auto Clear	Severity	Is Ticketable	Auto Remove	Flapping
BFD rate limit high warning syslog	bfd rate limit high warning syslog	bfd rate limit high warning syslog	N/A	N	IBfdService	F	F	F	0	T	wrn	F	T	F
RIP authentication failed syslog	rip authenticatio n failed syslog	rip authentica tion failed syslog	N/A	N	IIPInterface	F	F	F	0	T	min	F	T	F
RIP configuration error syslog	rip configuration error syslog	rip configurat ion error syslog	N/A	N	IManagedEl ement	F	F	F	0	T	min	F	T	F
RIP out of memory event syslog	rip out of memory event syslog	rip out of memory event syslog	N/A	N	IManagedEl ement	F	F	F	0	F	info	F	T	F
routing ISIS neighbor down syslog	routing isis neighbor down syslog	routing isis neighbor down syslog	down	N	IPhysicalLa yer	F	T	F	0	F	maj	F	T	F
routing ISIS neighbor up syslog	routing isis neighbor down syslog	routing isis neighbor up syslog	up	N	IPhysicalLa yer	F	F	F	0	F	clr	F	T	F
Ethernet OAM Remote loopback session stopped Syslog	Ethernet OAM loopback session stopped	Ethernet OAM Remote loopback session stopped	remote,st opped	oam	IPhysicalLa yer	F	F	F	0	T	min	F	T	F
Ethernet OAM Remote loopback session started Syslog	Ethernet OAM loopback session stopped	Ethernet OAM Remote loopback session started	remote,sta rted	oam	IPhysicalLa yer	F	F	F	0	T	min	F	T	F

Table 17-7 Cisco ASR 9000 Syslog Registry Parameters (continued)

Short Description	Event Type	Event Subtype	Subtype Value	Expedites Polling	Event Source (IMO Name)	Activate	Correlate	Is Correlation Allowed	Weight	Auto Clear	Severity	Is Ticketable	Auto Remove	Flapping
Ethernet OAM Local loopback session stopped Syslog	Ethernet OAM loopback session stopped	Ethernet OAM Local loopback session stopped	local,stopped	oam	IPhysicalLayer	F	F	F	0	T	min	F	T	F
Ethernet OAM Local loopback session started Syslog	Ethernet OAM loopback session stopped	Ethernet OAM Local loopback session started	local,started	oam	IPhysicalLayer	F	F	F	0	T	min	F	T	F
Ethernet OAM Session down Syslog	Ethernet OAM Session down Syslog	Ethernet OAM Session down Syslog	DOWN	oam	IPhysicalLayer	F	F	F	0	F	info	F	T	F
Ethernet OAM Session up Syslog	Ethernet OAM Session down Syslog	Ethernet OAM Session up Syslog	UP	oam	IPhysicalLayer	F	F	F	0	F	info	F	T	F
CFM cc error syslog	CFM cc error syslog	CFM cc error syslog	errors set		ICFMService	F	F	F	0	F	info	F	T	F
CFM cc error cleared syslog	CFM cc error syslog	CFM cc error cleared syslog	errors cleared		ICFMService	F	F	F	0	F	clr	F	T	F
Mac Table resync completed syslog	Mac Table resync completed syslog	Mac Table resync completed syslog	NA	Expediate-ce-ios xr-39-bridge-table-telnet	IModule	F	F	F	0	T	info	F	T	F

Cisco ASR 1000 Registry Parameters

Table 17-8 lists the associated event types, event subtypes, and Prime Network registry parameters for the Cisco ASR 1000 syslogs shown in Table 17-3.

Table 17-8 Cisco ASR 1000 Registry Parameters

Short Description	Event Type	Event Subtype	Subtype Value	Expedites Polling	Event Source (IMO Name)	Activate Flow	Correlate	Is Correlation Allowed	Weight	Auto Clear	Severity	Is Ticketable	Auto Remove	Flapping
Crypto session status up syslog	crypto tunnel updown syslog	crypto tunnel up syslog	Up	N	IIPSecTunnel	F	F	F	0	F	clr	T	T	F
Crypto session status down syslog	crypto tunnel updown syslog	crypto tunnel down syslog	Down	N	IIPSecTunnel	F	F	F	0	F	min	T	T	F

Cisco IOS Syslog Registry Parameters

Table 17-9 lists the associated event types, event subtypes, and Prime Network registry parameters for the Cisco IOS syslogs shown in Table 17-3.

Table 17-9 Cisco IOS Registry Parameters

Short Description	Event Type	Event Subtype	Subtype Value	Expedites Polling	Event Source (IMO Name)	Activate Flow	Correlate	Is Correlation Allowed	Weight	Auto Clear	Severity	Is Ticketable	Auto Remove	Flapping
Link down syslog	link down syslog	link down syslog		mtop-mlppp bundle-status-telnet/ mtop-ima-group-state-telnet/mtop-cem-group-status/bun \dle-status/ mpls traffic engineering tunnel information/ip interface oper status	IIPInterface	F	T	F	0	T	maj	F	T	T
Link up syslog	link down syslog	link up syslog		mtop-mlppp bundle-status-telnet/ mtop-ima-group-state-telnet/mtop-cem-group-status/bun \dle-status/ mpls traffic engineering tunnel information/ip interface oper status	IIPInterface	F	F	F	0	F	clr	F	T	T
FR DLCI down syslog	dlci change syslog	dlci down		N	IPhysicalLayer	T	T	F	0	T	maj	F	T	F

Table 17-9 Cisco IOS Registry Parameters (continued)

Short Description	Event Type	Event Subtype	Subtype Value	Expedites Polling	Event Source (IMO Name)	Activate Flow	Correlate	Is Correlation Allowed	Weight	Auto Clear	Severity	Is Ticketable	Auto Remove	Flapping
FR DLCI up syslog	dlci change syslog	dlci up		N	IPhysicalLayer	F	F	F	0	F	clr	F	T	F
HSRP group change syslog	hsrp syslog	hsrp group change syslog		hsrp	IIPInterface	F	T	F	0	F	info	F	T	F
HSRP group restored syslog	hsrp syslog	hsrp group restored syslog		hsrp	IIPInterface	F	F	F	0	F	clr	F	T	F
SNMP message has not properly authenticated	snmp 5 snmp auth fail syslog	snmp 5 snmp auth fail syslog		N	IManagedElement	F	T	F	0	T	min	F	T	F
Memory allocation is not available	memory allocation syslog	memory allocation syslog		N	IManagedElement	F	T	F	0	T	min	F	T	F
process ran too long	process ran too long syslog	process ran too long syslog		N	IManagedElement	F	T	F	0	T	min	F	T	F
registered timer is expired	registered timer expired syslog	registered timer expired syslog		N	IManagedElement	F	T	F	0	F	min	F	T	F
EIGRP router query to neighbors timeouted syslog	EIGRP router query to neighbors timeouted syslog	EIGRP router query to neighbors timeouted syslog		N	IManagedElement	T	T	F	0	F	info	F	T	F
Ethernet cable is not connected	ethernet cable is not connected syslog	ethernet cable is not connected syslog		N	IManagedElement	F	T	F	0	T	min	F	T	F
frame with an invalid control code	frmr report syslog	frmr report syslog		N	IPhysicalLayer	F	T	F	0	T	min	F	T	F

Table 17-9 Cisco IOS Registry Parameters (continued)

Short Description	Event Type	Event Subtype	Subtype Value	Expedites Polling	Event Source (IMO Name)	Activate Flow	Correlate	Is Correlation Allowed	Weight	Auto Clear	Severity	Is Ticketable	Auto Remove	Flapping
Interface changed to non trunk	dtp 5 non port trunk syslog	dtp 5 non port trunk syslog		N	IPhysicalLayer	F	T	F	0	T	min	F	T	F
Line down syslog	line down syslog	line down syslog		basetech-lldp-neighbors-snmp/basetech-cdp-neighbors-snmp/mtop-mlpppbundle-status-telnet/mtop-ima-group-state-telnet/mtop-cem-group-status/bundle-status/mpls trafficengineering tunnel information/port-status/ip interface oper status	IIPInterface	F	T	F	0	T	maj	F	T	T

Table 17-9 Cisco IOS Registry Parameters (continued)

Short Description	Event Type	Event Subtype	Subtype Value	Expedites Polling	Event Source (IMO Name)	Activate Flow	Correlate	Is Correlation Allowed	Weight	Auto Clear	Severity	Is Ticketable	Auto Remove	Flapping
Line up syslog	line down syslog	line up syslog		basetech-lldp-neighbors-snmp/basetech-cdp-neighbors-snmp/mtop-mlpppbundle-status-telnet/mtop-ima-group-state-telnet/mtop-cem-group-status/bundle-status/mpls trafficengineering tunnel information/port-status/ip interface oper status	IIPInterface	F	F	F	0	F	clr	F	T	T
Cannot send incremental SAP update to peer	ipx 3 bad igrp sap syslog	ipx 3 bad igrp sap syslog		N	IPhysicalLayer	F	T	F	0	T	min	F	T	F
An Ethernet cable is broken or unterminated	lance 5 coll syslog	lance 5 coll syslog		N	IManagedElement	F	T	F	0	F	info	F	T	F
An Ethernet transceiver is unplugged or defective	lance 5 late coll syslog	lance 5 late coll syslog		N	IManagedElement	F	T	F	0	T	min	F	T	F
Device configuration changed	sys 5 config i syslog	sys 5 config i syslog		N	IManagedElement	F	F	F	0	F	info	F	T	F
AppleTalk invalid network number	at 6 node wrong syslog	at 6 node wrong syslog		N	IManagedElement	F	T	F	0	T	min	F	T	F

Table 17-9 Cisco IOS Registry Parameters (continued)

Short Description	Event Type	Event Subtype	Subtype Value	Expedites Polling	Event Source (IMO Name)	Activate Flow	Correlate	Is Correlation Allowed	Weight	Auto Clear	Severity	Is Ticketable	Auto Remove	Flapping
security port shut down	security 1 port shut down syslog	security 1 port shut down syslog		N	IPhysicalLayer	F	T	F	0	T	min	F	T	F
BPDU spanning-tree portfast enabled	span tree 2 rx port fast syslog	span tree 2 rx port fast syslog		N	IPhysicalLayer	F	T	F	0	T	min	F	T	F
Fault has been detected in a fiber Ethernet port connection	udld 3 disable syslog	udld 3 disable syslog		N	IPhysicalLayer	F	T	F	0	T	min	F	T	F
Unidirectional link detected	udld 3 disable fail syslog	udld 3 disable fail syslog		N	IPhysicalLayer	F	T	F	0	T	min	F	T	F
Fault has been detected in a fiber Ethernet connection	udld 4 one way path syslog	udld 4 one way path syslog		N	IPhysicalLayer	F	T	F	0	T	min	F	T	F
OSPF neighbor down syslog	ospf neighbor syslog	ospf neighbor down syslog		bfd session,ospf-interfaces,ospf-neighbors	Ospf process key	T	T	F	0	T	maj	F	T	F
OSPF neighbor up syslog	ospf neighbor syslog	ospf neighbor up syslog		bfd session,ospf-interfaces,ospf-neighbors	Ospf process key	F	F	F	0	F	clr	F	T	F
No BPDUs were received on port	span tree 2 loop guard block syslog	span tree 2 loop guard block syslog		N	IPhysicalLayer	F	T	F	0	T	min	F	T	F
BPDUs were received on port	span tree 2 loop guard un block syslog	span tree 2 loop guard un block syslog		N	IPhysicalLayer	F	T	F	0	T	min	F	T	F

Table 17-9 Cisco IOS Registry Parameters (continued)

Short Description	Event Type	Event Subtype	Subtype Value	Expedites Polling	Event Source (IMO Name)	Activate Flow	Correlate	Is Correlation Allowed	Weight	Auto Clear	Severity	Is Ticketable	Auto Remove	Flapping
Ethernet is seeing multiple collisions	amdp2 fe 5 coll syslog	amdp2 fe 5 coll syslog		N	IPhysicalLayer	F	T	F	0	F	info	F	T	F
Fast Ethernet packet has been dropped	dec 21140-5 coll syslog	dec 21140-5 coll syslog		N	IManagedElement	F	T	F	0	T	min	F	T	F
An Ethernet cable is broken	ilacc 5 coll syslog	ilacc 5 coll syslog		N	IManagedElement	F	T	F	0	T	min	F	T	F
pquicc 5 coll syslog: An Ethernet cable is broken	pquicc 5 coll syslog	pquicc 5 coll syslog		N	IManagedElement	F	T	F	0	T	min	F	T	F
pquicc ether 5 coll syslog: An Ethernet cable is broken	pquicc ether 5 coll syslog	pquicc ether 5 coll syslog		N	IManagedElement	F	F	F	0	T	min	F	T	F
Ethernet is detecting multiple collisions	pquicc fe 5 coll syslog	pquicc fe 5 coll syslog		N	IPhysicalLayer	F	T	F	0	T	min	F	T	F
quicc ether 5 coll syslog: An Ethernet cable is broken	quicc ether 5 coll syslog	quicc ether 5 coll syslog		N	IManagedElement	F	T	F	0	T	min	F	T	F
Late collisions have occurred	amdp2 fe 5 latecoll syslog	amdp2 fe 5 latecoll syslog		N	IPhysicalLayer	F	T	F	0	T	min	F	T	F
IS-IS neighbor down syslog	is is neighbor down syslog	is is neighbor down syslog		N	IPhysicalLayer	F	T	F	0	F	maj	F	T	F
IS-IS neighbor up syslog	is is neighbor down syslog	is is neighbor up syslog		N	IPhysicalLayer	F	F	F	0	F	clr	F	T	F

Table 17-9 Cisco IOS Registry Parameters (continued)

Short Description	Event Type	Event Subtype	Subtype Value	Expedites Polling	Event Source (IMO Name)	Activate Flow	Correlate	Is Correlation Allowed	Weight	Auto Clear	Severity	Is Ticketable	Auto Remove	Flapping
Late collisions have occurred	dec 21140-5 late coll syslog	dec 21140-5 late coll syslog		N	IPhysicalLayer	F	T	F	0	T	min	F	T	F
ilacc 5 late coll syslog: Late collisions have occurred	ilacc 5 late coll syslog	ilacc 5 late coll syslog		N	IManagedElement	F	F	F	0	T	min	F	T	F
pquicc 5 late coll syslog: Late collisions have occurred	pquicc 5 late coll syslog	pquicc 5 late coll syslog		N	IManagedElement	F	F	F	0	T	min	F	T	F
A new network may not have been engineered properly	pquicc ether 5 late coll syslog	pquicc ether 5 late coll syslog		N	IManagedElement	F	T	F	0	T	min	F	T	F
pquicc fe 5 late coll syslog: Late collisions have occurred	pquicc fe 5 late coll syslog	pquicc fe 5 late coll syslog		N	IPhysicalLayer	F	T	F	0	T	min	F	T	F
quicc ether 5 late coll syslog: Late collisions have occurred	quicc ether 5 late coll syslog	quicc ether 5 late coll syslog		N	IManagedElement	F	F	F	0	T	min	F	T	F
Link trap down has occurred	snmp 5 link trap syslog	snmp 5 link trap down syslog		N	IPhysicalLayer	F	T	F	0	T	min	F	T	F
Link trap up has occurred	snmp 5 link trap syslog	snmp 5 link trap up syslog		N	IPhysicalLayer	F	F	F	0	F	clr	F	T	F

Table 17-9 Cisco IOS Registry Parameters (continued)

Short Description	Event Type	Event Subtype	Subtype Value	Expedites Polling	Event Source (IMO Name)	Activate Flow	Correlate	Is Correlation Allowed	Weight	Auto Clear	Severity	Is Ticketable	Auto Remove	Flapping
configured port changed state from learning to forwarding	snmp 5 top trap syslog	snmp 5 top trap syslog		N	IManagedElement	F	F	F	0	T	min	F	T	F
DUAL 5 neighbor down syslog	dual5 neighbor change	dual5 neighbor down		N	IPhysicalLayer	T	T	F	0	F	maj	F	T	F
DUAL 5 neighbor up syslog	dual5 neighbor change	dual5 neighbor up		N	IPhysicalLayer	F	F	F	0	F	clr	F	T	F
Link down syslog	link down syslog	link down syslog		ce-qinq-status-telnet/mtop-mlpppbundle-status-telnet/mtop-ima-group-state-telnet/mtop-cem-group-status/bundle-status/mpls traffic engineering tunnel information/ipinterface oper status	IIPInterface	F	T	F	0	T	maj	F	T	T

Table 17-9 Cisco IOS Registry Parameters (continued)

Short Description	Event Type	Event Subtype	Subtype Value	Expedites Polling	Event Source (IMO Name)	Activate Flow	Correlate	Is Correlation Allowed	Weight	Auto Clear	Severity	Is Ticketable	Auto Remove	Flapping
Link up syslog	link down syslog	link up syslog		ce-qinq-status-telnet/mtop-mlpppbundle-status-telnet/mtop-ima-group-state-telnet/mtop-cem-group-status/bundle-status/mpls traffic engineering tunnel information/ipinterface oper status	IIPInterface	F	F	F	0	F	clr	F	T	T
BGP neighbor down syslog	bgp neighbor down syslog	bgp neighbor down syslog		bgp neighbours	IMpBgpOid	F	T	F	0	T	maj	F	T	F
BGP neighbor up syslog	bgp neighbor down syslog	bgp neighbor up syslog		bgp neighbours	IMpBgpOid	F	F	F	0	F	clr	F	T	F
BGP neighbor down syslog	bgp neighbor down syslog	bgp neighbor down syslog		bgp neighbours	IMpBgpOid	F	T	F	0	T	maj	F	T	F
BGP neighbor up syslog	bgp neighbor down syslog	bgp neighbor up syslog		bgp neighbours	IMpBgpOid	F	F	F	0	F	clr	F	T	F
card in syslog	card out syslog	card in syslog		physical-command	IModule	F	F	F	0	F	clr	F	T	T
card out syslog	card out syslog	card out syslog		physical-command	IModule	F	T	F	0	T	maj	F	T	T
oir sp 3 power cycle syslog	oir sp 3 power cycle	oir sp 3 power cycle		N	IModule	F	F	F	0	F	info	F	T	F

Table 17-9 Cisco IOS Registry Parameters (continued)

Short Description	Event Type	Event Subtype	Subtype Value	Expedites Polling	Event Source (IMO Name)	Activate Flow	Correlate	Is Correlation Allowed	Weight	Auto Clear	Severity	Is Ticketable	Auto Remove	Flapping
Reloading device syslog	reloading device syslog	reloading device syslog		N	IManagedElement	F	F	T	200000	F	info	T	T	T
System restart	system restart syslog	system restart syslog		physical-command	IManagedElement	F	F	F	0	F	info	F	T	T
Interface changed to non trunk	dtp 5 non port trunk syslog	dtp 5 non port trunk syslog		N	IPhysicalLayer	F	T	F	0	T	min	F	T	F
Interface changed to trunk	dtp 5 non port trunk syslog	dtp 5 port trunk syslog		N	IPhysicalLayer	F	F	F	0	F	clr	F	T	F
ISDN connect syslog	isdn 6 connect syslog	isdn 6 connect syslog		N	IPhysicalLayer	F	T	F	0	T	maj	F	T	F
ISDN disconnect syslog	isdn 6 connect syslog	isdn 6 disconnect syslog		N	IPhysicalLayer	F	F	F	0	F	clr	F	T	F
ISDN connect syslog	isdn 6 connect syslog	isdn 6 connect syslog		N	IPhysicalLayer	F	T	F	0	T	maj	F	T	F
ISDN disconnect syslog	isdn 6 connect syslog	isdn 6 disconnect syslog		N	IPhysicalLayer	F	F	F	0	F	clr	F	T	F
Duplex mismatch discovered	duplex mismatch	duplex mismatch		N	IPhysicalLayer	F	T	F	0	F	info	F	T	F
ISDN connect syslog	isdn 6 connect syslog	isdn 6 connect syslog		N	IPhysicalLayer	F	T	F	0	T	maj	F	T	F
ISDN disconnect syslog	isdn 6 connect syslog	isdn 6 disconnect syslog		N	IPhysicalLayer	F	F	F	0	F	clr	F	T	F
ISDN connect syslog	isdn 6 connect syslog	isdn 6 connect syslog		N	IPhysicalLayer	F	T	F	0	T	maj	F	T	F
ISDN disconnect syslog	isdn 6 connect syslog	isdn 6 disconnect syslog		N	IPhysicalLayer	F	F	F	0	F	clr	F	T	F

Table 17-9 Cisco IOS Registry Parameters (continued)

Short Description	Event Type	Event Subtype	Subtype Value	Expedites Polling	Event Source (IMO Name)	Activate Flow	Correlate	Is Correlation Allowed	Weight	Auto Clear	Severity	Is Ticketable	Auto Remove	Flapping
TDP neighbor down syslog	tdp neighbor down syslog	tdp neighbor down syslog		label switching table	ILseOid	F	T	F	0	T	maj	F	T	F
TDP neighbor up syslog	tdp neighbor down syslog	tdp neighbor up syslog		label switching table	ILseOid	F	F	F	0	T	clr	F	T	F
LDP neighbor down syslog	ldp neighbor down syslog	ldp neighbor down syslog		mpls interfaces	ILseOid	F	T	F	0	T	maj	F	T	F
LDP neighbor up syslog	ldp neighbor down syslog	ldp neighbor up syslog		mpls interfaces	ILseOid	F	F	F	0	F	clr	F	T	F
MPSL-TE tunnel reoptimized/rerouted syslog	mpls te tunnel reoptimized syslog	mpls te tunnel reoptimized syslog		N	IMplsTETunnel	T	T	F	0	F	info	T	T	F
MPLS TE tunnel down syslog	mpls te tunnel down syslog	mpls te tunnel down syslog		mpls traffic engineering tunnel information	IMplsTETunnel	F	T	F	0	T	maj	F	T	F
MPLS TE tunnel up syslog	mpls te tunnel down syslog	mpls te tunnel up syslog		mpls traffic engineering tunnel information	IMplsTETunnel	F	F	F	0	F	clr	F	T	F
MPLS TE tunnel down syslog	mpls te tunnel down syslog	mpls te tunnel down syslog		mpls traffic engineering tunnel information	IMplsTETunnel	F	T	F	0	T	maj	F	T	F

Table 17-9 Cisco IOS Registry Parameters (continued)

Short Description	Event Type	Event Subtype	Subtype Value	Expedites Polling	Event Source (IMO Name)	Activate Flow	Correlate	Is Correlation Allowed	Weight	Auto Clear	Severity	Is Ticketable	Auto Remove	Flapping
MPLS TE tunnel up syslog	mpls te tunnel down syslog	mpls te tunnel up syslog		mpls traffic engineering tunnel information	IMplsTETunnel	F	F	F	0	F	clr	F	T	F
A power supply is not working or has not been turned on	environment monitoring 2 supply syslog	environment monitoring 2 supply		N	IManagedElement	F	F	F	0	F	info	F	T	F
System restart	system sp restart syslog	system sp restart syslog		N	IManagedElement	F	F	F	0	F	info	F	T	F
Aggressive Mode Failure Detected	udld sp 4 disable syslog	udld sp 4 disable syslog		N	IPhysicalLayer	F	T	F	0	F	info	F	T	F
fabric sp 5 clear block down syslog	fabric sp 5 clear block off syslog	fabric sp 5 clear block off syslog		N	IPhysicalLayer	F	T	F	0	F	info	F	T	F
fabric sp 5 clear block up syslog	fabric sp 5 clear block off syslog	fabric sp 5 clear block on syslog		N	IPhysicalLayer	F	F	F	0	F	info	F	T	F
c6kenv sp 4 fan tray fail syslog	c6kenv sp 4 fan tray fail	c6kenv sp 4 fan tray fail		N	IManagedElement	F	F	F	0	F	info	F	T	F
pfredun sp 4 bootstring invalid syslog	pfredun sp 4 bootstring invalid	pfredun sp 4 bootstring invalid		N	IManagedElement	F	F	F	0	F	info	F	T	F
Power supply failed syslog	power supply failure syslog	power supply failed syslog		N	IPhysicalLayer	F	F	F	0	T	maj	F	T	F
Power supply okay syslog	power supply failure syslog	power supply okay syslog		N	IPhysicalLayer	F	F	F	0	F	clr	F	T	F

Table 17-9 Cisco IOS Registry Parameters (continued)

Short Description	Event Type	Event Subtype	Subtype Value	Expedites Polling	Event Source (IMO Name)	Activate Flow	Correlate	Is Correlation Allowed	Weight	Auto Clear	Severity	Is Ticketable	Auto Remove	Flapping
pm sp stdby 4 err disable syslog	pm sp stdby 4 err disable	pm sp stdby 4 err disable		N	IPhysicalLayer	F	F	F	0	F	info	F	T	F
HSRP group change syslog	hsrp syslog	hsrp group change syslog		hsrp	IPhysicalLayer	F	T	F	0	F	info	F	T	F
HSRP group restored syslog	hsrp syslog	hsrp group restored syslog		hsrp	IPhysicalLayer	F	F	F	0	F	clr	F	T	F
BGP notification syslog	bgp notification syslog	bgp notification syslog		N	IPhysicalLayer	T	T	F	0	F	info	F	T	F
new ethernet channel interface for VSL connection	VSL-connection-new-interface-syslog	VSL connection new interface		N	IManagedElement	F	F	F	110000	F	info	T	T	F
VSL link up syslog	VSL-link-state-change-syslog	VSL link up syslog		N	IManagedElement	F	F	F	110000	F	info	T	T	F
VSL link down syslog	VSL-link-state-change-syslog	VSL link down syslog		N	IManagedElement	F	F	F	110000	F	info	T	T	F
VSL link up syslog: active switch is #1	VSL-link-state-change-syslog	VSL link up and switch 1 is active		N	IShelf	F	F	F	110000	F	info	T	T	F
VSL link up syslog: active switch is #2	VSL-link-state-change-syslog	VSL link up and switch 2 is active		N	IShelf	F	F	F	110000	F	info	T	T	F
role mismatch resolved syslog, sent from active switch #1	VSL-role-mismatch-resolved-syslog	VSL role mismatch resolved sent from active switch 1		N	IShelf	F	F	F	110000	F	info	T	T	F

Table 17-9 Cisco IOS Registry Parameters (continued)

Short Description	Event Type	Event Subtype	Subtype Value	Expedites Polling	Event Source (IMO Name)	Activate Flow	Correlate	Is Correlation Allowed	Weight	Auto Clear	Severity	Is Ticketable	Auto Remove	Flapping
role mismatch resolved syslog, sent from active switch #2	VSL-role-mismatch-resolved-syslog	VSL role mismatch resolved sent from active switch 2		N	IShelf	F	F	F	110000	F	info	T	T	F
env sp 4 fan tray fail syslog	env sp 4 fan tray fail	env sp 4 fan tray fail		N	IManagedElement	F	F	F	0	F	info	F	T	F
pwr sp 2 power supply fail syslog	pwr sp 2 power supply fail	pwr sp 2 power supply fail		N	IManagedElement	F	F	F	0	F	info	T	T	F
BGP neighbor down syslog	bgp neighbor down syslog	bgp neighbor down syslog		bgp neighbours, BFD	IMpBgpOid	F	T	F	0	T	maj	F	T	F
BGP neighbor up syslog	bgp neighbor down syslog	bgp neighbor up syslog		bgp neighbours, BFD	IMpBgpOid	F	F	F	0	F	clr	F	T	F
VRRP State Changed syslog	vrrp state changed syslog	vrrp state changed syslog		N	IManagedElement	F	F	F	0	F	info	T	T	F
Ima Link Status Change Down Syslog	Ima Link Status Change Down Syslog	Ima Link Status Change Down Syslog			IPhysicalLayer	F	T	F	0	T	maj	F	T	T
Ima Link Status Change Up Syslog	Ima Link Status Change Down Syslog	Ima Link Status Change Up Syslog			IPhysicalLayer	F	F	F	0	T	clr	F	T	T
IMA Active Link Change Syslog	IMA Active Link Change Syslog	IMA Active Link Change Syslog		mtop-ima-group-state,port-status	IMAGroupOid	F	F	F	0	F	info	F	T	F
Native VLAN mismatch discovered	native VLAN mismatch	native VLAN mismatch		N	IPhysicalLayer	F	T	F	0	F	info	F	T	F

Table 17-9 Cisco IOS Registry Parameters (continued)

Short Description	Event Type	Event Subtype	Subtype Value	Expedites Polling	Event Source (IMO Name)	Activate Flow	Correlate	Is Correlation Allowed	Weight	Auto Clear	Severity	Is Ticketable	Auto Remove	Flapping
Clock status change syslog	clock status change syslog	clock status change syslog		N	defaultClockDC	F	T	F	0	F	info	F	T	F
Clock source change syslog	clock source change syslog	clock source change syslog		N	defaultClockDC	F	T	F	0	F	info	F	T	F
pseudo wire tunnel down syslog	pseudo wire tunnel syslog	pseudo wire tunnel down syslog		ce-pw-tunnel-status-telnet	PTPLayer2MplsTunnel	F	T	F	0	T	min	F	T	T
pseudo wire tunnel up syslog	pseudo wire tunnel syslog	pseudo wire tunnel up syslog		ce-pw-tunnel-status-telnet	PTPLayer2MplsTunnel	F	F	F	0	F	clr	T	T	T
EFP service error disabled syslog	efp service error disabled syslog	efp service error disabled syslog		EFP status	IEFP	F	T	F	0	F	info	F	T	F
EFP down syslog	efp down syslog	efp down syslog		EFP status	IEFP	F	T	F	0	T	maj	F	T	F
EFP up syslog	efp down syslog	efp up syslog		EFP status	IEFP	F	T	F	0	F	clr	F	T	F
REP link not operational syslog	REP link operational status change	REP link not operational		Rep status	IREPService	F	T	F	0	T	min	F	T	F
REP link operational syslog	REP link operational status change	REP link operational		Rep status	IREPService	F	F	F	0	F	clr	F	T	F
OSPFv3 neighbor down syslog	ospfv3 neighbor syslog	ospfv3 neighbor down syslog	Down / DOWN	bfd session,ospf-interfaces,ospf-neighbors	Ospf process key	T	T	F	0	T	maj	F	T	F

Table 17-9 Cisco IOS Registry Parameters (continued)

Short Description	Event Type	Event Subtype	Subtype Value	Expedites Polling	Event Source (IMO Name)	Activate Flow	Correlate	Is Correlation Allowed	Weight	Auto Clear	Severity	Is Ticketable	Auto Remove	Flapping
OSPFv3 neighbor up syslog	ospfv3 neighbor syslog	ospfv3 neighbor up syslog	Up / FULL	bfd session,ospf-interfaces,ospf-neighbors	Ospf process key	F	F	F	0	T	clr	F	T	F
CFM enter AIS defect syslog	CFM enter AIS defect syslog	CFM enter AIS defect syslog	ENTER	N	ICfmServiceOid	F	T	F	0	F	info	F	T	F
CFM exit AIS defect syslog	CFM enter AIS defect syslog	CFM exit AIS defect syslog	EXIT	N	ICfmServiceOid	F	T	F	0	F	info	F	T	F
CFM enter AIS defect syslog	CFM enter AIS defect syslog	CFM enter AIS defect syslog	ENTER	N	ICfmServiceOid	F	T	F	0	F	info	F	T	F
CFM exit AIS defect syslog	CFM enter AIS defect syslog	CFM exit AIS defect syslog	EXIT	N	ICfmServiceOid	F	T	F	0	F	info	F	T	F
CFM interface enter AIS defect syslog	CFM interface enter AIS syslog	CFM interface enter AIS syslog	ENTER	N	ICfmServiceOid	F	T	F	0	F	info	F	T	F
CFM interface exit AIS defect syslog	CFM interface exit AIS syslog	CFM interface exit AIS syslog	EXIT	N	ICfmServiceOid	F	T	F	0	F	info	F	T	F
CFM interface enter AIS defect syslog	CFM interface enter AIS syslog	CFM interface enter AIS syslog	ENTER	N	ICfmServiceOid	F	T	F	0	F	info	F	T	F
CFM interface exit AIS defect syslog	CFM interface exit AIS syslog	CFM interface exit AIS syslog	EXIT	N	ICfmServiceOid	F	T	F	0	F	info	F	T	F
CFM enter LCK defect syslog	CFM enter LCK defect syslog	CFM enter LCK defect syslog	ENTER	N	ICfmServiceOid	F	T	F	0	F	info	F	T	F

Table 17-9 Cisco IOS Registry Parameters (continued)

Short Description	Event Type	Event Subtype	Subtype Value	Expedites Polling	Event Source (IMO Name)	Activate Flow	Correlate	Is Correlation Allowed	Weight	Auto Clear	Severity	Is Ticketable	Auto Remove	Flapping
CFM exit LCK defect syslog	CFM enter LCK defect syslog	CFM exit LCK defect syslog	EXIT	N	ICfmServiceOid	F	T	F	0	F	info	F	T	F
CFM interface enter LCK syslog	CFM interface enter LCK defect syslog	CFM interface enter LCK defect syslog	ENTER	N	ICfmServiceOid	F	T	F	0	F	info	F	T	F
CFM interface exit LCK syslog	CFM interface enter LCK defect syslog	CFM interface exit LCK defect syslog	EXIT	N	ICfmServiceOid	F	T	F	0	F	info	F	T	F
CFM Mep Down syslog	Mep Down syslog	Mep Down syslog	DOWN	N	ICfmMaintenanceAssociationOid	F	T	F	0	T	minor	F	T	F
CFM Mep Up syslog	Mep Down syslog	Mep Up syslog	UP	N	ICfmMaintenanceAssociationOid	F	F	F	0	F	clr	F	T	F
CFM Mep Down syslog	Mep Down syslog	Mep Down syslog	DOWN	N	ICfmMaintenanceAssociationOid	F	T	F	0	T	minor	F	T	F
CFM Mep Up syslog	Mep Down syslog	Mep Up syslog	UP	N	ICfmMaintenanceAssociationOid	F	F	F	0	F	clr	F	T	F
CFM Mep Down syslog	Mep Down syslog	Mep Down syslog	DOWN	N	ICfmMaintenanceAssociationOid	F	T	F	0	T	minor	F	T	F
CFM Mep Up syslog	Mep Down syslog	Mep Up syslog	UP	N	ICfmMaintenanceAssociationOid	F	F	F	0	F	clr	F	T	F
Timing over packet application down syslog	timing over packet application down syslog	timing over packet application down syslog	down	N	IManagedElement	F	F	F	0	F	min	T	T	T

Table 17-9 Cisco IOS Registry Parameters (continued)

Short Description	Event Type	Event Subtype	Subtype Value	Expedites Polling	Event Source (IMO Name)	Activate Flow	Correlate	Is Correlation Allowed	Weight	Auto Clear	Severity	Is Ticketable	Auto Remove	Flapping
Timing over packet application up syslog	timing over packet application down syslog	timing over packet application up syslog	up	N	IManagedElement	F	F	F	0	F	clr	F	T	T
HSRP group change syslog	hsrp syslog	hsrp group change syslog		hsrp	IPhysicalLayer	F	T	F	0	F	info	F	T	F
HSRP group restored syslog	hsrp syslog	hsrp group restored syslog		hsrp	IPhysicalLayer	F	F	F	0	F	clr	F	T	F
Layer2 G709 alarm syslog	layer2 G709 alarm syslog	layer2 G709 alarm syslog	declared	N	DWDM Oid	F	F	F	0	T	wrn	F	T	F
Layer2 G709 clear syslog	layer2 G709 alarm syslog	layer2 G709 clear syslog	cleared	N	DWDM Oid	F	F	F	0	F	clr	F	T	F
Ethernet OAM Loopback Error syslog	EOAM Loopback Error syslog	EOAM Loopback Error syslog		N	IPhysicalLayer	F	F	F	0	F	info	F	T	F
Ethernet OAM Link Monitor syslog		EOAM Link Monitor syslog		N	IPhysicalLayer	F	F	F	0	F	info	F	T	F
Ethernet OAM Link Monitor high threshold syslog	EOAM Link Monitor high threshold syslog	EOAM Link Monitor high threshold syslog		N	IPhysicalLayer	F	F	F	0	F	info	F	T	F
Ethernet OAM exited the session	Ethernet OAM Session Syslog	EOAM exit session	EXIT	N	IPhysicalLayer	F	F	F	0	F	info	F	T	F

Table 17-9 Cisco IOS Registry Parameters (continued)

Short Description	Event Type	Event Subtype	Subtype Value	Expedites Polling	Event Source (IMO Name)	Activate Flow	Correlate	Is Correlation Allowed	Weight	Auto Clear	Severity	Is Ticketable	Auto Remove	Flapping
Ethernet OAM entered the session	Ethernet OAM Session Syslog	EOAM enter session	ENTER	N	IPhysicalLayer	F	F	F	0	F	info	F	T	F
Ethernet OAM Link timeout Syslog	Ethernet OAM Link timeout Syslog	Ethernet OAM Link timeout Syslog		N	IPhysicalLayer	F	F	F	0	F	info	F	T	F
VRRP backup to master syslog	vrrp state changed syslog	vrrp backup to master syslog	Backup	N	IManagedElement	F	F	F	0	F	info	T	T	F
VRRP master to backup syslog	vrrp state changed syslog	vrrp master to backup syslog	Master	N	IManagedElement	F	F	F	0	F	info	T	T	F
ELMI Vlan configured syslog	ELMI Vlan not configured syslog	ELMI Vlan configured syslog	CONFIGURED	N	IPhysicalLayer	F	F	F	0	F	clr	F	T	F
ELMI Vlan not configured syslog	ELMI Vlan not configured syslog	ELMI Vlan not configured syslog	NOT_CONFIGURED	N	IPhysicalLayer	F	F	F	0	F	min	T	T	F
ELMI Vlan disabled syslog	ELMI Vlan disabled syslog	ELMI Vlan disabled syslog	DISABLE	N	IPhysicalLayer	F	F	F	0	F	min	T	T	F
ELMI Vlan enabled syslog	ELMI Vlan disabled syslog	ELMI Vlan enabled syslog	RECOVER	N	IPhysicalLayer	F	F	F	0	F	clr	F	T	F
EOAM RFI dying gasp syslog - admin shutdown on peer	EOAM rfi dying gasp failure syslog	admin shutdown on peer	remote client down	oam	IPhysicalLayer	F	T	F	0	T	min	F	T	F

Table 17-9 Cisco IOS Registry Parameters (continued)

Short Description	Event Type	Event Subtype	Subtype Value	Expedites Polling	Event Source (IMO Name)	Activate Flow	Correlate	Is Correlation Allowed	Weight	Auto Clear	Severity	Is Ticketable	Auto Remove	Flapping
EOAM RFI dying gasp syslog - no ethernet oam	EOAM rfi dying gasp failure syslog	no ethernet oam	remote client administratively turned off	oam	IPhysicalLayer	F	T	F	0	T	min	F	T	F
EOAM RFI dying gasp syslog - admin reload on peer	EOAM rfi dying gasp failure syslog	admin reload on peer	remote client reloaded	oam	IPhysicalLayer	F	T	F	0	T	min	F	T	F
EOAM RFI dying gasp syslog - no org specific TLV	EOAM rfi dying gasp failure syslog	no org specific TLV	dying gasp	oam	IPhysicalLayer	F	T	F	0	T	min	F	T	F
Eoam RFI dying gasp clear syslog	EOAM rfi dying gasp failure syslog	dying gasp clear syslog		oam	IPhysicalLayer	F	F	F	0	T	clr	F	T	F
EOAM RFI link fault syslog	EOAM rfi link fault syslog	EOAM rfi link fault syslog		oam	IPhysicalLayer	F	T	F	0	T	min	F	T	F
EOAM RFI link fault clear syslog	EOAM rfi link fault syslog	EOAM rfi link fault clear syslog		oam	IPhysicalLayer	F	F	F	0	T	clr	F	T	F
PM Error disable syslog	PM Error disable syslog	PM Error disable syslog		oam	IPhysicalLayer	F	T	F	0	T	maj	F	T	F
PM Error recover syslog	PM Error disable syslog	PM Error recover syslog		oam	IPhysicalLayer	F	F	F	0	T	clr	F	T	F
PM SP Error disable syslog	PM SP Error disable syslog	PM SP Error disable syslog		oam	IPhysicalLayer	F	T	F	0	T	maj	F	T	F

Table 17-9 Cisco IOS Registry Parameters (continued)

Short Description	Event Type	Event Subtype	Subtype Value	Expedites Polling	Event Source (IMO Name)	Activate Flow	Correlate	Is Correlation Allowed	Weight	Auto Clear	Severity	Is Ticketable	Auto Remove	Flapping
Eoam entered master loopback mode syslog	EOAM loopback syslog	Enter master loopback mode	entered ,master	oam	IPhysicalLayer	F	F	F	0	T	min	F	T	F
Eoam exited master loopback mode syslog	EOAM loopback syslog	Exit master loopback mode	exited, master	oam	IPhysicalLayer	F	F	F	0	T	min	F	T	F
Eoam entered slave loopback mode syslog	EOAM loopback syslog	Enter slave loopback mode	entered ,slave	oam	IPhysicalLayer	F	F	F	0	T	min	F	T	F
Eoam exited slave loopback mode syslog	EOAM loopback syslog	Exit slave loopback mode	exited,s lave	oam	IPhysicalLayer	F	F	F	0	T	min	F	T	F
Transceiver inserted syslog	transceive r removed syslog	transceiv er inserted syslog		physical-c ommand	IPortConnector	F	F	F	0	F	clr	T	T	F
Transceiver removed syslog	transceive r removed syslog	transceiv er removed syslog		physical-c ommand	IPortConnector	F	F	F	0	T	maj	T	T	F
card in syslog	card out syslog	card in syslog		physical-c ommand	IModule	F	F	F	0	F	clr	F	T	T
card out syslog	card out syslog	card out syslog		physical-c ommand	IModule	F	T	F	0	T	maj	F	T	T
MPLS-TE tunnel lsp up syslog	mpls te tunnel lsp down syslog	mpls te tunnel lsp up syslog	Up,UP, up	mpls traffic engineerin g tunnel informatio n	IMplsTETunnel	F	T	F	0	T	clr	F	T	F
MPLS-TE tunnel lsp down syslog	mpls te tunnel lsp down syslog	mpls te tunnel lsp down syslog	Down, DOWN ,down	mpls traffic engineerin g tunnel informatio n	IMplsTETunnel	F	T	F	0	T	maj	F	T	F

Table 17-9 Cisco IOS Registry Parameters (continued)

Short Description	Event Type	Event Subtype	Subtype Value	Expedites Polling	Event Source (IMO Name)	Activate Flow	Correlate	Is Correlation Allowed	Weight	Auto Clear	Severity	Is Ticketable	Auto Remove	Flapping
mLACP ICCP Version Incompatible syslog	mLACP ICCP Version Incompatible syslog	mLACP ICCP Version Incompatible syslog		N	IIccpRedundancy Container	F	F	F	0	T	info	F	T	F
mLACP duplicate node-id syslog	mLACP duplicate node-id syslog	mLACP duplicate node-id syslog		N	IIccpRedundancy Container	F	F	F	0	T	info	F	T	F
mLACP duplicate node-id syslog	mLACP duplicate node-id syslog	mLACP duplicate node-id syslog		N	IIccpRedundancy Container	F	F	F	0	T	info	F	T	F
mLACP invalid node-id syslog	mLACP invalid node-id syslog	mLACP invalid node-id syslog		N	IIccpRedundancy Container	F	F	F	0	T	info	F	T	F
mLACP Core isolation failure syslog	mLACP Core isolation failure syslog	mLACP Core isolation failure syslog	ISOLATION	iccp-redundancy-container	IIccpRedundancy Group	T	F	F	0	F	minor	T	T	F
mLACP Core isolation recover syslog	mLACP Core isolation failure syslog	mLACP Core isolation recover syslog	CONNECTED	iccp-redundancy-container	IIccpRedundancy Group	T	F	F	0	F	minor	T	T	F
mLACP Peer down syslog	mLACP Peer down syslog	mLACP Peer down syslog	DOWN	iccp-redundancy-container	IIccpRedundancy Group	F	F	F	0	F	minor	T	T	F
mLACP Peer up syslog	mLACP Peer down syslog	mLACP Peer up syslog	UP	iccp-redundancy-container	IIccpRedundancy Group	F	F	F	0	F	minor	T	T	F
mLACP Peer disconnect syslog	mLACP Peer disconnect syslog	mLACP Peer disconnect syslog	DISCONNECT	iccp-redundancy-container	IIccpRedundancy Group	F	F	F	0	F	minor	T	T	F

Table 17-9 Cisco IOS Registry Parameters (continued)

Short Description	Event Type	Event Subtype	Subtype Value	Expedites Polling	Event Source (IMO Name)	Activate Flow	Correlate	Is Correlation Allowed	Weight	Auto Clear	Severity	Is Ticketable	Auto Remove	Flapping
mLACP Peer connected syslog	mLACP Peer disconnect syslog	mLACP Peer connected syslo	CONNECT	iccp-redundancy-container	IIccpRedundancyGroup	F	F	F	0	F	minor	T	T	F
MPLS TP Tunnel up syslog	mpls tp tunnel down syslog	mpls tp tunnel up syslog	Up, up	Mpls tunnel ep status	IMPLSTPTunnelEP	F	F	F	0	F	clr	F	T	F
MPLS TP Tunnel down syslog	mpls tp tunnel down syslog	mpls tp tunnel down syslog	Down, down, Admin Down	Mpls tunnel ep status	IMPLSTPTunnelEP	F	F	F	0	T	min	F	T	F
MPLS TP Lsp down syslog	mpls tp lsp down syslog	mpls tp lsp down syslog	Down.down	mplstp-lsp entries-telnet	IMPLSTPGlobal	F	F	F	0	T	min	F	T	F
MPLS TP Lsp down syslog	mpls tp lsp down syslog	mpls tp lsp down syslog	Down.down	mplstp-lsp entries-telnet	IMPLSTPGlobal	F	F	F	0	T	min	F	T	F
MPLS TP Lsp Up syslog	mpls tp lsp down syslog	mpls tp lsp up syslog	Up, up	mplstp-lsp entries-telnet	IMPLSTPGlobal	F	F	F	0	F	clr	F	T	F
MPLS TP tunnel switched from working to protect	mpls tp tunnel switched syslog	mpls tp tunnel working to protect syslog	Working to protect	mplstp-lsp entries-telnet	IMPLSTPGlobal	F	F	F	0	F	info	F	T	F
MPLS TP tunnel switched from protect to working	mpls tp tunnel switched syslog	mpls tp tunnel protect to working syslog	Protect to working	mplstp-lsp entries-telnet	IMPLSTPGlobal	F	F	F	0	F	info	F	T	F
MPLS TP Lsp enter lockdown syslog	mpls tp lsp enter lockdown syslog	mpls tp lsp enter lockdown syslog	Entering	mplstp-lsp entries-telnet	IMPLSTPGlobal	F	F	F	0	T	min	F	T	F
MPLS TP Lsp exit lockdown syslog	mpls tp lsp enter lockdown syslog	mpls tp lsp exit lockdown syslog	Exiting	mplstp-lsp entries-telnet	IMPLSTPGlobal	F	F	F	0	F	clr	F	T	F

Table 17-9 Cisco IOS Registry Parameters (continued)

Short Description	Event Type	Event Subtype	Subtype Value	Expedites Polling	Event Source (IMO Name)	Activate Flow	Correlate	Is Correlation Allowed	Weight	Auto Clear	Severity	Is Ticketable	Auto Remove	Flapping
MPLS TP tunnel added syslog	mpls tp tunnel changed syslog	mpls tp tunnel added syslog	Added	mplstp-tunnelep-telnet	IMPLSTPGlobal	F	F	F	0	F	info	F	T	F
MPLS TP tunnel updated syslog	mpls tp tunnel changed syslog	mpls tp tunnel updated syslog	Updated	mplstp-tunnelep-telnet	IMPLSTPGlobal	F	F	F	0	F	info	F	T	F
MPLS TP tunnel deleted syslog	mpls tp tunnel changed syslog	mpls tp tunnel deleted syslog	Deleted	mplstp-tunnelep-telnet	IMPLSTPGlobal	F	F	F	0	F	info	F	T	F
MPLS TP lsp added syslog	mpls tp lsp changed	mpls tp lsp added syslog	Added	mplstp-lsp entries-telnet	IMPLSTPGlobal	F	F	F	0	F	info	F	T	F
MPLS TP lsp updated syslog	mpls tp lsp changed	mpls tp lsp updated syslog	Updated	mplstp-lsp entries-telnet	IMPLSTPGlobal	F	F	F	0	F	info	F	T	F
MPLS TP lsp deleted syslog	mpls tp lsp changed	mpls tp lsp deleted syslog	Deleted	mplstp-lsp entries-telnet	IMPLSTPGlobal	F	F	F	0	F	info	F	T	F
MPLS TP link added syslog	mpls tp link changed syslog	mpls tp link added syslog	Added	mplstp-tpenabled-link	IMPLSTPGlobal	F	F	F	0	F	info	F	T	F
MPLS TP link updated syslog	mpls tp link changed syslog	mpls tp link updated syslog	Updated	mplstp-tpenabled-link	IMPLSTPGlobal	F	F	F	0	F	info	F	T	F
MPLS TP link deleted syslog	mpls tp link changed syslog	mpls tp link deleted syslog	Deleted	mplstp-tpenabled-link	IMPLSTPGlobal	F	F	F	0	F	info	F	T	F
MPLS TP static label range changed syslog	mpls tp label range changed syslog	mpls tp static label range changed syslog	Static	mpls-label-range	ILse	F	F	F	0	F	info	F	T	F

Table 17-9 Cisco IOS Registry Parameters (continued)

Short Description	Event Type	Event Subtype	Subtype Value	Expedites Polling	Event Source (IMO Name)	Activate Flow	Correlate	Is Correlation Allowed	Weight	Auto Clear	Severity	Is Ticketable	Auto Remove	Flapping
MPLS TP dynamic label range changed syslog	mpls tp label range changed syslog	mpls tp dynamic label range changed syslog	dynamic	mpls-label-range	ILse	F	F	F	0	F	info	F	T	F
Fan module in syslog	fan out syslog	fan in syslog		physical-command	IModule	F	F	F	0	F	clr	F	T	T
Fan module out syslog	fan out syslog	fan out syslog		physical-command	IModule	F	T	F	0	T	maj	F	T	T
Power module in syslog	power out syslog	power in syslog		physical-command	IModule	F	F	F	0	F	clr	F	T	T
Power module out syslog	power out syslog	power out syslog		physical-command	IModule	F	T	F	0	T	maj	F	T	T

Cisco IOX Syslog Registry Parameters

Table 17-10 lists the associated event types, event subtypes, and Prime Network registry parameters for the Cisco IOX syslogs shown in Table 17-4.

Table 17-10 Cisco IOX Registry Parameters

Short Description	Event Type	Event Subtype	Subtype Value	Expedites Polling	Event Source (IMO Name)	Activate Flow	Correlate	Is Correlation Allowed	Weight	Auto Clear	Severity	Is Ticketable	Auto Remove	Flapping
Link down syslog	link down syslog	link down syslog	down / Down	ce-qinq-status-telnet/mtop-mlpppbundle-status-telnet/mtop-ima-group-state-telnet/mtop-cem-group-status/bundle-status/mpls traffic engineering tunnel information/ipinterface oper status	IIPInterface	F	T	F	0	T	maj	F	T	T
Link up syslog	link down syslog	link up syslog	up / Up	ce-qinq-status-telnet/mtop-mlpppbundle-status-telnet/mtop-ima-group-state-telnet/mtop-cem-group-status/bundle-status/mpls traffic engineering tunnel information/ipinterface oper status	IIPInterface	F	F	F	0	F	clr	F	T	T
Link down syslog	link down syslog	link down syslog	down / Down	ip interface oper status	IIPInterface	F	T	F	0	T	maj	F	T	T
Link up syslog	link down syslog	link up syslog	up / Up	mtop-mlpppbundle-status-telnet/mtop-ima-group-state-telnet/mtop-cem-group-status/bundle-status/mpls traffic engineering tunnel information/ip interface oper status	IIPInterface	F	F	F	0	F	clr	F	T	T
Line down syslog	line down syslog	line down syslog	down / Down	mtop-mlpppbundle-status-telnet/mtop-ima-group-state-telnet/mpls traffic engineering tunnel information / port-status/ip interface oper status	IPortLayer1	F	T	F	0	T	maj	F	T	T

Table 17-10 Cisco IOX Registry Parameters (continued)

Short Description	Event Type	Event Subtype	Subtype Value	Expedites Polling	Event Source (IMO Name)	Activate Flow	Correlate	Is Correlation Allowed	Weight	Auto Clear	Severity	Is Ticketable	Auto Remove	Flapping
Line up syslog	line down syslog	line up syslog	up / Up	mtop-mlpppbundle-status-telnet/mtop-ima-group-state-telnet/mpls traffic engineering tunnel information / port-status/ip interface oper status	IPortLayer1	F	F	F	0	F	clr	F	T	T
OSPF neighbor down syslog	ospf neighbor syslog	ospf neighbor down syslog	Down	bfd session,ospf-interfaces,ospf-neighbors	ospfProckey	T	T	F	0	T	maj	F	T	F
OSPF neighbor up syslog	ospf neighbor syslog	ospf neighbor up syslog	Up / LOADING to FULL	bfd session,ospf-interfaces,ospf-neighbors	ospfProckey	F	F	F	0	F	clr	F	T	F
envmon powersupply syslog	envmon powersupply syslog	envmon powersupply syslog	N/A	N	IManagedElement	F	T	T	0	T	maj	F	T	F
envmon condition syslog	envmon condition syslog	envmon condition syslog	ENV_CONDITION	N	IManagedElement	F	T	T	0	T	maj	F	T	F
envmon condition clear syslog	envmon condition syslog	envmon condition clear syslog	ENV_CONDITION_CLEAR	N	IManagedElement	F	F	F	0	F	clr	F	T	F
envmon fan syslog	envmon fan syslog	envmon fan syslog	FAN	N	IManagedElement	F	T	T	0	T	maj	F	T	F
envmon fan clear syslog	envmon fan syslog	envmon fan clear syslog	FAN_CLEAR	N	IManagedElement	F	F	F	0	F	clr	F	T	F
envmon fan syslog	envmon fan syslog	envmon fan syslog	N/A	N	IManagedElement	F	T	T	0	T	maj	F	T	F
envmon tempretaure syslog	envmon tempretaure syslog	envmon tempretaure syslog	OVERTEMP	N	IManagedElement	F	T	T	0	T	maj	F	T	F

Table 17-10 Cisco IOX Registry Parameters (continued)

Short Description	Event Type	Event Subtype	Subtype Value	Expedites Polling	Event Source (IMO Name)	Activate Flow	Correlate	Is Correlation Allowed	Weight	Auto Clear	Severity	Is Ticketable	Auto Remove	Flapping
envmon tempretaure clear syslog	envmon tempretaure syslog	envmon tempretaure clear syslog	OVERTEMP_CLEAR	N	IManagedElement	F	F	F	0	F	clr	F	T	F
card out syslog	card out syslog	card out syslog	REMOVE	physical-command	IManagedElement	F	T	F	0	T	maj	F	T	T
card in syslog	card out syslog	card in syslog	INSERT	physical-command	IManagedElement	F	F	F	0	F	clr	F	T	T
envmon powersupply syslog	envmon powersupply syslog	envmon powersupply syslog	POWERSUPPLY_CURRENT	N	IManagedElement	F	T	T	0	T	maj	F	T	F
envmon powersupply clear syslog	envmon powersupply syslog	envmon powersupply clear syslog	POWERSUPPLY_CURRENT_CLEAR	N	IManagedElement	F	F	F	0	F	clr	F	T	F
envmon powersupply syslog	envmon powersupply syslog	envmon powersupply syslog	POWERSUPPLY_NONOP	N	IManagedElement	F	T	T	0	T	maj	F	T	F
envmon powersupply clear syslog	envmon powersupply syslog	envmon powersupply clear syslog	POWERSUPPLY_NONOP_CLEAR	N	IManagedElement	F	F	F	0	F	clr	F	T	F
envmon powersupply syslog	envmon powersupply syslog	envmon powersupply syslog	POWERSUPPLY_VOLTAGE	N	IManagedElement	F	T	T	0	T	maj	F	T	F
envmon powersupply clear syslog	envmon powersupply syslog	envmon powersupply clear syslog	POWERSUPPLY_VOLTAGE_CLEAR	N	IManagedElement	F	F	F	0	F	clr	F	T	F
envmon tempretaure syslog	envmon tempretaure syslog	envmon tempretaure syslog	TEMP	N	IManagedElement	F	T	T	0	T	maj	F	T	F

Table 17-10 Cisco IOX Registry Parameters (continued)

Short Description	Event Type	Event Subtype	Subtype Value	Expedites Polling	Event Source (IMO Name)	Activate Flow	Correlate	Is Correlation Allowed	Weight	Auto Clear	Severity	Is Ticketable	Auto Remove	Flapping
envmon tempretaure clear syslog	envmon tempretaure syslog	envmon tempreta ure clear syslog	TEMP_ CLEAR	N	IManagedElement	F	F	F	0	F	clr	F	T	F
envmon powersupply syslog	envmon powersupply syslog	envmon powersupply syslog	VOLTAGE	N	IManagedElement	F	T	T	0	T	maj	F	T	F
envmon powersupply clear syslog	envmon powersupply syslog	envmon powersupply clear syslog	VOLTAGE_CLEAR-	N	IManagedElement	F	F	F	0	F	clr	F	T	F
fabric hardware syslog	fabric hardware syslog	fabric hardware syslog	FIAHW_ LOS	N	IManagedElement	F	T	T	0	T	maj	F	T	F
fabric hardware clear syslog	fabric hardware syslog	fabric hardware clear syslog	FIAHW_ LOS_CLEAR	N	IManagedElement	F	F	F	0	F	clr	F	T	F
flash card removed syslog	flash card removed syslog	flash card removed syslog	UNAVAILABLE	N	IManagedElement	F	T	T	0	T	maj	F	T	F
flash card inserted syslog	flash card removed syslog	flash card inserted syslog	SWAPPED	N	IManagedElement	F	F	F	0	F	clr	F	T	F
Memory allocation is not available	memory allocation syslog	memory allocation syslog	N/A	N	IManagedElement	F	T	F	0	T	min	F	T	F
Module reset syslog	reset module syslog	reset module syslog	N/A	N	IManagedElement	F	T	T	0	F	info	T	T	T
Card oper status changed	card down syslog	card down syslog	UNPOWERED / DOWN / BRING DOWN / NOT / DISABLED	card status	IModule	F	T	F	0	T	min	F	T	T

Table 17-10 Cisco IOX Registry Parameters (continued)

Short Description	Event Type	Event Subtype	Subtype Value	Expedites Polling	Event Source (IMO Name)	Activate Flow	Correlate	Is Correlation Allowed	Weight	Auto Clear	Severity	Is Ticketable	Auto Remove	Flapping
Card oper status changed	card down syslog	card up syslog	IOS XR RUN / OK	card status	IModule	F	F	F	0	F	clr	F	T	T
card out syslog	card out syslog	card out syslog	OIROUT	physical-command	IModule	F	T	F	0	T	maj	F	T	T
card in syslog	card out syslog	card in syslog	OIRIN	N	IModule	F	F	F	0	F	clr	F	T	T
card out syslog	card out syslog	card out syslog	OIROUT	physical-command	IModule	F	T	F	0	T	maj	F	T	T
card in syslog	card out syslog	card in syslog	OIRIN	N	IModule	F	F	F	0	F	clr	F	T	T
pim neighbor loss syslog	pim neighbor loss syslog	pim neighbor loss syslog	DOWN	N	IIPInterface	F	T	F	0	T	maj	F	T	F
pim neighbor up syslog	pim neighbor loss syslog	pim neighbor up syslog	UP	N	IIPInterface	F	F	F	0	F	clr	F	T	F
pim interface down syslog	pim interface down syslog	pim interface down syslog	DOWN	N	IManagedElement	F	T	F	0	T	maj	F	T	F
pim interface up syslog	pim interface down syslog	pim interface up syslog	UP	N	IManagedElement	F	F	F	0	F	clr	F	T	F
pim invalid join syslog	pim invalid join syslog	pim invalid join syslog	N/A	N	IManagedElement	F	T	F	0	T	min	F	T	F
Card oper status changed	card down syslog	card down syslog	off	N	IManagedElement	F	T	F	0	T	min	F	T	T
Card oper status changed	card down syslog	card up syslog	on	N	IManagedElement	F	F	F	0	F	clr	F	T	T
Line down syslog	line down syslog	line down syslog	N/A	N	IPortLayer1	F	T	F	0	T	maj	F	T	T
Line up syslog	line down syslog	line up syslog	cleared	N	IPortLayer1	F	F	F	0	F	clr	F	T	T

Table 17-10 Cisco IOX Registry Parameters (continued)

Short Description	Event Type	Event Subtype	Subtype Value	Expedites Polling	Event Source (IMO Name)	Activate Flow	Correlate	Is Correlation Allowed	Weight	Auto Clear	Severity	Is Ticketable	Auto Remove	Flapping
card out syslog	card out syslog	card out syslog	REMOVED	physical-command	IModule	F	T	F	0	T	maj	F	T	T
card in syslog	card out syslog	card in syslog	INSERTED	N	IModule	F	F	F	0	F	clr	F	T	T
LDP neighbor down syslog	ldp neighbor down syslog	ldp neighbor down syslog	DOWN	mpls interfaces, label switching table, mpls-ldp-peers	IProfileContainer (LSE)	F	T	F	0	T	maj	F	T	F
LDP neighbor up syslog	ldp neighbor down syslog	ldp neighbor up syslog	UP	mpls interfaces, label switching table, mpls-ldp-peers	IProfileContainer (LSE)	F	F	F	0	F	clr	F	T	F
BGP neighbor down syslog	bgp neighbor down syslog	bgp neighbor down syslog	down / Down	bgp neighbours	IBgpNeighbourEntry	F	T	F	0	T	maj	F	T	F
BGP neighbor up syslog	bgp neighbor down syslog	bgp neighbor up syslog	up / Up	bgp neighbours	IBgpNeighbourEntry	F	F	F	0	F	clr	F	T	F
Login authentication failed syslog	login authentication failed syslog	login authentication failed syslog	N/A	N	IManagedElement	F	F	F	0	F	min	T	T	F
If-Table in sync syslog	if table in sync syslog	if table in sync syslog	N/A	physical-command	IModule	F	T	F	0	F	info	F	T	F
bfd session down syslog	bfd session down syslog	bfd session down syslog	down	bfd session	IBfdService	F	T	F	0	T	maj	F	T	F
bfd session removed syslog	bfd session down syslog	bfd session removed syslog	removed	bfd session	IBfdService	F	T	F	0	T	maj	F	T	F
bfd session up syslog	bfd session down syslog	bfd session up syslog	up	bfd session	IBfdService	F	F	F	0	F	clr	F	T	F

Table 17-10 Cisco IOX Registry Parameters (continued)

Short Description	Event Type	Event Subtype	Subtype Value	Expedites Polling	Event Source (IMO Name)	Activate Flow	Correlate	Is Correlation Allowed	Weight	Auto Clear	Severity	Is Ticketable	Auto Remove	Flapping
Layer2 G709 alarm syslog	layer2 G709 alarm syslog	layer2 G709 alarm syslog	N/A	N	DWDM Oid	F	F	F	0	T	wrn	F	T	F
Layer2 G709 clear syslog	layer2 G709 alarm syslog	layer2 G709 clear syslog	cleared	N	DWDM Oid	F	F	F	0	F	clr	F	T	F
Layer2 dwdm info syslog	layer2 dwdm info syslog	layer2 dwdm info syslog	N/A	N	IManagedElement	F	F	F	0	T	info	F	T	F
Layer1 PM TCA syslog	layer1 PM TCA syslog	layer1 PM TCA syslog	N/A	N	DWDM Oid	F	F	F	0	T	wrn	F	T	F
Layer2 SPA failure syslog	layer2 SPA failure syslog	layer2 SPA failure syslog	N/A	N	IManagedElement	F	T	F	0	T	min	F	T	F
OSPF routing neighbor down syslog	ospf routing neighbor syslog	ospf routing neighbor down syslog	Down/DOWN	bfd session,ospf-interfaces,ospf-neighbors	ospfProckey	T	T	F	0	F	maj	T	T	F
OSPF routing neighbor up syslog	ospf routing neighbor syslog	ospf routing neighbor up syslog	Up / LOADING to FULL	bfd session,ospf-interfaces,ospf-neighbors	ospfProckey	F	F	F	0	F	clr	F	T	F
OSPFv3 neighbor down syslog	ospfv3 neighbor syslog	ospfv3 neighbor down syslog	Down / DOWN	bfd session,ospf-interfaces,ospf-neighbors	ospfProckey	T	T	F	0	T	maj	F	T	F
OSPFv3 neighbor up syslog	ospfv3 neighbor syslog	ospfv3 neighbor up syslog	Up / FULL	bfd session,ospf-interfaces,ospf-neighbors	ospfProckey	F	F	F	0	T	clr	F	T	F
OSPFv3 routing neighbor down syslog	ospfv3 routing neighbor down syslog	ospfv3 routing neighbor down syslog	Down / DOWN	bfd session,ospf-interfaces,ospf-neighbors	ospfProckey	F	T	F	0	T	maj	F	T	F

Table 17-10 Cisco IOX Registry Parameters (continued)

Short Description	Event Type	Event Subtype	Subtype Value	Expedites Polling	Event Source (IMO Name)	Activate Flow	Correlate	Is Correlation Allowed	Weight	Auto Clear	Severity	Is Ticketable	Auto Remove	Flapping
OSPFv3 routing neighbor up syslog	ospfv3 routing neighbor down syslog	ospfv3 routing neighbor up syslog	Up / FULL	bfd session,ospf-interfaces,ospf-neighbors	ospfProckey	F	F	F	0	T	clr	F	T	F
Routing BGP neighbor down syslog	routing bgp neighbor down syslog	routing bgp neighbor down syslog	down / Down	N	IBgpNeighbourEntry	F	T	F	0	T	maj	F	T	F
Routing BGP neighbor up syslog	routing bgp neighbor down syslog	routing bgp neighbor up syslog	up / Up	N	IBgpNeighbourEntry	F	F	F	0	T	clr	F	T	F
IPv6 Routing BGP neighbor down syslog	ipv6 routing bgp neighbor down syslog	ipv6 routing bgp neighbor down syslog	down / Down	N	IManagedElement	F	T	F	0	T	maj	F	T	F
IPv6 Routing BGP neighbor up syslog	ipv6 routing bgp neighbor down syslog	ipv6 routing bgp neighbor up syslog	up / Up	N	IManagedElement	F	F	F	0	T	clr	F	T	F
pseudo wire tunnel down syslog	pseudo wire tunnel syslog	pseudo wire tunnel down syslog		ce-pw-tunnel-status-telnet	PTPLayer2MplsTunnel	F	T	F	0	T	min	F	T	T
pseudo wire tunnel up syslog	pseudo wire tunnel syslog	pseudo wire tunnel up syslog		ce-pw-tunnel-status-telnet	PTPLayer2MplsTunnel	F	F	F	0	T	clr	F	T	T
EFP service error disabled syslog	efp service error disabled syslog	efp service error disabled syslog		EFP status	IEFP	F	T	F	0	F	info	F	T	F

Table 17-10 Cisco IOX Registry Parameters (continued)

Short Description	Event Type	Event Subtype	Subtype Value	Expedites Polling	Event Source (IMO Name)	Activate Flow	Correlate	Is Correlation Allowed	Weight	Auto Clear	Severity	Is Ticketable	Auto Remove	Flapping
DWDM feature not implemented yet	Dwdm not implemented syslog	Dwdm not implemented syslog		N	IManagedElement	F	F	F	0	T	wrn	false	T	F
DWDM fatal error with reason and error number	DWDM fatal error 2 syslog	DWDM fatal error 2 syslog		N	IManagedElement	F	F	F	0	T	maj	false	T	F
DWDM fatal error with reason	DWDM fatal error syslog	DWDM fatal error 2 syslog		N	IManagedElement	F	F	F	0	T	maj	false	T	F
PLIM EIO training errors syslog	PLIM EIO training errors syslog	PLIM EIO training errors syslog		N	IManagedElement	F	F	F	0	T	maj	false	T	F
PLIM Checkpoint Initialization Failure syslog	PLIM check point failure syslog	PLIM check point failure syslog		N	IManagedElement	F	F	F	0	T	min	false	T	F
PLIM ASIC error syslog	PLIM asic error syslog	PLIM asic error syslog		N	IManagedElement	F	F	F	0	T	min	false	T	F
PLIM memory error syslog	PLIM memory error syslog	PLIM memory error syslog		N	IManagedElement	F	F	F	0	T	maj	false	T	F
PLIM squid error syslog	PLIM squid error syslog	PLIM squid error syslog		N	IManagedElement	F	F	F	0	T	min	false	T	F
PLIM 7 error syslog	PLIm 7b error syslog	PLIm 7b error syslog		N	IManagedElement	F	F	F	0	T	min	false	T	F

Table 17-10 Cisco IOX Registry Parameters (continued)

Short Description	Event Type	Event Subtype	Subtype Value	Expedites Polling	Event Source (IMO Name)	Activate Flow	Correlate	Is Correlation Allowed	Weight	Auto Clear	Severity	Is Ticketable	Auto Remove	Flapping
PLIM OC768 critical error syslog	PLIM OC768 critical error syslog	PLIM OC768 critical error syslog		N	IManagedElement	F	F	F	0	T	maj	false	T	F
PLIM OC768 INFO syslog	PLIM OC768 INFO syslog	PLIM OC768 INFO syslog		N	IManagedElement	F	F	F	0	T	info	false	T	F
PLIM OC768 debug syslog	PLIM OC768 debug syslog	PLIM OC768 debug syslog		N	IManagedElement	F	F	F	0	T	info	false	T	F
BGP notification syslog	bgp notification syslog	bgp notification syslog		N	IPhysicalLayer	T	T	F	0	F	info	F	T	F
BGP notification syslog	bgp notification syslog	bgp notification syslog		N	IPhysicalLayer	T	T	F	0	F	info	F	T	F
routing ISIS neighbor down syslog	routing isis neighbor down syslog	routing isis neighbor down syslog	Down	N	IPhysicalLayer	F	T	F	0	T	maj	F	T	F
routing ISIS neighbor up syslog	routing isis neighbor down syslog	routing isis neighbor up syslog	Up	N	IPhysicalLayer	F	F	F	0	F	clr	F	T	F
Backup to Master change syslog	Backup to Master syslog	Backup to Master syslog	Backup	N	IIPInterface	F	F	F	0	F	info	T	T	F
Master to Backup change syslog	Backup to Master syslog	Master to Backup syslog	Master	N	IIPInterface	F	F	F	0	F	info	T	T	F
IP standby state change syslog	IP standby state change syslog	IP standby state change syslog	Init, Disabled	hsrp	IPInterface	F	T	F	0	T	minor	F	T	F

Table 17-10 Cisco IOX Registry Parameters (continued)

Short Description	Event Type	Event Subtype	Subtype Value	Expedites Polling	Event Source (IMO Name)	Activate Flow	Correlate	Is Correlation Allowed	Weight	Auto Clear	Severity	Is Ticketable	Auto Remove	Flapping
IP standby state restored syslog	IP standby state change syslog	IP standby state restored syslog	!=Init, Disabled	hsrp	IPInterface	F	T	F	0	F	clr	F	T	F
DWDM5 SRLG OVERFLOW syslog	DWDM5 SRLG OVERFLOW syslog	DWDM5 SRLG OVERFLOW syslog		N	IManagedElement	F	F	F	0	T	wrn	false	T	F
L2 SONET APS Disabled syslog	L2 SONET APS	L2 SONET APS Disabled	Disabled	N	IPhysicalLayer	F	F	F	0	F	min	false	T	F
L2 SONET APS enabled syslog	L2 SONET APS	L2 SONET APS Enabled	Enabled	N	IPhysicalLayer	F	F	F	0	F	clr	false	T	F
Bfd per member link session down syslog	bfd per member link session down syslog	bfd per member link session down syslog	REMOVED	bfd session	IBfdService	F	T	F	0	T	maj	F	T	T
Bfd per member link session up syslog	bfd per member link session down syslog	bfd per member link session up syslog	STATE_UP	bfd session	IBfdService	F	F	F	0	F	clr	F	F	T
Bfd session state down syslog	bfd session state down syslog	bfd session state down syslog	STATE_DOWN	bfd session	IBfdService	F	T	F	0	T	maj	F	T	T
Bfd session state up syslog	bfd session state down syslog	bfd session state up syslog	UP	bfd session	IBfdService	F	F	F	0	F	clr	F	F	T

Table 17-10 Cisco IOX Registry Parameters (continued)

Short Description	Event Type	Event Subtype	Subtype Value	Expedites Polling	Event Source (IMO Name)	Activate Flow	Correlate	Is Correlation Allowed	Weight	Auto Clear	Severity	Is Ticketable	Auto Remove	Flapping
Bundle manager inactive syslog	bundle manager active syslog	bundle manager inactive syslog	no longer Active	NA	BundleEther channel	F	F	F	0	T	maj	F	T	F
Bundle manager active syslog	bundle manager active syslog	bundle manager active syslog	Active	NA	BundleEther channel	F	F	F	0	F	clr	F	F	F
Bundle manager bfd session starting syslog	bundle manager bfd session syslog	bundle manager bfd session starting syslog	STARTING	NA	IBfdService	F	F	F	0	F	info	F	F	F
Bundle manager bfd session up syslog	bundle manager bfd session syslog	bundle manager bfd session up syslog	SESSION_UP	NA	IBfdService	F	F	F	0	F	info	F	F	F
Bfd MPLS TE warning syslog	mpls te warning syslog	mpls te warning syslog		NA	IBfdService	F	F	F	0	F	info	F	F	F
Bfd session inherit off syslog	bfd session inherit syslog	bfd session inherit off syslog	OFF	NA	IBfdService	F	F	F	0	F	info	F	F	F
Bfd session inherit on syslog	bfd session inherit syslog	bfd session inherit on syslog	ON	NA	IBfdService	F	F	F	0	F	info	F	F	F
Resynchronization of the MAC address table is complete	Dropping	Dropping	MAC Resync	Expediate - ce-iosxr-39-bridge-table-telnet	IModule	F	F	F	0	F	min	F	F	F

Table 17-10 Cisco IOX Registry Parameters (continued)

Short Description	Event Type	Event Subtype	Subtype Value	Expedites Polling	Event Source (IMO Name)	Activate Flow	Correlate	Is Correlation Allowed	Weight	Auto Clear	Severity	Is Ticketable	Auto Remove	Flapping
Fan module oper status changed	fan down syslog	fan down syslog	UNPOWERED / DOWN / BRING DOWN / NOT / DISABLED	card status	IModule	F	T	F	0	T	min	F	T	T
Fan module oper status changed	fan down syslog	fan up syslog	IOS XR RUN / OK	card status	IModule	F	F	F	0	F	clr	F	T	T
Fan module out syslog	fan out syslog	fan out syslog	OIROUT	physical-command	IModule	F	T	F	0	T	maj	F	T	T
Fan module in syslog	fan out syslog	fan in syslog	OIRIN	physical-command, redandant card command	IModule	F	F	F	0	F	clr	F	T	T
Power module oper status changed	power down syslog	power down syslog	UNPOWERED / DOWN / BRING DOWN / NOT / DISABLED	card status	IModule	F	T	F	0	T	min	F	T	T
Power module oper status changed	power down syslog	power up syslog	IOS XR RUN / OK	card status	IModule	F	F	F	0	F	clr	F	T	T
Power module out syslog	power out syslog	power out syslog	OIROUT	physical-command	IModule	F	T	F	0	T	maj	F	T	T
Power module in syslog	power out syslog	power in syslog	OIRIN	physical-command, redandant card command	IModule	F	F	F	0	F	clr	F	T	T
L2 Sonet APS 6 K1K2 info syslog	L2 Sonet APS K1K2 info	l2 sonet APS 6 k1k2 info syslog	NA	N	IManagedElement	F	F	F	0	F	info	F	T	F

Table 17-10 Cisco IOX Registry Parameters (continued)

Short Description	Event Type	Event Subtype	Subtype Value	Expedites Polling	Event Source (IMO Name)	Activate Flow	Correlate	Is Correlation Allowed	Weight	Auto Clear	Severity	Is Ticketable	Auto Remove	Flapping
L2 Sonet APS 6 Contact syslog	L2 Sonet APS Contact syslog	l2 sonet APS 6 contact info syslog	NA	N	IManagedElement	F	F	F	0	F	info	F	T	F
L2 T3E3 line state up syslog	L2 T3E3 4 UPDOWN	t3e3 line state UP	UP	port-status	IPortLayer1	F	T	F	0	F	clr	T	T	F
L2 T3E3 line state down syslog	L2 T3E3 4 UPDOWN	t3e3 line state DOWN	DOWN	port-status	IPortLayer2	F	T	F	0	T	maj	T	T	F
SONET Line AIS cleared syslog	SONET-LOCAL-4-ALARM	SONET Line AIS cleared syslog	cleared	port-status	IPortLayer3	F	T	F	1	T	clr	T	T	F
SONET PATH AIS cleared syslog	SONET-LOCAL-4-ALARM	SONET Path AIS cleared syslog	cleared	port-status	IPortLayer4	F	T	F	2	T	clr	T	T	F
SONET Line AIS syslog	SONET-LOCAL-4-ALARM-UP	SONET Line AIS syslog	Up	port-status	IPortLayer5	F	T	F	3	T	min	T	T	F
SONET PATH AIS syslog	SONET-LOCAL-4-ALARM-UP	SONET Path AIS syslog	Up	port-status	IPortLayer6	F	T	F	4	T	min	T	T	F

Cisco ACE Syslog Registry Parameters

Table 17-11 lists the associated event types, event subtypes, and Prime Network registry parameters for the Cisco ACE syslogs shown in Table 17-5.

Table 17-11 Cisco ACE Syslog Registry Parameters

Short Description	Event Type	Event Subtype	Subtype Value	Expedites Polling	Event Source (IMO Name)	Activate	Correlate	Is Correlation Allowed	Weight	Auto Clear	Severity	Is Ticketable	Auto Remove	Flapping
Link down syslog	link down syslog	link down syslog		ip interface oper status	IIPInterface	F	T	F	0	T	min	F	T	T
Link up syslog	link down syslog	link up syslog		ip interface oper status	IIPInterface	F	F	F	0	F	clr	F	T	T
Link down syslog	link down syslog	link down syslog		ip interface oper status	IIPInterface	F	T	F	0	T	min	F	T	T
Link up syslog	link down syslog	link up syslog		ip interface oper status	IIPInterface	F	F	F	0	F	clr	F	T	T
Deny protocol reverse path check	ACE-106021 -syslog	ACE-1060 21-syslog				F	F	F	0	T	maj	F	T	F
Access rule memory exhausted	ACE-106028 -syslog	ACE-1060 28-syslog				F	F	F	0	T	maj	F	T	F
License manager exiting	ACE-444006 -syslog	ACE-4440 06-syslog				F	F	F	0	T	maj	F	T	F
The ACE attempted to start or set up the application acceleration core daemon process	ACE-456029 -syslog	ACE-4560 29-syslog				F	F	F	0	T	maj	F	T	F
Critical shared memory setup failure	ACE-456078 -syslog	ACE-4560 78-syslog				F	F	F	0	T	maj	F	T	F
Critical Semaphore related errors	ACE-456080 -syslog	ACE-4560 80-syslog				F	F	F	0	T	maj	F	T	F
A generic alert-level message	ACE-456085 -syslog	ACE-4560 85-syslog				F	F	F	0	T	info	F	T	F
The ACE initialization has failed	ACE-456086 -syslog	ACE-4560 86-syslog				F	F	F	0	T	maj	F	T	F
Peer IP address is not reachable	ACE-727001 -syslog	ACE-7270 01-syslog				F	F	F	0	T	maj	F	T	F
Peer device is not reachable on an FT Interface	ACE-727002 -syslog	ACE-7270 02-syslog				F	F	F	0	T	maj	F	T	F
Mismatch incontext names detected for FTgroup	ACE-727003 -syslog	ACE-7270 03-syslog				F	F	F	0	T	maj	F	T	F

Table 17-11 Cisco ACE Syslog Registry Parameters (continued)

Short Description	Event Type	Event Subtype	Subtype Value	Expedites Polling	Event Source (IMO Name)	Activate	Correlate	Is Correlation Allowed	Weight	Auto Clear	Severity	Is Ticketable	Auto Remove	Flapping
Both devices were detected to be Active for the same FT group	ACE-727004 -syslog	ACE-7270 04-syslog				F	F	F	0	T	maj	F	T	F
Configuration could not be synced to the peer device	ACE-727005 -syslog	ACE-7270 05-syslog				F	F	F	0	T	maj	F	T	F
Peer is incompatible	ACE-727006 -syslog	ACE-7270 06-syslog				F	F	F	0	T	maj	F	T	F
Module Initialization failure	ACE-727007 -syslog	ACE-7270 07-syslog				F	F	F	0	T	maj	F	T	F
Failed to send heartbeats to peer	ACE-727008 -syslog	ACE-7270 08-syslog				F	F	F	0	T	maj	F	T	F
Initialization failure - general	ACE-728001 -syslog	ACE-7280 01-syslog				F	F	F	0	T	maj	F	T	F
Initialization failure - sticky	ACE-728002 -syslog	ACE-7280 02-syslog				F	F	F	0	T	maj	F	T	F
Initialization failure - sticky hash	ACE-728003 -syslog	ACE-7280 03-syslog				F	F	F	0	T	maj	F	T	F
The CLI end of line (EOL) function	ACE-100001 -syslog	ACE-1000 01-syslog				F	F	F	0	T	maj	F	T	F
Reload started	ACE-199006 -syslog	ACE-1990 06-syslog				F	F	F	0	T	maj	F	T	F
SNMPD initialization failed	ACE-212007 -syslog	ACE-2120 07-syslog				F	F	F	0	T	maj	F	T	F
ICMP Manager Initialization Failed	ACE-313006 -syslog	ACE-3130 06-syslog				F	F	F	0	T	maj	F	T	F
System experienced fatal failure	ACE-443001 -syslog	ACE-4430 01-syslog				F	F	F	0	T	maj	F	T	F
License checkout failure	ACE-444001 -syslog	ACE-4440 01-syslog				F	F	F	0	T	maj	F	T	F
Evaluation license expired	ACE-444004 -syslog	ACE-4440 04-syslog				F	F	F	0	T	maj	F	T	F
Invalid stream	ACE-456014 -syslog	ACE-4560 14-syslog				F	F	F	0	T	maj	F	T	F

Table 17-11 Cisco ACE Syslog Registry Parameters (continued)

Short Description	Event Type	Event Subtype	Subtype Value	Expedites Polling	Event Source (IMO Name)	Activate	Correlate	Is Correlation Allowed	Weight	Auto Clear	Severity	Is Ticketable	Auto Remove	Flapping
Critical error parsing ACC module configuration	ACE-456090 -syslog	ACE-4560 90-syslog				F	F	F	0	T	maj	F	T	F
Communication failure	ACE-727009 -syslog	ACE-7270 09-syslog				F	F	F	0	T	maj	F	T	F
Data replication failed and not synced to the peer device	ACE-727010 -syslog	ACE-7270 10-syslog				F	F	F	0	T	maj	F	T	F
Configuration synchronization does not occurred	ACE-727011 -syslog	ACE-7270 11-syslog				F	F	F	0	T	maj	F	T	F
The state transitions made by an HA state device for a context.	ACE-727012 -syslog	ACE-7270 12-syslog				F	F	F	0	T	info	F	T	F
The peer is now reachable	ACE-727013 -syslog	ACE-7270 13-syslog				F	F	F	0	T	info	F	T	F
The redundancy heartbeats from a peer have become unidirectional	ACE-727014 -syslog	ACE-7270 14-syslog				F	F	F	0	T	maj	F	T	F
Detected mismatch in heartbeat interval from the peer	ACE-727015 -syslog	ACE-7270 15-syslog				F	F	F	0	T	info	F	T	F
The replication is being carried out to a peer	ACE-727016 -syslog	ACE-7270 16-syslog				F	F	F	0	T	info	F	T	F
ACE FT Track UP syslog	ACE FT Track down syslog	ACE FT Track up syslog				F	F	F	0	T	clr	F	T	F
ACE FT Track DOWN syslog	ACE FT Track down syslog	ACE FT Track down syslog				F	F	F	0	T	maj	F	T	F
Drop connection as Application Acceleration Maximum	ACE-LB_Ge neral-728033 -syslog	ACE-LB_ General-7 28033-sys log				F	F	F	0	T	info	F	T	F

Table 17-11 Cisco ACE Syslog Registry Parameters (continued)

Short Description	Event Type	Event Subtype	Subtype Value	Expedites Polling	Event Source (IMO Name)	Activate	Correlate	Is Correlation Allowed	Weight	Auto Clear	Severity	Is Ticketable	Auto Remove	Flapping
Disabled Web Application Acceleration	ACE-LB_General-728035-syslog	ACE-LB_General-728035-syslog				F	F	F	0	T	info	F	T	F
Enabled Web Application Acceleration	ACE-LB_General-728036-syslog	ACE-LB_General-728036-syslog				F	F	F	0	T	info	F	T	F

Cisco Nexus Syslog Registry Parameters

Table 17-12 lists the associated event types, event subtypes, and Prime Network registry parameters for the Cisco Nexus syslogs shown in Table 17-6.

Table 17-12 Cisco Nexus Syslog Registry Parameters

Short Description	Event Type	Event Subtype	Subtype Value	Expedites Polling	Event Source (IMO Name)	Activate	Correlate	Is Correlation Allowed	Weight	Auto Clear	Severity	Is Ticketable	Auto Remove	Flapping
HSRP group change syslog	hsrp syslog	hsrp group change syslog	Init	NA	ME	F	T	F	0	F	info	F	T	F
HSRP group restored syslog	hsrp syslog	hsrp group restored syslog	Active,Standby	NA	ME	F	F	F	0	F	clr	F	T	F
BGP neighbor down syslog	bgp neighbor down syslog	bgp neighbor down syslog	Down	NA	ME	F	T	F	0	T	maj	F	T	F
BGP neighbor up syslog	bgp neighbor down syslog	bgp neighbor up syslog	Up	NA	ME	F	F	F	0	F	clr	F	T	F
OSPF neighbor down syslog	ospf neighbor syslog	ospf neighbor down syslog	DOWN	NA	ME	T	T	F	0	T	maj	F	T	F
OSPF neighbor up syslog	ospf neighbor syslog	ospf neighbor up syslog	FULL	NA	ME	F	F	F	0	F	clr	F	T	F

Table 17-12 Cisco Nexus Syslog Registry Parameters (continued)

Short Description	Event Type	Event Subtype	Subtype Value	Expedites Polling	Event Source (IMO Name)	Activate	Correlate	Is Correlation Allowed	Weight	Auto Clear	Severity	Is Ticketable	Auto Remove	Flapping
OSPF neighbor down syslog	ospf neighbor syslog	ospf neighbor down syslog		NA	IPortLayer1	F	T	F	0	T	maj	F	T	F
OSPF neighbor up syslog	ospf neighbor syslog	ospf neighbor up syslog		NA	IPortLayer1	F	F	F	0	F	clr	F	T	F
Interface is down syslog	Port_5_Down	Interface_is_down		NA	IPortLayer1	F	T	F	0	T	maj	F	T	F
Configuration error has occurred syslog	Port_5_Down	Configuration_error_occurred		NA	IPortLayer1	F	T	F	0	T	min	F	T	F
Configuration error has occurred syslog	Port_5_Down	Configuration_error_occurred		NA	IPortLayer1	F	T	F	0	T	min	F	T	F
Interface is down syslog	Port_5_Down	Interface_is_down		NA	IPortLayer1	F	T	F	0	T	maj	F	T	F
Configuration error has occurred syslog	Port_5_Down	Configuration_error_occurred		NA	IPortLayer1	F	T	F	0	T	min	F	T	F
Configuration error has occurred syslog	Port_5_Down	Configuration_error_occurred		NA	IPortLayer1	F	T	F	0	T	min	F	T	F
Configuration error has occurred syslog	Port_5_Down	Configuration_error_occurred		NA	IPortLayer1	F	T	F	0	T	min	F	T	F
Configuration error has occurred syslog	Port_5_Down	Configuration_error_occurred		NA	IPortLayer1	F	T	F	0	T	min	F	T	F
Configuration error has occurred syslog	Port_5_Down	Configuration_error_occurred		NA	IPortLayer1	F	T	F	0	T	min	F	T	F
Configuration error has occurred syslog	Port_5_Down	Configuration_error_occurred		NA	IPortLayer1	F	T	F	0	T	min	F	T	F
Configuration error has occurred syslog	Port_5_Down	Configuration_error_occurred		NA	IPortLayer1	F	T	F	0	T	min	F	T	F

Table 17-12 Cisco Nexus Syslog Registry Parameters (continued)

Short Description	Event Type	Event Subtype	Subtype Value	Expedites Polling	Event Source (IMO Name)	Activate	Correlate	Is Correlation Allowed	Weight	Auto Clear	Severity	Is Ticketable	Auto Remove	Flapping
Configuration error has occurred syslog	Port_5_Down	Configuration_error_occurred		NA	IPortLayer1	F	T	F	0	T	min	F	T	F
Configuration error has occurred syslog	Port_5_Down	Configuration_error_occurred		NA	IPortLayer1	F	T	F	0	T	min	F	T	F
Configuration error has occurred syslog	Port_5_Down	Configuration_error_occurred		NA	IPortLayer1	F	T	F	0	T	min	F	T	F
Configuration error has occurred syslog	Port_5_Down	Configuration_error_occurred		NA	IPortLayer1	F	T	F	0	T	min	F	T	F
Configuration error has occurred syslog	Port_5_Down	Configuration_error_occurred		NA	IPortLayer1	F	T	F	0	T	min	F	T	F
Interface is removed syslog	Port_5_Down	Interface_is_removed		NA	IPortLayer1	F	T	F	0	T	maj	F	T	F
Configuration error has occurred syslog	Port_5_Down	Configuration_error_occurred		NA	IPortLayer1	F	T	F	0	T	min	F	T	F
Configuration error has occurred syslog	Port_5_Down	Configuration_error_occurred		NA	IPortLayer1	F	T	F	0	T	min	F	T	F
Link down syslog	Port_5_Down	Link_is_down		NA	IPortLayer1	F	T	F	0	T	min	F	T	F
Configuration error has occurred syslog	Port_5_Down	Configuration_error_occurred		NA	IPortLayer1	F	T	F	0	T	min	F	T	F
Configuration error has occurred syslog	Port_5_Down	Configuration_error_occurred		NA	IPortLayer1	F	T	F	0	T	min	F	T	F
Interface down due to module syslog	Port_5_Down	Interface_down_due_to_module		NA	IPortLayer1	F	T	F	0	T	maj	F	T	F
Interface is down syslog	Port_5_Down	Interface_is_down		NA	IPortLayer1	F	T	F	0	T	maj	F	T	F
Link down syslog	Port_5_Down	Link_is_down		NA	IPortLayer1	F	T	F	0	T	min	F	T	F

Table 17-12 Cisco Nexus Syslog Registry Parameters (continued)

Short Description	Event Type	Event Subtype	Subtype Value	Expedites Polling	Event Source (IMO Name)	Activate	Correlate	Is Correlation Allowed	Weight	Auto Clear	Severity	Is Ticketable	Auto Remove	Flapping
Interface is down syslog	Port_5_Down	Interface_is_down		NA	IPortLayer1	F	T	F	0	T	maj	F	T	F
Interface is down syslog	Port_5_Down	Interface_is_down		NA	IPortLayer1	F	T	F	0	T	maj	F	T	F
Link down syslog	Port_5_Down	Link_is_down		NA	IPortLayer1	F	T	F	0	T	min	F	T	F
Interface is down syslog	Port_5_Down	Interface_is_down		NA	IPortLayer1	F	T	F	0	T	maj	F	T	F
Interface is down syslog	Port_5_Down	Interface_is_down		NA	IPortLayer1	F	T	F	0	T	maj	F	T	F
Configuration error has occurred syslog	Port_5_Down	Configuration_error_occurred		NA	IPortLayer1	F	T	F	0	T	min	F	T	F
Configuration error has occurred syslog	Port_5_Down	Configuration_error_occurred		NA	IPortLayer1	F	T	F	0	T	min	F	T	F
Configuration error has occurred syslog	Port_5_Down	Configuration_error_occurred		NA	IPortLayer1	F	T	F	0	T	min	F	T	F
Configuration error has occurred syslog	Port_5_Down	Configuration_error_occurred		NA	IPortLayer1	F	T	F	0	T	min	F	T	F
Interface is removed syslog	Port_5_Down	Interface_down_due_to_module		NA	IPortLayer1	F	T	F	0	T	maj	F	T	F
Interface is up syslog	Port_5_Down	Port_5_Up		NA	IPortLayer1	F	F	F	0	F	clr	F	T	F
IPV6 configuration changed syslog	IPV6_config_event	IPV6_config_event		NA	IManagedElement	F	F	F	0	T	info	F	T	F
IPV6 interface deleted syslog	IPV6_interface_deleted	IPV6_interface_deleted		NA	IPortLayer1	F	F	F	0	T	info	F	T	F
IPV6 interface changed syslog	IPV6_interface_event	IPV6_interface_event		NA	IPortLayer1	F	F	F	0	T	info	F	T	F
IPV6 stats error syslog	IPV6_stats_error	IPV6_stats_error		NA	IPortLayer1	F	F	F	0	T	info	F	T	F

Table 17-12 Cisco Nexus Syslog Registry Parameters (continued)

Short Description	Event Type	Event Subtype	Subtype Value	Expedites Polling	Event Source (IMO Name)	Activate	Correlate	Is Correlation Allowed	Weight	Auto Clear	Severity	Is Ticketable	Auto Remove	Flapping
IPV6 route not active syslog	IPV6_route_not_active	IPV6_route_not_active		NA	IManagedElement	F	F	F	0	T	info	F	T	F
IPV6 configuration manager started	IPV6_starting	IPV6_starting		NA	IManagedElement	F	F	F	0	T	info	F	T	F
IPV6 PIM6 Data Register suppressed syslog	IPV6_register_send_message	IPV6_register_send_message		NA	IManagedElement	F	F	F	0	T	info	F	T	F



PART 4

Commands



CHAPTER 18

Using Connectivity Fault Management Commands

Ethernet Connectivity Fault Management (CFM) is an end-to-end, per-service-instance Ethernet layer operations, administration, and maintenance (OAM) protocol. CFM includes proactive connectivity, monitoring, fault verification, and fault isolation for large Ethernet metropolitan-area networks (MANs) and WANs.

End-to-end network elements can be premises equipment (PE)-to-PE or customer equipment (CE)-to-CE. A service can be a service provider VLAN (S-VLAN) or an Ethernet virtual connection (EVC).

Cisco Prime Network discovers and represents device configurations for CFM 802.1ag (draft 8.1) and Cisco draft mode, including:

- Maintenance domains
- Maintenance endpoints (up-facing, down-facing)
- Maintenance intermediate points (up-facing, down-facing)
- Continuity check message status

For each CFM domain, Prime Network discovers and represents the following CFM domain attributes within the logical inventory:

- Domain name
- Maintenance level (a value from 0 to 7)
- Maintenance associations (802.1ag D8.1)
- VLAN IDs specified for a maintenance association

Prime Network discovers and represents CFM maintenance endpoints (MEPs) that are configured under:

- Switch port
- Port channel (that is, link aggregation group [LAG])
- Subinterface
- Service instance or bridge domain

Note You can navigate from the MEP logical inventory to the interface or port channel on which the MEP is configured.

CFM uses standard Ethernet frames. CFM frames are distinguishable by EtherType and for multicast messages, by MAC address. CFM frames are sourced, terminated, processed, and relayed by bridges. Routers support only limited CFM functions.

Bridges that cannot interpret CFM messages forward them as normal data frames. All CFM messages are confined to a maintenance domain and to an S-VLAN (PE-VLAN or Provider-VLAN). CFM supports three types of messages:

- Continuity check—Multicast heartbeat messages exchanged periodically among MEPs. They allow MEPs to discover other MEPs within a domain and allow maintenance intermediate points (MIPs) to discover MEPs. Continuity check messages (CCMs) are confined to a domain and S-VLAN.
- Loopback—Unicast frames that a MEP transmits, at the request of an administrator, to verify connectivity to a particular maintenance point. A reply to a loopback message indicates whether a destination is reachable but does not allow hop-by-hop discovery of the path. A loopback message is similar in concept to an Internet Control Message Protocol (ICMP) Echo (ping) message.
- Traceroute—Multicast frames that a MEP transmits, at the request of an administrator, to track the path (hop-by-hop) to a destination MEP. They allow the transmitting node to discover vital connectivity data about the path, and allow the discovery of all MIPs along the path that belong to the same maintenance domain. For each visible MIP, traceroute messages indicate ingress action, relay action, and egress action. Traceroute messages are similar in concept to User Datagram Protocol (UDP) traceroute messages.

From the Logical Inventory tree, you can launch the following troubleshooting commands for a MEP:

- CFM ping
- CFM traceroute
- CFM MEP status
- CFM MEP cross-check status

Prime Network associates alarms with the corresponding MEP or global CFM logical inventory objects.

Prime Network correlates MEP down, MEP up, MEP missing, ETH-AIS, and ETH-RDI events with root cause alarms and corresponding tickets that exist along the path between the MEP on the reporting network element and the network element hosting the remote MEP.

Supported Network Elements

You can run the CFM commands on the following network elements:

- Cisco 7600 Series Routers
- Cisco ME 3400 Series Ethernet Access Switches
- Cisco ME 3750 Series Ethernet Access Switches
- Cisco ASR 9000 Series Aggregation Services Routers (supported only for the CFM IEEE 802.1ag (draft 8.1))
- Cisco Mobile Wireless Router 2941 (supported only for the CFM Cisco draft mode)
- Cisco Catalyst 6500 Series (IOS) Switches
- Cisco 3900 Series Integrated Services Routers
- Cisco XR 12000 Series Routers
- Cisco CRS Carrier Routing System
- Cisco ME3600X and Cisco ME3800X Carrier Ethernet Switches

- Cisco 3900 Series Integrated Services Routers
- Cisco MWR 2900 Series Mobile Wireless Routers
- Cisco Carrier Packet Transport (CPT) System
- Cisco ASR 903 Series Aggregation Services Routers

See Part 1—Cisco VNEs for details on the software versions Prime Network supports for these network elements.

Note You can execute the CFM commands that are supported by the software installed on the network element.

Configuring CFM Components

The following commands facilitate the configuration of CFM components:

- Configure CFM Maintenance Domain, page 18-3
- Configure CFM Global Parameters, page 18-4
- Configure CFM MIP, page 18-5
- Configure CFM Continuity Check, page 18-6
- Configure CFM Service ID, page 18-8
- Configure CFM MEP, page 18-8
- Enable CFM Continuity Check, page 18-10
- Enable CFM SNMP Server Traps, page 18-10

Note In the GUI, parameters that are displayed in bold text are mandatory.

Configure CFM Maintenance Domain

Use the **Configure CFM Maintenance Domain** command to configure the CFM domain on a device.

A maintenance domain is a management space for the purpose of managing and administering a network. A single entity owns and operates a domain and is defined by the set of ports internal to it and at its boundary.

Each maintenance domain can contain any number of maintenance associations. Each maintenance association identifies a service that can be uniquely identified within the maintenance domain. The CFM protocol runs within a particular maintenance association.

Step 1 In the inventory window, expand the Logical Inventory tree.

Step 2 Right-click the CFM node and choose **Commands > Configure > Cisco > Maintenance Domain**. The Maintenance Domain dialog box opens.

Step 3 By default, the General tab is selected. Enter values for the following parameters.

Input Parameter	Description
Domain Name	Name of the domain.
Maintenance Level	Maintenance level number. The range is from 0 to 7. A network administrator assigns a unique maintenance level to each domain. Levels and domain names are useful for defining the hierarchical relationship that exists among domains. The hierarchical relationship of domains parallel the structure of customer, service provider, and operator. The larger the domain, the higher the level value. For example, a customer domain would be larger than an operator domain. The customer domain may have a maintenance level of 7 and the operator domain may have a maintenance level of 0. Typically, operators have the smallest domains and customers the largest domains, with service provider domains between them in size. All levels of the hierarchy must operate together.
MEP Archive Hold Time	Maintenance endpoint archived hold time. The range is from 1 to 65535 minutes. A maintenance point is a demarcation point on an interface (port) that participates in CFM within a maintenance domain. Maintenance points on device ports act as filters that confine CFM frames within the bounds of a domain by dropping frames that do not belong to the correct level. Maintenance points must be explicitly configured on Cisco devices. Two classes of maintenance points exist: MEPs and maintenance intermediate points (MIPs).

Step 4 To see the commands that will be applied on the device, click **Preview**.

You can view the commands in the Result tab. You can go back and make any required changes to the input parameters.

Step 5 To schedule the command, click the Scheduling tab. For more details on scheduling, see Scheduling a Command.

Step 6 To run the commands, click **Execute Now**.

You can view errors in the Result tab, if there are any.

Step 7 To close the dialog box, click **Close**.

Configure CFM Global Parameters

Use the **Configure CFM Global Parameters** command to enable CFM globally for a network element.

Step 1 In the inventory window, expand the Logical Inventory tree.

Step 2 Right-click the CFM node and choose **Commands > Configure > Cisco > Global Parameters**. The Global Parameters dialog box opens.

Step 3 By default, the General tab is selected. Enter values for the following parameters.

Input Parameter	Description
Trace Route Cache Size	Number of cached lines. The range is from 1 to 4095. Using CFM, you can configure the device to transmit traceroute and loopback messages. This parameter sets the CFM traceroute cache size used by the CFM service.
Trace Route Cache Hold Time	Hold time. The range is from 1 to 65535 minutes. A CFM service is configurable with a hold-time value to indicate to the receiver the validity of the message. The default is 2.5 times the transmit interval.

Step 4 To see the commands that will be applied on the device, click **Preview**.

You can view the commands in the Result tab. You can go back and make any required changes to the input parameters.

Step 5 To schedule the command, click the Scheduling tab. For more details on scheduling, see Scheduling a Command.

Step 6 To run the commands, click **Execute Now**.

You can view errors in the Result tab, if there are any.

Step 7 To close the dialog box, click **Close**.

Configure CFM MIP

Use the **Configure CFM MIP** command to configure an operator-level maintenance intermediate point (MIP) for the domain-level ID. MIPs have the following characteristics:

- Per-maintenance domain (level) for all S-VLANs enabled or allowed on a port.
- Internal to a domain, not at the boundary.
- CFM frames received from MEPs and other MIPs are cataloged and forwarded, using both the wire and the relay function.
- All CFM frames at a lower level are stopped and dropped, independent of whether they originate from the wire or from relay function.
- All CFM frames at a higher level are forwarded, independent of whether they arrive from the wire or from relay function.
- Passive points respond only when triggered by CFM traceroute and loopback messages.
- Bridge-brain MAC addresses are used.

If the port on which a MIP is configured is blocked by Spanning-Tree Protocol (STP), the MIP cannot receive CFM messages or relay them toward the relay function side. The MIP can, however, receive and respond to CFM messages from the wire.

A MIP has only one level associated with it, and the command-line interface (CLI) does not allow you to configure a MIP for a domain that does not exist.

Note This command is not supported on the Cisco Carrier Packet Transport (CPT) System.

Step 1 In the inventory window, expand the Logical Inventory tree.

Step 2 Right-click the CFM node and choose **Commands > Configure > Cisco > MIP**. The MIP dialog box opens.

Step 3 By default, the General tab is selected. Enter values for the following parameters.

Input Parameter	Description
Interface Name	Name of the interface. Specify a physical interface or a port channel to configure.
Maintenance Level	Maintenance level number. The range is from 0 to 7.
VLANs[1]	VLAN ID on which to apply the remote maintenance point identifier (ID). The VLAN ID range is from 1 to 4094. Alternatively, you can choose *any* to specify all VLAN IDs. **Note** You can execute the **any** command only if the sub mode **any** is supported by the software image version of the network element.
Inner VLAN[2]	Check the check box if you have an inner VLAN tag.
Inner VLANs[2]	Inner VLAN ID on which to apply the remote maintanance point ID. The VLAN ID range is from 1 to 4094.

1. Applicable only for Cisco ME 3400 Series and Cisco ME 3750 Ethernet Access Switches running Cisco IOS Release 12.2 (52) SE and Cisco 7600 Series Routers running Cisco IOS Release 12.2(33)SRE
2. Applicable only for Cisco ME 3400 Series and Cisco ME 3750 Ethernet Access Switches running Cisco IOS Release 12.2 (54) SE

Step 4 To see the commands that will be applied on the device, click **Preview**.

You can view the commands in the Result tab. You can go back and make any required changes to the input parameters.

Step 5 To schedule the command, click the Scheduling tab. For more details on scheduling, see Scheduling a Command.

Step 6 To run the commands, click **Execute Now**.

You can view errors in the Result tab, if there are any.

Step 7 To close the dialog box, click **Close**.

Configure CFM Continuity Check

Use the **Configure CFM Continuity Check** command to configure the per-domain continuity check messages (CCMs).

CFM CCMs have the following characteristics:

- Transmitted at a configurable periodic interval by MEPs. The interval range is from 10 to 65535 seconds; the default is 30.

- Contain a configurable hold-time value to indicate to the receiver the validity of the message.
- Cataloged by MIPs at the same maintenance level.
- Terminated by remote MEPs at the same maintenance level.
- Unidirectional and do not solicit a response.
- Carry the status of the port on which the MEP is configured.

Step 1 In the inventory window, expand the Logical Inventory tree.

Step 2 Right-click the CFM node and choose **Commands > Configure > Cisco > Continuity Check**. The Continuity Check dialog box opens.

Step 3 By default, the General tab is selected. Enter values for the following parameters.

Input Parameter	Description
Maintenance Level	Maintenance level number. The range is from 0 to 7. Alternatively, you can choose *any* to specify all maintenance levels.
VLANs for Cross-Check	VLAN ID on which to apply the cross check. The VLAN ID range is from 1 to 4095. You can choose: • A single VLAN ID from 1 to 4095 • A range of VLAN IDs separated by a hyphen (-) • A series of VLAN IDs separated by commas (,) • *any* to specify all VLAN IDs
Interval for CC Messages	Interval, in seconds, for continuity check messages. The default value is 30 seconds and the range is 10 to 65535 seconds.
Loss Threshold Level for CC Packets	Loss threshold level for continuity check packets. The default value is two seconds and the range is 2 to 255 seconds.
Service[1]	The service name.
Domain[1]	The domain name.

1. Applicable for network elements that run on Cisco IOS software release 15.1

Step 4 To see the commands that will be applied on the device, click **Preview**.

You can view the commands in the Result tab. You can go back and make any required changes to the input parameters.

Step 5 To schedule the command, click the Scheduling tab. For more details on scheduling, see Scheduling a Command.

Step 6 To run the commands, click **Execute Now**.

You can view errors in the Result tab, if there are any.

Step 7 To close the dialog box, click **Close**.

Configure CFM Service ID

Use the **Configure CFM Service ID** command to configure the CFM service ID.

Step 1 In the inventory window, expand the Logical Inventory tree.

Step 2 Right-click the CFM node and choose **Commands > Configure > Cisco > Service ID**. The Service ID dialog box opens.

Step 3 By default, the General tab is selected. Enter values for the following parameters.

Input Parameter	Description
Domain Name	Name of the domain.
Maintenance Level	Maintenance level number. The range is from 0 to 7.
Service VLAN ID ([1-4094])	Service VLAN ID. A customer service instance is an Ethernet virtual connection, which is identified by an S-VLAN within an Ethernet island. You can identify an S-VLAN by using a globally unique service ID. The Service VLAN ID range is from 1 to 4094.
Inner VLAN [1]	Check the check box if you have an inner VLAN tag.
Inner VLANs[1]	Inner VLAN ID on which to apply the remote maintanance point ID. The VLAN ID range is from 1 to 4094.
EVC Name	The EVC name.

1. Applicable only for Cisco ME 3400 Series and Cisco ME 3750 Ethernet Access Switches running Cisco IOS Release 12.2 (54) SE and later.

Step 4 To see the commands that will be applied on the device, click **Preview**.

You can view the commands in the Result tab. You can go back and make any required changes to the input parameters.

Step 5 To schedule the command, click the Scheduling tab. For more details on scheduling, see Scheduling a Command.

Step 6 To run the commands, click **Execute Now**.

You can view errors in the Result tab, if there are any.

Step 7 To close the dialog box, click **Close**.

Configure CFM MEP

Use the **Configure CFM MEP** command to configure maintenance endpoints (MEPs), which have the following characteristics:

- Per-maintenance domain (level) and service (S-VLAN or EVC)
- At the edge of a domain, define the boundary
- Within the bounds of a maintenance domain, confine CFM messages
- When configured to do so, proactively transmit CFM continuity check messages (CCMs)

- At the request of an administrator, transmit traceroute and loopback messages

Note This command is not supported on the Cisco Carrier Packet Transport (CPT) System.

Step 1 In the inventory window, expand the Logical Inventory tree.

Step 2 Right-click the CFM node and choose **Commands > Configure > Cisco > MEP**. The MEP dialog box opens.

Step 3 By default, the General tab is selected. Enter values for the following parameters.

Input Parameter	Description
Domain Name	Name of the domain.
Interface Name	Name of the interface. Specify a physical interface or a port channel to configure.
Maintenance Level	Maintenance level number. The range is from 0 to 7.
Maintenance End Point Identifier	Maintenance endpoint identifier, which must be unique for each VLAN (service instance). The MEP ID is a CFM identifier used to: • Identify a MEP in CFM communications. • Catalog CFM frames in the local CFM database. The MEP ID is significant throughout the CFM domain and the maintenance association. The range is from 1 to 8191.
VLANs	VLAN ID on which to apply the maintenance endpoint. The VLAN ID range is from 1 to 4095. Alternatively, you can choose *any* to specify all VLAN IDs. **Note** You can execute the **any** command only if the sub mode **any** is supported by the software image version of the network element.

Step 4 To see the commands that will be applied on the device, click **Preview**.

You can view the commands in the Result tab. You can go back and make any required changes to the input parameters.

Step 5 To schedule the command, click the Scheduling tab. For more details on scheduling, see Scheduling a Command.

Step 6 To run the commands, click **Execute Now**.

You can view errors in the Result tab, if there are any.

Step 7 To close the dialog box, click **Close**.

Enable CFM Continuity Check

Use the **Enable CFM Continuity Check** command to enable continuity check parameters.

Step 1 In the inventory window, expand the Logical Inventory tree.

Step 2 Right-click the CFM node and choose **Commands > Enable > Cisco > Continuity Check**. The Continuity Check dialog box opens.

Step 3 By default, the General tab is selected. Enter values for the following parameters.

Input Parameter	Description
Domain Name	The domain name on which to enable the continuity check.
Maintenance Level	Maintenance level number. The range is from 0 to 7. Alternatively, you can choose *any* to specify all maintenance levels.
VLANs for Cross-Check	VLAN ID on which to apply the continuity check. The VLAN ID range is from 1 to 4094. Alternatively, you can choose *any* to specify all VLAN IDs.
Service Name[1]	The service name on which to enable the continuity check.
Bridge Group Name[1]	The bridge group name on which to enable the continuity check.
Bridge Domain Name[1]	The bridge domain name on which to enable the continuity check.
Interval for CC Messages	Interval, in seconds, for continuity check messages. The default value is 30 seconds.
Loss Threshold Level for CC Packets	The loss threshold level for CC packets. The value ranges from 2 to 225. The default value is 2.

1. Applicable for Cisco ASR 9000 series that run on Cisco IOS XR software.

Step 4 To see the commands that will be applied on the device, click **Preview**.

You can view the commands in the Result tab. You can go back and make any required changes to the input parameters.

Step 5 To schedule the command, click the Scheduling tab. For more details on scheduling, see Scheduling a Command.

Step 6 To run the commands, click **Execute Now**.

You can view errors in the Result tab, if there are any.

Step 7 To close the dialog box, click **Close**.

Enable CFM SNMP Server Traps

Use the **Enable CFM SNMP Server Traps** command to enable Ethernet CFM continuity check traps and Ethernet CFM cross-check traps.

Step 1 In the inventory window, expand the Logical Inventory tree.

Step 2 Right-click the CFM node and choose **Commands > Enable > Cisco > SNMP Server Traps**. The SNMP Server Traps dialog box opens.

The command enables SNMP server traps and does not require any input parameters.

Step 3 To see the commands that will be applied on the device, click **Preview**.

Step 4 To schedule the command, click the Scheduling tab. For more details on scheduling, see Scheduling a Command.

Step 5 To run the command, click **Execute Now**.

You can view errors in the Result tab, if there are any.

Step 6 To close the dialog box, click **Close**.

Diagnose CFM Components

The following commands facilitate diagnosing the CFM components:

- Diagnose CFM with Show MEP Status, page 18-11
- Diagnose CFM with Show MEP Crosscheck Status, page 18-12
- Diagnose CFM with Ping Remote MEP with MAC, page 18-12
- Diagnose CFM with Ping Remote MEP with MPID, page 18-13
- Diagnose CFM with Ping Remote MEP with Multicast, page 18-14
- Diagnose CFM with Traceroute Remote MEP with MAC, page 18-14
- Diagnose CFM with Traceroute Remote MEP with MPID, page 18-15

Diagnose CFM with Show MEP Status

Use the **Diagnose CFM with Show MEP Status** command to show the MEP status of CFM diagnostics.

Step 1 In the inventory window, expand the Logical Inventory tree.

Step 2 Right-click the CFM node and choose **Commands > Diagnose > Cisco > Show MEP Status**. The Show MEP Status dialog box opens.

The command checks the MEP status and does not require any input parameters.

Step 3 To see the commands that will be applied on the device, click **Preview**.

Step 4 To schedule the command, click the Scheduling tab. For more details on scheduling, see Scheduling a Command.

Step 5 To run the command, click **Execute Now**.

You can view errors in the Result tab, if there are any.

Step 6 To close the dialog box, click **Close**.

Diagnose CFM with Show MEP Crosscheck Status

Use the **Diagnose CFM with Show MEP Crosscheck Status** command to show the cross-check status of CFM MEP diagnostics.

Step 1 In the inventory window, expand the Logical Inventory tree.

Step 2 Right-click the CFM node and choose **Commands > Diagnose > Cisco > Show MEP Crosscheck Status**. The Show MEP Crosscheck Status dialog box opens.

The command checks the MEP crosscheck status and does not require any input parameters.

Step 3 To see the commands that will be applied on the device, click **Preview**.

Step 4 To schedule the command, click the Scheduling tab. For more details on scheduling, see Scheduling a Command.

Step 5 To run the command, click **Execute Now**.

You can view errors in the Result tab, if there are any.

Step 6 To close the dialog box, click **Close**.

Diagnose CFM with Ping Remote MEP with MAC

Use the **Diagnose CFM with Ping Remote MEP with MAC** command to ping the remote maintenance endpoint that supplies the MAC address.

Step 1 In the inventory window, expand the Logical Inventory tree.

Step 2 Right-click the CFM node and choose **Commands > Diagnose > IEEE > Ping Remote MEP with MAC**. The Ping Remote MEP with MAC dialog box opens.

Step 3 By default, the General tab is selected. Enter values for the following parameters.

Input Parameter	Description
Remote MAC Address	MAC address of the remote interface on which the remote MEP is configured. The MAC address has the format *aaaa.bbbb.cccc*; the default is 0000.0000.0000. CFM frames are distinguishable by EtherType and, for multicast messages, by MAC address.
Domain Name	Domain name for the remote MEP.
Option[1]	Select VLAN option for a VLAN configuration and Service option for service configuration.
VLAN ID[1]	VLAN ID on which to apply the remote MAC address. The VLAN ID range is from 1 to 4094.

1. Applicable only for Cisco ME 3400 Series and Cisco ME 3750 Ethernet Access Switches running Cisco IOS Release 12.2 (54) SE and later.

Step 4 To see the commands that will be applied on the device, click **Preview**.

You can view the commands in the Result tab. You can go back and make any required changes to the input parameters.

Step 5 To schedule the command, click the Scheduling tab. For more details on scheduling, see Scheduling a Command.

Step 6 To run the commands, click **Execute Now**.

You can view errors in the Result tab, if there are any.

Step 7 To close the dialog box, click **Close**.

Diagnose CFM with Ping Remote MEP with MPID

Use the **Diagnose CFM with Ping Remote MEP with MPID** command to ping the remote maintenance endpoint that supplies the maintenance point ID (MPID).

Step 1 In the inventory window, expand the Logical Inventory tree.

Step 2 Right-click the CFM node and choose **Commands > Diagnose > IEEE > Ping Remote MEP with MPID**. The Ping Remote MEP with MPID dialog box opens.

Step 3 By default, the General tab is selected. Enter values for the following parameters.

Input Parameter	Description
Remote MPID Address	Address of the remote maintenance point ID.
Domain Name	Name of the domain.
Option[1]	Select VLAN option for a VLAN configuration and Service option for a Service configuration.
VLAN ID[1]	VLAN ID on which to apply the remote maintenance point ID. The VLAN ID range is from 1 to 4095.

1. Applicable only for Cisco ME 3400 Series and Cisco ME 3750 Ethernet Access Switches running Cisco IOS Release 12.2 (54) SE and later.

Step 4 To see the commands that will be applied on the device, click **Preview**.

You can view the commands in the Result tab. You can go back and make any required changes to the input parameters.

Step 5 To schedule the command, click the Scheduling tab. For more details on scheduling, see Scheduling a Command.

Step 6 To run the commands, click **Execute Now**.

You can view errors in the Result tab, if there are any.

Step 7 To close the dialog box, click **Close**.

Diagnose CFM with Ping Remote MEP with Multicast

Use the **Diagnose CFM with Ping Remote MEP with Multicast** command to ping the remote maintenance endpoint that supplies the multicast.

Step 1 In the inventory window, expand the Logical Inventory tree.

Step 2 Right-click the CFM node and choose **Commands > Diagnose > IEEE > Ping Remote MEP with Multicast**. The Ping Remote MEP with Multicast dialog box opens.

Step 3 By default, the General tab is selected. Enter values for the following parameters.

Input Parameter	Description
Domain Name	Name of the domain.
Option[1]	Select VLAN option for a VLAN configuration and Service option for Service configuration.
VLAN ID[1]	VLAN ID on which to apply the remote maintenance endpoint with multicast. The VLAN ID range is from 1 to 4094.

1. Applicable only for Cisco ME 3400 Series and Cisco ME 3750 Ethernet Access Switches running Cisco IOS Release 12.2 (54) SE and later.

Step 4 To see the commands that will be applied on the device, click **Preview**.

You can view the commands in the Result tab. You can go back and make any required changes to the input parameters.

Step 5 To schedule the command, click the Scheduling tab. For more details on scheduling, see Scheduling a Command.

Step 6 To run the commands, click **Execute Now**.

You can view errors in the Result tab, if there are any.

Step 7 To close the dialog box, click **Close**.

Diagnose CFM with Traceroute Remote MEP with MAC

Use the **Diagnose CFM with Traceroute Remote MEP with MAC** command to traceroute the remote maintenance endpoint that supplies the MAC address.

Step 1 In the inventory window, expand the Logical Inventory tree.

Step 2 Right-click the CFM node and choose **Commands > Diagnose > IEEE > Traceroute Remote MEP with MAC**. The Traceroute Remote MEP with MAC dialog box opens.

Step 3 By default, the General tab is selected. Enter values for the following parameters.

Input Parameter	Description
Remote MAC Address	Remote MAC address, in the format *aaaa.bbbb.cccc*. The default MAC address is 0000.0000.0000.
Domain Name	Name of the domain.
Option[1]	Select VLAN option for a VLAN configuration and Service option for Service configuration.
VLAN ID[1]	VLAN ID on which to apply the remote MAC address. The VLAN ID range is from 1 to 4094.

1. Applicable only for Cisco ME 3400 Series and Cisco ME 3750 Ethernet Access Switches running Cisco IOS Release 12.2 (54) SE and later.

Step 4 To see the commands that will be applied on the device, click **Preview**.

You can view the commands in the Result tab. You can go back and make any required changes to the input parameters.

Step 5 To schedule the command, click the Scheduling tab. For more details on scheduling, see Scheduling a Command.

Step 6 To run the commands, click **Execute Now**.

You can view errors in the Result tab, if there are any.

Step 7 To close the dialog box, click **Close**.

Diagnose CFM with Traceroute Remote MEP with MPID

Use the **Diagnose CFM with Traceroute Remote MEP with MPID** command to traceroute the remote maintenance endpoint that supplies the maintenance point ID.

Step 1 In the inventory window, expand the Logical Inventory tree.

Step 2 Right-click the CFM node and choose **Commands > Diagnose > IEEE > Traceroute Remote MEP with MPID**. The Traceroute Remote MEP with MPID dialog box opens.

Step 3 By default, the General tab is selected. Enter values for the following parameters.

Input Parameter	Description
Remote MPID Address	Address of the remote maintenance endpoint identifier.
Domain Name	Name of the domain.
Option[1]	Select VLAN option for a VLAN configuration and Service option for Service configuration.
VLAN ID[1]	VLAN ID on which to apply the remote MPID address. The VLAN ID range is from 1 to 4094.

1. Applicable only for Cisco ME 3400 Series and Cisco ME 3750 Ethernet Access Switches running Cisco IOS Release 12.2 (54) SE and later.

Step 4 To see the commands that will be applied on the device, click **Preview**.

You can view the commands in the Result tab. You can go back and make any required changes to the input parameters.

Step 5 To schedule the command, click the Scheduling tab. For more details on scheduling, see Scheduling a Command.

Step 6 To run the commands, click **Execute Now**.

You can view errors in the Result tab, if there are any.

Step 7 To close the dialog box, click **Close**.



CHAPTER 19

Using Resilient Ethernet Protocol Command

Resilient Ethernet Protocol (REP) is a key part of the Carrier Ethernet and Mobile Transport over Packet (MToP) access network for fast and predictable convergence of Ethernet transport. REP is used primarily among access and aggregation devices that are connected in the Ethernet ring topologies.

Cisco Prime Network discovers and displays the following REP attributes in the Logical Inventory tree of the Prime Network Vision application:

- REP Segments. All of these segments are identified by a REP segment identifier that is locally configured on the network element. These segments, discovered on a switch, include the following attributes:
  - REP segment port 1 (interface name, port channel, or link aggregation group [LAG]).
  - REP segment port 2 (interface name, port channel, or LAG).
  - REP segment complete. This indicates whether the segment is complete so that no port is in the failed state.
- Global REP configuration details:
  - REP version used on the device.
  - REP administrative VLAN.
  - REP notification enabled.
  - Process and its status.
  - REP on EVC.
  - REP no neighbour.
  - REP on port-channel.

The following REP port attributes are modeled in Prime Network:

- REP segment ID.
- REP port ID.
- REP port state.
- REP port type (regular REP segment port, REP edge port, and primary REP edge port).
- REP port role (Open, Alternate, and Failed).
- Operational link state of the REP port (none, initDown, noNeighbour, oneWay, twoWay, flapping, wait, and unknown).

- Link status layer age-out timer (time, in milliseconds, for which the REP interface remains up without receiving a hello from a neighbor). REP must be configured on Layer 2 trunk ports (Network Node Interface (NNI) ports on access switches).
- VLAN load balancing configurations on REP primary edge ports. This includes:
  - REP alternate port (the port to be blocked for VLAN load balancing).
  - Blocked VLAN list.
  - Preempt timer.
- Remote device name, MAC and port interface.

REP details (port or interface) are not displayed in the Physical Inventory tree of the Cisco Prime Network Vision application.

You can view the REP port roles (open, alternate, and failed) in the Cisco Prime Network Vision map. The REP port role is displayed as a tool-tip between the REP enabled trunk ports in the Ethernet links. Using the Cisco Prime Network Vision map, you can identify if the segment is open or closed.

The map displays the forwarding direction (REP port roles) along the Physical links within VLAN overlays. It also displays the forwarding direction along the VLAN links among the switching elements within the VLAN logical domain topology.

In Prime Network 3.9, REP implementation supports the following faults:

- A REP Port Role change to Failed service event will be generated when a REP port role is change from Alternate or Open to Failed.
- A REP Port Role change to OK clearing service event will be generated when a REP port role is change from Failed to Alternate or Open.

Correlation to these service events to physical layer events (for example Link down or Port down will also be performed in Prime Network 3.9.

Supported Network Elements

You can run the REP commands on the following network elements:

- Cisco 7600 Series Routers
- Cisco MWR 2941 Mobile Wireless Routers
- Cisco ME 3600X and Cisco ME 3800X Carrier Ethernet Switches
- Cisco Catalyst 3750 Metro Series Switches
- Cisco ME 6524 Ethernet Switch
- Cisco Carrier Packet Transport (CPT) System
- All Cisco Catalyst Switches

See Part 1—Cisco VNEs for details on the software versions Prime Network supports for these network elements. To run the REP commands, the software on the network element must support the REP technology.

Displaying REP Segment Data

Use the **Show REP Segment Information** command to get the REP topology information for the specified segment.

Step 1 In the inventory window, expand the Logical Inventory tree and Resilient Ethernet Protocol node.

Step 2 Choose SegmentId and right-click **Commands > REP > Show REP Segment Information**. The Show REP Segment Information dialog box opens.

Step 3 By default, the General tab is selected. To see the commands that will be applied on the device, click **Preview**.

You can view the commands in the Result tab.

Step 4 To schedule the command, click the Scheduling tab. For more details on scheduling, see Scheduling a Command.

Step 5 To run the commands, click **Execute Now**.

The result contains information about all ports in the segment, including which one was configured and selected as the primary edge port.

Any errors are displayed in the Result tab.

Step 6 To close the dialog box, click **Close**.



CHAPTER 20

Using Cisco Carrier Grade NAT Commands

Carrier Grade NAT is a large-scale Network Address Translation (NAT) that provides translation of millions of private IPv4 addresses to public IPv4 addresses. These translations support subscribers and content providers with a bandwidth throughput of at least 10 Gbps full-duplex.

Carrier Grade NAT addresses the IPv4 address completion problem. It employs Network Address and Port Translation (NAPT) to aggregate many private IPv4 addresses into fewer public IPv4 addresses. For example, a single public IPv4 address with a pool of 32,000 port numbers supports 320 individual private IP subscribers, assuming that each subscriber requires 100 ports. Carrier Grade NAT also offers a way to implement a graceful transition to IPv6 addresses.

Carrier Grade NAT attributes and instances are configured as a CRS-ADVSVC-PLIM card on Cisco CRS-1 routers. To route internal public addresses to external public addresses, a VPN Routing and Forwarding (VRF) instance is created. Interfaces are created for the VRF at the subscriber-side (private) and the Internet-side (public). The VRF enables static or dynamic routing of protocols on the interfaces.

Cisco Prime Network displays the following attributes in the logical inventory of the Cisco Prime Network Vision application:

- Carrier Grade NAT Instance Name — The Carrier Grade NAT instance name identifies the Carrier Grade NAT instance. Cisco Prime Network supports the following instances for Carrier Grade NAT:
  - Stateful Address Translation- NAT44 Stateful
  - Stateless Address Translation- NAT 64 Stateless (X-LAT)
  - IPv6 rapid deployment (6rd)

Each Carrier Grade NAT instance has several attributes listed under them. The attributes are grouped under related categories. The categories and attributes are listed below:

- Preferred Location
  - Preferred Location—Hyperlink to the card in physical inventory
  - Preferred Location—Alternate name for card location
  - Location Type—Configured type of location
  - Redundancy Status
  - Service Infra Interface—Hyperlink to routing entity in logical inventory
- Address Pools
  - Inside VRF—Hyperlink to inside VRF in logical inventory
  - Outside VRF—Hyperlink to outside VRF in logical inventory
  - Address Pool—Range of IP Addresses for the instance

  - Address Family—Type of IP Address in this pool
- Associated Interfaces
  - Interface—SVI service-related hyperlink entry to logical inventory
- Statistics
  - Statistics Name
  - Statistics Value

Supported Network Elements

You can run the Carrier Grade NAT commands on the following network element:

- Cisco CRS Series Routers

  Cisco CRS series includes both the CRS-1 and CRS-3 Series Routers.

See Part 1—Cisco VNEs for details on the software versions Prime Network supports for these network elements. To run the Carrier Grade NAT commands, the software on the network element must support the Carrier Grade NAT technology.

The following commands facilitate the configuration of Carrier Grade NAT components:

- Configuring Carrier Grade NAT Instance, page 20-2
- Removing a Carrier Grade NAT instance, page 20-3
- Displaying Pool Utilization, page 20-3
- Adding 6rd Forwarding, page 20-4
- Adding Carrier Grade Nat 64 Forwarding, page 20-5

Configuring Carrier Grade NAT Instance

Use the **Add Static Port Forwarding** command to add a Carrier Grade NAT instance to the device.

Step 1 In the inventory window, expand the Logical Inventory tree and Carrier Grade NAT node.

Step 2 Right-click any Carrier Grade NAT instance and choose **Commands > Configure > Static Port Forwarding**.

The Static Port Forwarding dialog box opens.

Step 3 By default, the General tab is selected. Enter values for the following parameters.

Input Parameter	Description
Carrier Grade NAT Instance Name	Name of the Carrier Grade NAT instance.
Inside VRF Name	Name of the inside VPN routing and forwarding (VRF).
CGN Instance Name	Name of the CGN instance added under each Carrier Grade NAT Instance Name.
Address Family	Name of the IP address family. The default and only value is IPv4.

Input Parameter	Description
Protocol	Name of the protocol session. The values are TCP, UDP, or ICMP. The default value is TCP.
Address	Address of the inside VRF.
Port Number	Port number for the inside VRF. The range is from 1 to 65535.

Step 4 To see the commands that will be applied on the device, click **Preview**.

You can view the commands in the Result tab. You can go back and make any required changes to the input parameters.

Step 5 To schedule the command, click the Scheduling tab. For more details on scheduling, see Scheduling a Command.

Step 6 To run the commands, click **Execute Now**.

The newly added Carrier Grade NAT instance appears in the Carrier Grade NAT tree. Any errors are displayed in the Result tab.

Step 7 To close the dialog box, click **Close**.

Removing a Carrier Grade NAT instance

Use the **Static Port Forwarding** command to remove a Carrier Grade NAT instance from the device.

Step 1 In the inventory window, expand the Logical Inventory tree and Carrier Grade NAT node.

Step 2 Right-click the Carrier Grade NAT instance that you want to remove and choose **Commands > Delete > Static Port Forwarding**.

Step 3 The Static Port Forwarding dialog box opens. By default, the General tab is selected.

Step 4 To see the commands that will be applied on the device, click **Preview**.

You can view the commands in the Result tab.

Step 5 To schedule the command, click the Scheduling tab. For more details on scheduling, see Scheduling a Command.

Step 6 To run the commands, click **Execute Now**.

The Carrier Grade NAT instance is no longer visible under the Carrier Grade NAT tree. Any errors are displayed in the Result tab.

Step 7 To close the dialog box, click **Close**.

Displaying Pool Utilization

Use the **Pool Utilization** command to view the ports that the Carrier Grade NAT instances use in the given address range.

Step 1 In the inventory window, expand the Logical Inventory tree and Carrier Grade NAT node.

Step 2 Right-click the Carrier Grade NAT instance and choose **Commands > Show > Pool Utilization.**

The Pool Utilization dialog box opens.

Step 3 By default, the General tab is selected. Enter values for the following parameters.

Input Parameter	Description
CGN Instance Name	Name of the CGN instance.
Inside VRF Name	Name of the inside VRF.
Start Address	Starting IPv4 address in the range.
End Address	Ending IPv4 address in the range.

Step 4 To see the commands that will be applied on the device, click **Preview**.

You can view the commands in the Result tab. You can go back and make any required changes to the input parameters.

Step 5 To schedule the command, click the Scheduling tab. For more details on scheduling, see Scheduling a Command.

Step 6 To run the commands, click **Execute Now**.

Any errors are displayed in the Result tab.

Step 7 To close the dialog box, click **Close**.

Adding 6rd Forwarding

Use the **Add 6rd Forwarding** command to add a 6rd forwarding.

Step 1 In the inventory window, expand the Logical Inventory tree and Carrier Grade NAT node.

Step 2 Right-click the Carrier Grade NAT instance and choose **Commands > Configure > Static Port Forwarding.**

The Add 6rd Forwarding dialog box opens.

Step 3 By default, the General tab is selected. Enter values for the following parameters.

Input Parameter	Description
CGN Instance Name	Name of the CGN instance.
6rd Name	Name of the 6rd instance.
ServiceAppipv4	Name of serviceApp Ipv4 interface.
ServiceAppipv6	Name of serviceApp Ipv6 interface.

Step 4 To see the commands that will be applied on the device, click **Preview**.

You can view the commands in the Result tab. You can go back and make any required changes to the input parameters.

Step 5 To schedule the command, click the Scheduling tab. For more details on scheduling, see Scheduling a Command.

Step 6 To run the commands, click **Execute Now**.

Any errors are displayed in the Result tab.

Step 7 To close the dialog box, click **Close**.

Adding Carrier Grade Nat 64 Forwarding

Use the **Add Nat 64 Forwarding** command to add a 6rd forwarding.

Step 1 In the inventory window, expand the Logical Inventory tree and Carrier Grade NAT node.

Step 2 Right-click the Carrier Grade NAT instance and choose **Commands > Configure > Static Port Forwarding.**

The Add 6rd Forwarding dialog box opens.

Step 3 By default, the General tab is selected. Enter values for the following parameters.

Input Parameter	Description
CGN Instance Name	Name of the CGN instance.
Nat 64 Name	Name of the Nat 64 instance.
ServiceAppipv4	Name of serviceApp Ipv4 interface.
ServiceAppipv6	Name of serviceApp Ipv6 interface.

Step 4 To see the commands that will be applied on the device, click **Preview**.

You can view the commands in the Result tab. You can go back and make any required changes to the input parameters.

Step 5 To schedule the command, click the Scheduling tab. For more details on scheduling, see Scheduling a Command.

Step 6 To run the commands, click **Execute Now**.

Any errors are displayed in the Result tab.

Step 7 To close the dialog box, click **Close**.



CHAPTER 21

Using Pseudowire Virtual Circuit Connectivity Verification Commands

Pseudowire is a tunnel established between two provider edge (PE) routers to transport Layer 2 protocol data units (PDUs) across a public switched network (PSN). A multisegment pseudowire is a static or dynamically configured set of two or more contiguous pseudowire segments. These segments act as a single pseudowire, allowing you to:

- Manage the end-to-end service by separating administrative or provisioning domains.
- Keep IP addresses of PE nodes private across interautonomous system (inter-AS) boundaries.
- Use IP address of autonomous system boundary routers (ASBRs) and treat them as pseudowire aggregation routers. The ASBRs join the pseudowires of the two domains.

A multisegment pseudowire can span either an inter-AS boundary or two multiprotocol label switching (MPLS) networks.

Cisco Prime Network supports the discovery and modeling of Any Transport over MPLS (AToM) and Ethernet over MPLS (EoMPLS) domains that span multisegment pseudowires.

Cisco Prime Network also extends Virtual Circuit Connectivity Verification (VCCV) to support end-to-end connectivity verification across a pseudowire switching point and to provide the ability to trace the path of a multisegment pseudowire over any number of segments. You can use the ping command to verify the connectivity between any set of PE routers in the pseudowire path. This feature allows you to verify end-to-end VC connectivity in the case where the pseudowire spans multiple administrative domains and associated pseudowire switching points.

Cisco Prime Network 3.9 supports:

- Single segment pseudowires with no redundancy
- Single segment pseudowires with redundancy
- Single segment pseudowires with multiple backups
- Multi-segment pseudowires with no redundancy

Cisco Prime Network discovers and displays the pseudowires configured on a selected network element in the Logical Inventory tree of the Cisco Prime Network Vision application. Each pseudowire is configured with the following set of attributes:

- Name—The name of the pseudowire.
- Multi-segment Pseudowire—Whether or not the pseudowire is multi-segment: True or False.
- System Name—The name of the system on which the pseudowire is configured.
- Pseudowire Type—The type of pseudowire, such as Ethernet, Ethernet Tagged, or Point-to-Point Protocol (PPP).

When you select the pseudowire on the Logical Inventory tree, you can view the list of pseudowire tunnels or interfaces configured on the selected network element in the Tunnel Edges table on the content area of the Cisco Prime Network Vision application. The following tunnel or interface attributes are modeled in Cisco Prime Network:

- Port—Virtual Switch Interface (VSI) on which the tunnel is configured.
- Peer VC Label—The MPLS label that is used by the router to identify or access the tunnel.
- Tunnel Status—Operational state of the tunnel: Up or Down.
- Local VC Label—The MPLS label that is used to identify or access the tunnel.
- Local Router IP—The IP address of the tunnel endpoint, which is used as the MPLS router identifier.
- Tunnel ID—The tunnel identifier.
- Peer Router IP—The IP address of the peer tunnel endpoint, which is used as the MPLS router identifier.
- Local MTU—The size, in bytes, of the MTU on the local interface.
- Remote MTU—The size, in bytes, of the MTU on the remote interface.
- Signaling Protocol—The protocol used by MPLS to build the tunnel.
- Pseudowire Type—The type of pseudowire, such as Ethernet, Ethernet Tagged, or PPP.

Supported Network Elements

You can run the psuedowire commands on all Cisco IOS and Cisco IOS XR devices that support pseudowire technology, such as

- Cisco 7200 series routers
- Cisco 7600 series routers
- Cisco ASR 9000 series aggregation services routers
- Cisco XR 12000 series routers
- Cisco ME 3600X and Cisco ME 3800X Carrier Ethernet Switches
- Cisco Carrier Packet Transport (CPT) System

See Part 1—Cisco VNEs for details on the software versions Prime Network supports for these network elements. To run the pseudowire commands, the software on the network element must support the pseudowire technology.

Pinging the Peer Router from a Single Segment or Multisegment Pseudowire

Use the **Ping Pseudowire** command to ping the peer router with a tunnel ID from a single or multisegment pseudowire. This command can be used to verify connectivity between any set of PE routers in the pseudowire path. For a multisegment pseudowire this command can be used to verify that all the segments of the multisegment pseudowire are operating. You can use this command to verify connectivity at the following pseudowire points:

- From one end of the pseudowire to the other

- From one of the pseudowires to a specific segment
- The segment between two adjacent PE routers

You can choose to ping the peer router by default or provide the IP of the required destination router to ping.

Note The **Ping Pseudowire** command applies to all Cisco IOS and Cisco IOS XR devices that support pseudowire technology.

Step 1 In the inventory window, expand the Logical Inventory tree and choose Pseudowires.

The Tunnel Edges table is displayed on the content area, listing the pseudowire tunnels or interfaces configured on the selected element.

Step 2 Right-click the required interface and choose **Commands > Configure > Ping Pseudowire**. The Ping Pseudowire dialog box opens.

By default, the General tab is displayed. Enter values for the following parameters.

Input Parameter	Description
Multisegment Ping[1]	Select **Enable** or **Disable** to activate or deactivate multisegment pinging.
Ping with default Destination IP and VC-ID	Check this to ping the peer router by default. The destination router is identified from the peer router IP specified in the Tunnel Edges table.
Destination IP address	The IP address of the router to ping. Leave this blank if the Ping with default Destination IP and VC-ID check box is selected.
VC-ID	The pseudowire virtual circuit (VC) identifier. Leave this blank if the Ping with default Destination IP and VC-ID check box is selected.

1. This parameter is available only for Cisco IOS XR devices.

Step 3 To see the command that will be applied on the device, click **Preview**.

Step 4 To schedule the command, click the Scheduling tab. For more details on scheduling, see Scheduling a Command.

Step 5 To run the command, click **Execute**.

Any errors are displayed in the Result tab.

Step 6 To close the dialog box, click **Close**.

Displaying Pseudowire Information

Use the **Display Pseudowire** command to show the MPLS Layer 2 (L2) transport binding using tunnel identifier. MPLS L2 transport binding allows you to identify the VC label binding information. This command can be used to display information about the pseudowire switching point.

Note The **Display Pseudowire** command applies to all Cisco IOS and Cisco IOS XR devices that support pseudowire technology.

Step 1 In the inventory window, expand the Logical Inventory tree and choose Pseudowires.

The Tunnel Edges table is displayed on the content area, listing the pseudowire tunnels or interfaces configured on the selected element.

Step 2 Right-click the required interface and choose **Commands > Show > Display Pseudowire**. The Display Pseudowire dialog box opens.

By default, the Result tab is displayed. The command does not require any input parameters.

Step 3 To see the command that will be applied on the device, click **Preview**.

You can view the command in the Result tab. You can go back and modify the parameter setting if required.

Step 4 To schedule the command, click the Scheduling tab. For more details on scheduling, see Scheduling a Command.

Step 5 To run the command, click **Execute Now**.

Any errors are displayed in the Result tab.

Step 6 To close the dialog box, click **Close**.



CHAPTER 22

Using Ethernet Operations, Administration and Maintenance Operations Commands

Ethernet Operations, Administration, and Maintenance (E-OAM) consists of three main feature sets:

- IEEE 802.1ag and ITU-T Y.1731 Connectivity Fault Management (CFM).
- IEEE 802.3ah Ethernet OAM discovery, link monitoring, remote fault detection, and remote loopback.
- Ethernet Local Management Interface (Ethernet LMI), which allows a customer edge (CE) network element to obtain user network interface (UNI) and Ethernet virtual connection (EVC) status and service attribute information from the service provider edge.

The IOS OAM manager streamlines interaction between OAM protocols, and handles the interaction between CFM and Ethernet LMI. Ethernet LMI interaction with the OAM manager is unidirectional, running only from the OAM manager to Ethernet LMI on the U-PE side of the switch. Information is exchanged either as a result of a request from Ethernet LMI or triggered by the OAM manager when it receives notification of a change from the OAM protocol. The following type of information is relayed:

- EVC name and availability status
- Remote UNI name and status
- Remote UNI counts

Ethernet LMI is typically disabled by default.

Link (802.3AH) OAM (L-OAM) can be implemented on any full-duplex point-to-point or emulated point-to-point Ethernet link. The frames (OAM Protocol Data Units [OAMPDUs]) cannot propagate beyond a single hop within an Ethernet network and have modest bandwidth requirements (frame transmission rate is limited to a maximum of 10 frames per second). The major features covered by the E-OAM protocol are discovery, link monitoring, remote fault detection, and remote loopback.

Supported Network Elements

You can run the E-OAM commands on the following network elements:

- Cisco 7600 Series Routers
- Cisco Catalyst 3750 Metro Series Switches
- Cisco Catalyst 6500 Series (IOS) Switches
- Cisco ME 3400 Series Ethernet Access Switches
- Cisco MWR 2941 Mobile Wireless Routers

- Cisco ASR 9000 Series Aggregation Services Routers
- Cisco 2900 Series Integrated Services Routers
- Cisco 3900 Series Integrated Services Routers
- Cisco ME 3600X Ethernet Access Switches
- Cisco ME 3800X Carrier Ethernet Switch Routers
- Cisco 3900 Series Integrated Services Routers
- Cisco 2900 Series Integrated Services Routers
- Cisco 1900 Series Integrated Services Routers
- Cisco ASR 903 Series Aggregation Services Routers
- Cisco Carrier Packet Transport (CPT) System

See Part 1—Cisco VNEs for details on the software versions Prime Network supports for these network elements. To run the E-OAM commands, the software on the network element must support the E-OAM technology.

Configuring L-OAM Components

The following sections explain how to configure L-OAM components:

- Applying Template on an Interface, page 22-2
- Create Template, page 22-3
- Disabling OAM on an Interface, page 22-4
- Enabling OAM on an Interface, page 22-5
- Configuring OAM Parameters on an Interface, page 22-5
- Starting the Remote Loopback, page 22-6
- Stopping the Remote Loopback, page 22-6

Note In the GUI, parameters that are displayed in bold text are mandatory.

Applying Template on an Interface

Use the **Applying Template on Interface** command to create and apply a template to an interface.

Step 1 In the inventory window, expand the Logical Inventory tree.

Step 2 Right-click the OAM node and choose **Commands > Assign Template on Interface**. The Assign Template on interface dialog box opens.

Step 3 By default, the General tab is selected. Enter values for the following parameters.

Input Parameter	Description
Interface Name	Name of the interface.
Template Name	Name of the template.

Step 4 To see the commands that will be applied on the device, click **Preview**.

You can view the commands in the Result tab. You can go back and make any required changes to the input parameters.

Step 5 To schedule the command, click the Scheduling tab. For more details on scheduling, see Scheduling a Command.

Step 6 To run the commands, click **Execute Now**.

Any errors are displayed in the Result tab.

Step 7 To close the dialog box, click **Close**.

Create Template

Use the **Create Template** command to create and apply a template to an interface.

Step 1 In the inventory window, expand the Logical Inventory tree.

Step 2 Right-click the OAM node and choose **Commands > Create Template**. The Create Template dialog box opens.

Step 3 By default, the General tab is selected. Enter values for the following parameters.

Input Parameter	Description
Template Name	Name of the template.
Symbol-Period Threshold Low	The range is from 1 to 65535. The low threshold value must be lower than the high threshold.
Symbol-Period Threshold High	The range is from 1 to 65535. The low threshold value must be lower than the high threshold.
Frame Window	The range is from 10 to 600, which represents milliseconds in multiples of 100. The default is 100.
Frame Threshold Low	The range is from 1 to 900. The default value is 1.
Frame Threshold High	The range is from 1 to 900. The default value is 1.
Frame-Period Window	The range is from 100 to 65535, which represents multiples of 10000 frames. The default is 1000.
Frame-Period Threshold Low	The range is from 0 to 65535. The default is 1.
Frame-Period Threshold High	The range is from 0 to 65535.
Frame-Seconds Window	The range is from 100 to 9000, which represents a multiple of 100 milliseconds. The default is 1000.
Frame-Seconds Threshold Low	The range is from 1 to 900. The default is 1.
Frame-Seconds Threshold High	The range is from 1 to 900.
Receive-Crc Window	The range is 10 to 1800 and represents the number of milliseconds in multiples of 100. The default is 100.
Receive-Crc Threshold High	The range is 1 to 65535.

Input Parameter	Description
Transmit-Crc Window	The range is from 10 to 1800.
Transmit-Crc Threshold High	The range is from 1 to 65535.

Step 4 To see the commands that will be applied on the device, click **Preview**.

You can view the commands in the Result tab. You can go back and make any required changes to the input parameters.

Step 5 To schedule the command, click the Scheduling tab. For more details on scheduling, see Scheduling a Command.

Step 6 To run the commands, click **Execute Now**.

Any errors are displayed in the Result tab.

Step 7 To close the dialog box, click **Close**.

Disabling OAM on an Interface

Use the **Disable OAM on Interface** command to disable L-OAM on an interface.

Step 1 In the inventory window, expand the Logical Inventory tree.

Step 2 Right-click the OAM node and choose **Commands > Disable OAM on Interface**. The Disable OAM on Interface dialog box opens.

Step 3 By default, the General tab is selected. Enter a value for the following parameter.

Input Parameter	Description
Interface Name	Name of the interface.

Step 4 To see the commands that will be applied on the device, click **Preview**.

You can view the commands in the Result tab. You can go back and make any required changes to the input parameters.

Step 5 To schedule the command, click the Scheduling tab. For more details on scheduling, see Scheduling a Command.

Step 6 To run the commands, click **Execute Now**.

Any errors are displayed in the Result tab.

Step 7 To close the dialog box, click **Close**.

Enabling OAM on an Interface

Use the **Enable OAM on Interface** command to enable L-OAM on an interface.

Step 1 In the inventory window, expand the Logical Inventory tree.

Step 2 Right-click the OAM node and choose **Commands > Enable OAM on Interface**. The Enable OAM on Interface dialog box opens.

Step 3 By default, the General tab is selected. Enter a value for the following parameter.

Input Parameter	Description
Interface Name	Name of the interface.

Step 4 To see the commands that will be applied on the device, click **Preview**.

You can view the commands in the Result tab. You can go back and make any required changes to the input parameters.

Step 5 To schedule the command, click the Scheduling tab. For more details on scheduling, see Scheduling a Command.

Step 6 To run the commands, click **Execute Now**.

Any errors are displayed in the Result tab.

Step 7 To close the dialog box, click **Close**.

Configuring OAM Parameters on an Interface

Use the **Configure OAM Parameter on Interface** command to configure L-OAM parameters on an interface.

Step 1 In the inventory window, expand the Logical Inventory tree.

Step 2 Right-click the OAM node and choose **Commands > Configure OAM Parameter on Interface**. The Configure OAM Parameter on Interface dialog box opens.

Step 3 By default, the General tab is selected. Enter values for the following parameters.

Input Parameter	Description
Interface Name	Name of the interface.
Max-Rate	Maximum number of OAM PDUs sent per second. The range is from 1 to 10.
Min-Rate	Minimum transmission rate, in seconds, when one OAM PDU is sent per second. The range is from 1 to 10.
Mode	Sets the OAM client mode to active or passive.
Remote Loopback	Supports or Unsupports Ethernet remote loopback on the interface.
Time Out	Timeout range, from 2 to 30.

Step 4 To see the commands that will be applied on the device, click **Preview**.

You can view the commands in the Result tab. You can go back and make any required changes to the input parameters.

Step 5 To schedule the command, click the Scheduling tab. For more details on scheduling, see Scheduling a Command.

Step 6 To run the commands, click **Execute Now**.

Any errors are displayed in the Result tab.

Step 7 To close the dialog box, click **Close**.

Starting the Remote Loopback

Use the **Start Remote Loopback** command to turn on Link OAM remote loopback on an interface.

Step 1 In the inventory window, expand the Logical Inventory tree.

Step 2 Right-click the OAM node and choose **Commands > Start Remote Loopback**.

The Start Remote Loopback dialog box opens.

Step 3 By default, the General tab is selected. Enter values for the following parameters.

Input Parameter	Description
Interface Name	Name of the interface.

Step 4 To see the commands that will be applied on the device, click **Preview**.

You can view the commands in the Result tab. You can go back and make any required changes to the input parameters.

Step 5 To schedule the command, click the Scheduling tab. For more details on scheduling, see Scheduling a Command.

Step 6 To run the commands, click **Execute Now**.

Any errors are displayed in the Result tab.

Step 7 To close the dialog box, click **Close**.

Stopping the Remote Loopback

Use the **Stop Remote Loopback** command to turn off Link OAM remote loopback on an interface.

Step 1 In the inventory window, expand the Logical Inventory tree.

Step 2 Right-click the OAM node and choose **Commands > Stop Remote Loopback**.

The Stop Remote Loopback dialog box opens.

Step 3 By default, the General tab is selected. Enter values for the following parameters.

Input Parameter	Description
Interface Name	Name of the interface.

Step 4 To see the commands that will be applied on the device, click **Preview**.

You can view the commands in the Result tab. You can go back and make any required changes to the input parameters.

Step 5 To schedule the command, click the Scheduling tab. For more details on scheduling, see Scheduling a Command.

Step 6 To run the commands, click **Execute Now**.

Any errors are displayed in the Result tab.

Step 7 To close the dialog box, click **Close**.



CHAPTER 23

Using Ethernet Local Management Interface Commands

Ethernet Operations, Administration, and Maintenance (E-OAM) consists of three main feature sets:

- IEEE 802.1ag and ITU-T Y.1731 Connectivity Fault Management (CFM).
- IEEE 802.3ah Ethernet OAM discovery, link monitoring, remote fault detection, and remote loopback.
- Ethernet Local Management Interface (Ethernet LMI), which allows a customer edge (CE) network element to obtain user network interface (UNI) and Ethernet virtual circuit (EVC) status and service attribute information from the service provider edge.

Ethernet LMI is a protocol between the CE network element and the provider edge (PE) network element. It runs only on the PE-CE UNI link and notifies the CE of connectivity status and configuration parameters of Ethernet services available on the CE port. Ethernet LMI interoperates with an OAM protocol, such as CFM, that runs within the provider network to collect OAM status. CFM runs at the provider maintenance level. Ethernet LMI relies on the OAM Ethernet Infrastructure (EI) to work with CFM for end-to-end status of EVCs across CFM domains.

The IOS OAM manager streamlines interaction between OAM protocols, and handles the interaction between CFM and Ethernet LMI. Ethernet LMI interaction with the OAM manager is unidirectional, running only from the OAM manager to Ethernet LMI on the U-PE side of the switch. Information is exchanged either as a result of a request from Ethernet LMI or triggered by the OAM manager when it receives notification of a change from the OAM protocol. The following type of information is relayed:

- EVC name and availability status
- Remote UNI name and status
- Remote UNI counts

Ethernet LMI is typically disabled by default.

Supported Network Elements

You can run the Ethernet LMI commands on the following network elements:

- Cisco 7600 Series Routers
- Cisco Catalyst 3750 Metro Series Switches
- Cisco Catalyst 6500 Series (IOS) Switches
- Cisco ME3600X and Cisco ME3800X Carrier Ethernet Switches

- Cisco ME 3400 Series Ethernet Access Switches
- Cisco MWR 2941 Mobile Wireless Routers
- Cisco ASR9000 Series Routers

See Part 1—Cisco VNEs for details on the software versions Prime Network supports for these network elements. To run the Ethernet LMI commands, the software on the network element must support the Ethernet LMI technology.

Configuring Ethernet LMI Components

The following sections explain how to configure Ethernet LMI components:

- Enabling Ethernet LMI Globally, page 23-2
- Configuring Multipoint-to-Multipoint or Point-to-Point Ethernet Virtual Connection, page 23-3
- Configuring UNI on an Interface, page 23-3
- Enabling Ethernet LMI on an Interface, page 23-4
- Configuring the Service Instance VLAN ID on an Interface, page 23-5

Note In the GUI, parameters that are displayed in bold text are mandatory.

Enabling Ethernet LMI Globally

Use the **Enable E-LMI Global** command to globally enable Ethernet LMI on all interfaces.

Note You can not execute the **Enable E-LMI Global** command on network elements that run on Cisco IOS XR software.

Step 1 In the inventory window, expand the Logical Inventory tree.

Step 2 Right-click the Ethernet LMI node and choose **Commands > Enable > Global E-LMI**. The Global Ethernet LMI dialog box opens.

The command enables Ethernet LMI on all interfaces and does not require any input parameters.

Step 3 To schedule the command, click the Scheduling tab. For more details on scheduling, see Scheduling a Command.

Step 4 To run the command, click **Execute Now**.

Any errors are displayed in the Result tab.

Step 5 To close the dialog box, click **Close**.

Configuring Multipoint-to-Multipoint or Point-to-Point Ethernet Virtual Connection

Use the **Configure MultiPoint To MultiPoint or Point To Point EVC** command to configure multipoint-to-multipoint or point-to-point Ethernet virtual connection (EVC).

Step 1 In the inventory window, expand the Logical Inventory tree.

Step 2 Right-click the Ethernet LMI node and choose **Commands > Configure MultiPoint To MultiPoint or Point To Point EVC**. The Configure MultiPoint To MultiPoint or Point To Point EVC dialog box opens.

Step 3 By default, the General tab is selected. Enter values for the following parameters.

Input Parameter	Description
Evc Name	Name of the Ethernet virtual connection.
Uni Count No	The range of the Unified network interface(UNI) is 2 to 1024; the default is 2. If you enter a value of 2, you have the option to select point-to-multipoint service. If you configure a value of 3 or greater, the service is point-to-multipoint.
Vlans to apply cross check to ([1-4094])	VLAN ID range from 1 to 4094.
Domain Name	Name of the domain.

Step 4 To see the commands that will be applied on the device, click **Preview**.

You can view the commands in the Result tab. You can go back and make any required changes to the input parameters.

Step 5 To schedule the command, click the Scheduling tab. For more details on scheduling, see Scheduling a Command.

Step 6 To run the commands, click **Execute Now**.

Any errors are displayed in the Result tab.

Step 7 To close the dialog box, click **Close**.

Configuring UNI on an Interface

Use the **Configure UNI in an Interface** command to configure UNI on an interface.

Step 1 In the inventory window, expand the Logical Inventory tree.

Step 2 Right-click the Ethernet LMI node and choose **Commands > Configure UNI in an Interface**. The Configure UNI in an Interface dialog box opens.

Step 3 By default, the General tab is selected. Enter values for the following parameters.

Input Parameter	Description
Interface Name	Name of the interface.
Uni Id	Unified network interface identifier.

Step 4 To see the commands that will be applied on the device, click **Preview**.

You can view the commands in the Result tab. You can go back and make any required changes to the input parameters.

Step 5 To schedule the command, click the Scheduling tab. For more details on scheduling, see Scheduling a Command.

Step 6 To run the commands, click **Execute Now**.

Any errors are displayed in the Result tab.

Step 7 To close the dialog box, click **Close**.

Enabling Ethernet LMI on an Interface

Use the **Enable On Interface** command to configure Ethernet LMI on the interface. If Ethernet LMI is disabled globally, you can use this command to enable it on specific interfaces.

Step 1 In the inventory window, expand the Logical Inventory tree.

Step 2 Right-click the Ethernet LMI node and choose **Commands > Enable On Interface**. The Enable On Interface dialog box opens.

Step 3 By default, the General tab is selected. Enter a value for the following parameter.

Input Parameter	Description
Interface Name	Name of the interface.

Step 4 To see the commands that will be applied on the device, click **Preview**.

You can view the commands in the Result tab. You can go back and make any required changes to the input parameters.

Step 5 To schedule the command, click the Scheduling tab. For more details on scheduling, see Scheduling a Command.

Step 6 To run the commands, click **Execute Now**.

Any errors are displayed in the Result tab.

Step 7 To close the dialog box, click **Close**.

Configuring the Service Instance VLAN ID on an Interface

Use the **Configure Service Instance Vlan Id on Interface** command to configure an Ethernet service instance on the interface.

Step 1 In the inventory window, expand the Logical Inventory tree.

Step 2 Right-click the Ethernet LMI node and choose **Commands > Configure Service Instance Vlan Id on Interface**. The Configure Service Instance Vlan Id on Interface dialog box opens.

Step 3 By default, the General tab is selected. Enter values for the following parameters.

Input Parameter	Description
Interface Name	Name of the interface.
Service Instance Id	Per-interface Ethernet service instance identifier that does not map to a VLAN. The identifier is from 1 to 8000.
Evc Name	Name of the Ethernet virtual connection.
VLAN to EVC Map	The VLAN EVC map value. Values include: • Value in the range1 to 4094 • Any • Default • Untagged

Step 4 To see the commands that will be applied on the device, click **Preview**.

You can view the commands in the Result tab. You can go back and make any required changes to the input parameters.

Step 5 To schedule the command, click the Scheduling tab. For more details on scheduling, see Scheduling a Command.

Step 6 To run the commands, click **Execute Now**.

Any errors are displayed in the Result tab.

Step 7 To close the dialog box, click **Close**.



CHAPTER 24

Using MPLS-TP Commands

MPLS-TP is a carrier-grade packet transport technology that enables the move from SONET and SDH time-division multiplexing (TDM) to packet switching. MPLS-TP enables MPLS to be deployed in a transport network and to operate similarly to existing transport technologies. MPLS-TP enables MPLS to support packet transport services with a degree of predictability that is similar to the existing transport networks.

The goal of MPLS-TP is to provide connection-oriented transport for packet and TDM services over networks leveraging the widely deployed MPLS technology. Operations, administration, and maintenance (OAM) and resiliency features are defined and implemented in MPLS-TP to ensure:

- Scalable operations
- High availability
- Performance monitoring
- Multidomain support
- Carrier-grade packet transport networks

An MPLS-TP tunnel has:

- Two endpoints where the tunnel is configure as a tunnel interface
- One or two bidirectional label switched path (LSP) pairs between the endpoints. If there are two pairs, then one is a working path, the second a protection path.
- Pair of bidirectional LSPs that are congruent.
- Where there is no control plane, the LSPs are configured at all the midpoints.
- The MPLS-TP tunnel is used to carry pseudowires.

Supported Network Elements

You can run the MPLS-TP commands on the following network elements:

- Cisco 7600 Series Routers
- Cisco Carrier Packet Transport (CPT) System
- Cisco ASR 9000 Series Aggregation Services Routers
- Cisco ASR 903 Series Aggregation Services Routers

Configuring MPLS-TP Components

The following commands facilitate the configuration of MPLS-TP components:

- Tunnel Ping, page 24-2
- Tunnel Trace, page 24-3
- LSP Path Lockout, page 24-3
- LSP Ping, page 24-4
- Lsp Trace, page 24-5
- Lsp Lockout, page 24-5
- Lsp Path No Lockout, page 24-6
- Add Global Configuration, page 24-6
- Remove Global Configuration, page 24-7
- Update Global Configuration, page 24-8
- Add Link Configuration, page 24-8
- Remove Link Configuration, page 24-9
- Add BFD Template Configuration, page 24-10
- Remove BFD Template Configuration, page 24-11
- Show BFD Template, page 24-11
- Show BFD Template At Tunnel, page 24-12
- Add Label Range Configuration, page 24-12
- Remove Label Range Configuration, page 24-13
- BFD Global Configuration, page 24-14

Tunnel Ping

Use the **Tunnel Ping** command to ping the MPLS-TP tunnel.

Step 1 In the inventory window, expand the Logical Inventory tree and MPLS-TP node.

Step 2 Right-click and choose **MPLS-TP Global > Commands > Configuration > Tunnel Ping.**

Step 3 Enter values for the following parameters.

Input Parameter	Description
TunnelId	The unique identifier of the MPLS-TP tunnel. The range of the tunnel is from 1 to 65535
LSP Path	The LSP path information- path, working.

Step 4 To see the commands that will be applied on the device, click **Preview**.

You can view the commands in the Result tab. You can go back and make any required changes to the input parameters.

Step 5 To schedule the command, click the Scheduling tab. For more details on scheduling, see Scheduling a Command.

Step 6 To run the commands, click **Execute Now**.

Any errors are displayed in the Result tab.

Step 7 To close the dialog box, click **Close**.

Tunnel Trace

Use the **Tunnel Trace** command to trace the MPLS-TP tunnel.

Step 1 In the inventory window, expand the Logical Inventory tree and MPLS-TP node.

Step 2 Right-click and choose **MPLS-TP Global > Commands > Configuration > Tunnel Trace**

Step 3 Enter values for the following parameters.

Input Parameter	Description
TunnelID	The unique identifier of the MPLS-TP tunnel. The range of the tunnel is from 1 to 65535
LSP Path	The LSP path information.

Step 4 To see the commands that will be applied on the device, click **Preview**.

You can view the commands in the Result tab. You can go back and make any required changes to the input parameters.

Step 5 To schedule the command, click the Scheduling tab. For more details on scheduling, see Scheduling a Command.

Step 6 To run the commands, click **Execute Now**.

Any errors are displayed in the Result tab.

Step 7 To close the dialog box, click **Close**.

LSP Path Lockout

Use the **LSP Path Lockout** command to lock the LSP path.

Step 1 In the inventory window, expand the Logical Inventory tree and MPLS-TP node.

Step 2 Right-click and choose **MPLS-TP Global > Commands > Configuration > LSP path lockout.**

Step 3 Enter values for the following parameters.

Input Parameter	Description
TunnelID	The unique identifier of the MPLS-TP tunnel. The range of the tunnel is from 1 to 65535
LSP Path	The LSP path information- Protect LSP, Working LSP.
Lockout	The lockout of the LSP is signaled from one endpoint to the other.

Step 4 To see the commands that will be applied on the device, click **Preview**.

You can view the commands in the Result tab. You can go back and make any required changes to the input parameters.

Step 5 To schedule the command, click the Scheduling tab. For more details on scheduling, see Scheduling a Command.

Step 6 To run the commands, click **Execute Now**.

Any errors are displayed in the Result tab.

Step 7 To close the dialog box, click **Close**.

Note You can acccess the Lsp Path Lock Out command at both the Lsp tunnel level and the end point level. While executing the commands in the end point level, Prime Network retrieves the values from the IMO object. You must specify if the Lsp is protected or working Lsp while executing the commands in the tunnel level.

LSP Ping

Use the LSP Ping command to ping the LSP tunnel interface.

Step 1 In the inventory window, expand the Logical Inventory tree and MPLS-TP node.

Step 2 Right-click and choose **MPLS-TP Global > Commands > Configuration > LSP ping.**

Step 3 To see the commands that will be applied on the device, click **Preview**.

You can view the commands in the Result tab. You can go back and make any required changes to the input parameters.

Step 4 To schedule the command, click the Scheduling tab. For more details on scheduling, see Scheduling a Command.

Step 5 To run the commands, click **Execute Now**.

Any errors are displayed in the Result tab.

Step 6 To close the dialog box, click **Close**.

Lsp Trace

Use the LSP trace command to trace the LSP tunnel interface.

Step 1 In the inventory window, expand the Logical Inventory tree and MPLS-TP node.

Step 2 Right-click and choose **MPLS-TP Global > Commands > Configuration > LSP Trace.**

Step 3 To see the commands that will be applied on the device, click **Preview**.

You can view the commands in the Result tab. You can go back and make any required changes to the input parameters.

Step 4 To schedule the command, click the Scheduling tab. For more details on scheduling, see Scheduling a Command.

Step 5 To run the commands, click **Execute Now**.

Any errors are displayed in the Result tab.

Step 6 To close the dialog box, click **Close**.

Lsp Lockout

Use the LSP Lockout command to perform an LSP lockout.

Step 1 In the inventory window, expand the Logical Inventory tree and MPLS-TP node.

Step 2 Right-click and choose **MPLS-TP Global > Commands > Configuration > LSP Lockout.**

Step 3 Enter values for the following parameters.

Input Parameter	Description
LSP Path	The LSP path information- Protect LSP, Working LSP.

Step 4 To see the commands that will be applied on the device, click **Preview**.

You can view the commands in the Result tab. You can go back and make any required changes to the input parameters.

Step 5 To schedule the command, click the Scheduling tab. For more details on scheduling, see Scheduling a Command.

Step 6 To run the commands, click **Execute Now**.

Any errors are displayed in the Result tab.

Step 7 To close the dialog box, click **Close**.

Note You can acccess the Lsp Lock Out command at both the Lsp tunnel level and the end point level. While executing the commands in the end point level, Prime Network retrieves the values from the IMO object. You must specify if the Lsp is protected or working Lsp while executing the commands in the tunnel level.

Lsp Path No Lockout

Use the lsp no lock out command to remove a lock out of the lsp path.

Step 1 In the inventory window, expand the Logical Inventory tree and MPLS-TP node.

Step 2 Right-click and choose **MPLS-TP Global > Commands > Configuration > LSP Path No Lockout.**

Step 3 Enter values for the following parameters

Input Parameter	Description
LSP Path	The LSP path information- Protect LSP, Working LSP.

Step 4 To see the commands that will be applied on the device, click **Preview**.

You can view the commands in the Result tab. You can go back and make any required changes to the input parameters.

Step 5 To schedule the command, click the Scheduling tab. For more details on scheduling, see Scheduling a Command.

Step 6 To run the commands, click **Execute Now**.

Any errors are displayed in the Result tab.

Step 7 To close the dialog box, click **Close**.

Note You can acccess the Lsp No Lockout command at both the Lsp tunnel level and the end point level. While executing the commands in the end point level, Prime Network retrieves the values from the IMO object. You must specify if the Lsp is protected or working while executing the commands in the tunnel level.

Add Global Configuration

Use the Add Global Configuration command to add a new global configuration.

Step 1 In the inventory window, expand the Logical Inventory tree and MPLS-TP node.

Step 2 Right-click and choose **MPLS-TP Global > Commands > Configuration > Add Global Configuration.**

Note To view the command in the Cisco Carrier Packet Transport (CPT) System, you must right-click the Cisco Carrier Packet Transport (CPT) System in the Prime Network Vision List or Map View and click **Logical Inventory > CPT Context Container**.

Step 3 Enter values for the following parameters.

Input Parameter	Description
Router-id	The unique identifier of the router.
Global-id	The range of the identifier for the global configuration.
Fault OAM refresh timer value	The refresh timer value.
Wait before restoring timer value	The waiting time value before restore.

Step 4 To see the commands that will be applied on the device, click **Preview**.

You can view the commands in the Result tab. You can go back and make any required changes to the input parameters.

Step 5 To schedule the command, click the Scheduling tab. For more details on scheduling, see Scheduling a Command.

Step 6 To run the commands, click **Execute Now**.

Any errors are displayed in the Result tab.

Step 7 To close the dialog box, click **Close**.

Remove Global Configuration

Use the Remove Global Configuration command to remove a global configuration.

Step 1 In the inventory window, expand the Logical Inventory tree and MPLS-TP node.

Step 2 Right-click and choose **MPLS-TP Global > Commands > Configuration > Remove Global Configuration.**

Note To view the command in the Cisco Carrier Packet Transport (CPT) System, you must right-click the Cisco Carrier Packet Transport (CPT) System in the Prime Network Vision List or Map View and click **Logical Inventory > CPT Context Container**.

Step 3 To see the commands that will be applied on the device, click **Preview**.

You can view the commands in the Result tab. You can go back and make any required changes to the input parameters.

Step 4 To schedule the command, click the Scheduling tab. For more details on scheduling, see Scheduling a Command.

Step 5 To run the commands, click **Execute Now**.

Any errors are displayed in the Result tab.

Step 6 To close the dialog box, click **Close**.

Update Global Configuration

Use the Update Global Configuration command to update an existing global configuration.

Step 1 In the inventory window, expand the Logical Inventory tree and MPLS-TP node.

Step 2 Right-click and choose **MPLS-TP Global > Commands > Configuration > Update Global Configuration.**

Note To view the command in the Cisco Carrier Packet Transport (CPT) System, you must right-click the Cisco Carrier Packet Transport (CPT) System in the Prime Network Vision List or Map View and click **Logical Inventory > CPT Context Container.**

Step 3 Enter values for the following parameters.

Input Parameter	Description
Router-id	The unique identifier of the router.
Global-id	The range of the identifier for the global configuration.
Fault OAM refresh timer value	The refresh timer value.
Wait before restoring timer value	The waiting time value before restore.

Step 4 To see the commands that will be applied on the device, click **Preview**.

You can view the commands in the Result tab. You can go back and make any required changes to the input parameters.

Step 5 To schedule the command, click the Scheduling tab. For more details on scheduling, see Scheduling a Command.

Step 6 To run the commands, click **Execute Now**.

Any errors are displayed in the Result tab.

Step 7 To close the dialog box, click **Close**.

Add Link Configuration

Use the Add Link Configuration command to add link configuration.

Step 1 In the inventory window, expand the Logical Inventory tree and MPLS-TP node.

Step 2 Right-click and choose **MPLS-TP Global > Commands > Configuration > Add Link Configuration.**

Note To view the command in the Cisco Carrier Packet Transport (CPT) System, you must right-click the Cisco Carrier Packet Transport (CPT) System in the Prime Network Vision List or Map View and click **Logical Inventory > CPT Context Container**.

Step 3 Enter values for the following parameters.

Input Parameter	Description
MPLS-TP link number	The link number of the MPLS-TP link number.
Next Hop Router Address	The next hop router address.

Step 4 To see the commands that will be applied on the device, click **Preview**.

You can view the commands in the Result tab. You can go back and make any required changes to the input parameters.

Step 5 To schedule the command, click the Scheduling tab. For more details on scheduling, see Scheduling a Command.

Step 6 To run the commands, click **Execute Now**.

Any errors are displayed in the Result tab.

Step 7 To close the dialog box, click **Close**.

Remove Link Configuration

Use the Remove Link Configuration command to remove a link configuration.

Step 1 In the inventory window, expand the Logical Inventory tree and MPLS-TP node.

Step 2 Right-click and choose **MPLS-TP Global > Commands > Configuration > Remove Link Configuration.**

Note To view the command in the Cisco Carrier Packet Transport (CPT) System, you must right-click the Cisco Carrier Packet Transport (CPT) System in the Prime Network Vision List or Map View and click **Logical Inventory > CPT Context Container**.

Step 3 Enter values for the following parameters.

Input Parameter	Description
MPLS-TP link number	The link number of the MPLS-TP link number.

Step 4 To see the commands that will be applied on the device, click **Preview**.

You can view the commands in the Result tab. You can go back and make any required changes to the input parameters.

Step 5 To schedule the command, click the Scheduling tab. For more details on scheduling, see Scheduling a Command.

Step 6 To run the commands, click **Execute Now**.

Any errors are displayed in the Result tab.

Step 7 To close the dialog box, click **Close**.

Add BFD Template Configuration

Use the Add BFD Template Configuration command to add a BFD template configuration.

Note This command does not apply to Cisco IOS XR devices.

Step 1 In the inventory window, expand the Logical Inventory tree and MPLS-TP node.

Step 2 Right-click and choose **MPLS-TP Global > Commands > Configuration > Add BFD Template Configuration.**

Note To view the command in the Cisco Carrier Packet Transport (CPT) System, you must right-click the Cisco Carrier Packet Transport (CPT) System in the Prime Network Vision List or Map View and click **Logical Inventory > CPT Context Container**.

Step 3 Enter values for the following parameters.

Input Parameter	Description
Template Type	The template type.
Template Name	The template name.
Interval Type	The interval type.
Interval Value	The interval value.
For compute hold down Check/UnCheck Multiplier	Check/Uncheck the multiplier.
Multiplier value	The multiplier value.

Step 4 To see the commands that will be applied on the device, click **Preview**.

You can view the commands in the Result tab. You can go back and make any required changes to the input parameters.

Step 5 To schedule the command, click the Scheduling tab. For more details on scheduling, see Scheduling a Command.

Step 6 To run the commands, click **Execute Now**.

Any errors are displayed in the Result tab.

Step 7 To close the dialog box, click **Close**.

Remove BFD Template Configuration

Use the Remove BFD Template Configuration command to remove a BFD template configuration.

Note This command does not apply to Cisco IOS XR devices.

Step 1 In the inventory window, expand the Logical Inventory tree and MPLS-TP node.

Step 2 Right-click and choose **MPLS-TP Global > Commands > Configuration > Remove BFD Template Configuration.**

Note To view the command in the Cisco Carrier Packet Transport (CPT) System, you must right-click the Cisco Carrier Packet Transport (CPT) System in the Prime Network Vision List or Map View and click **Logical Inventory > CPT Context Container**.

Step 3 Enter values for the following parameters.

Input Parameter	Description
Template Type	The template type.
Template Name	The template name.

Step 4 To see the commands that will be applied on the device, click **Preview**.

You can view the commands in the Result tab. You can go back and make any required changes to the input parameters.

Step 5 To schedule the command, click the Scheduling tab. For more details on scheduling, see Scheduling a Command.

Step 6 To run the commands, click **Execute Now**.

Any errors are displayed in the Result tab.

Step 7 To close the dialog box, click **Close**.

Show BFD Template

Use the Show BFD Template command to show a BFD template configuration.

Step 1 In the inventory window, expand the Logical Inventory tree and MPLS-TP node.

Step 2 Right-click and choose **MPLS-TP Global > Commands > Configuration > Show BFD Template Configuration.**

Note To view the command in the Cisco Carrier Packet Transport (CPT) System, you must right-click the Cisco Carrier Packet Transport (CPT) System in the Prime Network Vision List or Map View and click **Logical Inventory > CPT Context Container**.

Step 3 Enter values for the following parameters.

Input Parameter	Description
Template Name	The template name.

Step 4 To see the commands that will be applied on the device, click **Preview**.

You can view the commands in the Result tab. You can go back and make any required changes to the input parameters.

Step 5 To schedule the command, click the Scheduling tab. For more details on scheduling, see Scheduling a Command.

Step 6 To run the commands, click **Execute Now**.

Any errors are displayed in the Result tab.

Step 7 To close the dialog box, click **Close**.

Show BFD Template At Tunnel

Use the Show BFD Template At Tunnel command to show a BFD template at the tunnel.

Step 1 In the inventory window, expand the Logical Inventory tree and MPLS-TP node.

Step 2 Right-click and choose **MPLS-TP Global > Commands > Configuration > Show BFD Template At Tunnel.**

Step 3 To see the commands that will be applied on the device, click **Preview**.

You can view the commands in the Result tab. You can go back and make any required changes to the input parameters.

Step 4 To schedule the command, click the Scheduling tab. For more details on scheduling, see Scheduling a Command.

Step 5 To run the commands, click **Execute Now**.

Any errors are displayed in the Result tab.

Step 6 To close the dialog box, click **Close**.

Add Label Range Configuration

Use the Add Label Range Configuration command to add a label range configuration.

Note This command does not apply to Cisco IOS XR devices.

Step 1 In the inventory window, expand the Logical Inventory tree and MPLS-TP node.

Step 2 Right-click and choose **MPLS-TP Global > Commands > Configuration > Add Label Range Configuration.**

Step 3 Enter values for the following parameters.

Input Parameter	Description
Dynamic Label Minimum Value	The dynamic label minimum value.
Dynamic Label Maximum Value	The dynamic label maximum value.
Static Label Minimum Value	The static label minimum value.
Static Label Maximum Value	The static label maximum value.

Step 4 To see the commands that will be applied on the device, click **Preview**.

You can view the commands in the Result tab. You can go back and make any required changes to the input parameters.

Step 5 To schedule the command, click the Scheduling tab. For more details on scheduling, see Scheduling a Command.

Step 6 To run the commands, click **Execute Now**.

Any errors are displayed in the Result tab.

Step 7 To close the dialog box, click **Close**.

Remove Label Range Configuration

Use the Remove Label Range Configuration command to remove a label range configuration.

Note This command does not apply to Cisco IOS XR devices.

Step 1 In the inventory window, expand the Logical Inventory tree and MPLS-TP node.

Step 2 Right-click and choose **MPLS-TP Global > Commands > Configuration > Remove Label Range Configuration.**

Step 3 To see the commands that will be applied on the device, click **Preview**.

You can view the commands in the Result tab. You can go back and make any required changes to the input parameters.

Step 4 To schedule the command, click the Scheduling tab. For more details on scheduling, see Scheduling a Command.

Step 5 To run the commands, click **Execute Now**.

Any errors are displayed in the Result tab.

Step 6 To close the dialog box, click **Close**.

BFD Global Configuration

Use the BFD Global Configuration command to perform a BFD global configuration.

Note This command is only supported on Cisco ASR 9000 Series Aggregation Services Routers.

Step 1 In the inventory window, expand the Logical Inventory tree and MPLS-TP node.

Step 2 Right-click and choose **MPLS-TP Global > Commands > Configuration > BFD Global Configuration.**

Step 3 Enter values for the following parameters.

Input Parameter	Description
BFD minimum-interval	The BFD interval minimum value.
BFD Multiplier	The BFD multiplier.

Step 4 To see the commands that will be applied on the device, click **Preview**.

You can view the commands in the Result tab. You can go back and make any required changes to the input parameters.

Step 5 To schedule the command, click the Scheduling tab. For more details on scheduling, see Scheduling a Command.

Step 6 To run the commands, click **Execute Now**.

Any errors are displayed in the Result tab.

Step 7 To close the dialog box, click **Close**.



CHAPTER 25

Using mLACP Commands

In Carrier Ethernet networks, various redundancy mechanisms provide resilient interconnection of nodes and networks. The choice of redundancy mechanisms depends on various factors such as:

- Transport technology
- Topology
- Single node versus entire network multihoming
- Capability of devices
- Autonomous system (AS) boundaries
- Service provider operations model
- Service provider preferences.

Carrier Ethernet network high-availability can be achieved by employing both intra and interchassis redundancy mechanisms. The Multichassis EtherChannel (MCEC) solution of Cisco addresses the need for interchassis redundancy mechanisms, where a carrier wants to dual home a device to two upstream points of attachments (PoAs) for redundancy.

In Multichassis EtherChannel (MCEC), the DHD is dual-homed to two upstream PoAs. The DHD is incapable of running any loop prevention control protocol such as Multiple Spanning Tree (MST). Therefore, another mechanism is required to prevent forwarding loops over the redundant setup.

LACP, as defined in IEEE 802.3ad, is a link-level control protocol that allows the dynamic negotiation and establishment of LAGs. An extension of the LACP implementation to PoAs is required to convey to a DHD that it is connected to a single virtual LACP peer and not to two disjointed devices. This extension is called Multichassis LACP or mLACP.

The PoAs forming a virtual LACP peer, from the perspective of the DHD, are defined as members of a redundancy group. For the PoAs in a redundancy group to appear as a single device to the DHD, the states between them must be synchronized through the Interchassis Communication Protocol (ICCP), which provides a control-only interchassis communication channel (ICC).

Supported Network Elements

You can run the mLACP commands on all Cisco IOS and Cisco IOS XR devices that support pseudowire technology, such as

- Cisco 7600 series devices
- Cisco 6509 NEB-A series devices
- Cisco ASR 9000 series routers.

See Part 1—Cisco VNEs for details on the software versions Prime Network supports for these network elements. To run the mLACP commands, the software on the network element must support the mLACP technology.

Show Group

Use the **Show Group** command to show the group.

Step 1 In the inventory window, expand the Logical Inventory tree and choose Ethernet Link Aggregation.

Step 2 Right-click the required interface and choose **Commands > Show > Show Group**. The Show Group dialog box opens.

Step 3 To see the command that will be applied on the device, click **Preview**.

Step 4 To schedule the command, click the Scheduling tab. For more details on scheduling, see Scheduling a Command.

Step 5 To run the command, click **Execute Now**.

Any errors are displayed in the Result tab.

Step 6 To close the dialog box, click **Close**.

Show MPLS LDP

Use the **Show MPLS Label Distribution Protocol (LDP)** command to show the LDP used by the selected network element.

Step 1 In the inventory window, expand the Logical Inventory tree and choose Ethernet Link Aggregation.

Step 2 Right-click the required interface and choose **Commands > Show > Show Mpls Ldp**. The Show MPLS LDP dialog box opens.

Step 3 To see the command that will be applied on the device, click **Preview**.

Step 4 To schedule the command, click the Scheduling tab. For more details on scheduling, see Scheduling a Command.

Step 5 To run the command, click **Execute Now**.

Any errors are displayed in the Result tab.

Step 6 To close the dialog box, click **Close**.

Show Channel

Use the **Show Channel** command to show the channel in the selected network element.

Step 1 In the inventory window, expand the Logical Inventory tree and choose Ethernet Link Aggregation.

Step 2 Right-click the required interface and choose **Commands > Show > Show Channel**. The Show Channel dialog box opens.

Step 3 To see the command that will be applied on the device, click **Preview**.

Step 4 To schedule the command, click the Scheduling tab. For more details on scheduling, see Scheduling a Command.

Step 5 To run the command, click **Execute Now**.

Any errors are displayed in the Result tab.

Step 6 To close the dialog box, click **Close**.

Show LACP Internal

Use the **Show Link Aggregation Control Protocol (LACP) Internal** command to show the LACP in the selected network element.

Step 1 In the inventory window, expand the Logical Inventory tree and choose Ethernet Link Aggregation.

Step 2 Right-click the required interface and choose **Commands > Show > Show Lacp Internal**. The Show Lacp Internal dialog box opens.

Step 3 To see the command that will be applied on the device, click **Preview**.

Step 4 To schedule the command, click the Scheduling tab. For more details on scheduling, see Scheduling a Command.

Step 5 To run the command, click **Execute Now**.

Any errors are displayed in the Result tab.

Step 6 To close the dialog box, click **Close**.



CHAPTER 26

Using the Session Border Controller Commands

Session Border Controllers (SBCs) control and manage real-time multimedia traffic flows between IP network borders, handling signaling, and media. SBCs perform native IP interconnection functions required for real-time communications such as admission control, firewall traversal, accounting, signaling interworking, and quality-of-service (QoS) management.

The Cisco Prime Network platform provides fault management, configuration, and performance monitoring for SBC services. Prime Network SBC commands allow you to configure SBC components.

Before you can use Prime Network to manage an SBC device, you must add the SBC device as a Virtual Network Element (VNE) in Prime Network.

For a full description of how to use Cisco Prime Network Administration to add and define a VNE, see the *Cisco Prime Network 3.9 Administrator Guide*.

After the SBC device is added to Prime Network and the VNE is activated, you can see the physical and logical inventory information for the device. See the *Cisco Prime Network 3.9 User Guide* for more details.

SBC scripts are supported only on Cisco ASR 1000 Series Aggregation Services Routers.
See Part 1- Cisco VNEs section in this guide for details on the Cisco ASR 1000 Series software versions that Prime Network supports. To run the SBC commands, the software on the network element must support the SBC technology.

The following sections describe the commands to configure and monitor the performance of SBC services:

- Configuring SBC Components
- Monitoring the Performance of SBC Components

Configuring SBC Components

The following commands facilitate the configuration of SBC components:

- Add Commands
- Delete Commands
- Update Commands

Note In the GUI, parameters that are displayed in bold text are mandatory.

Add Commands

The add commands that you can use while configuration of SBC components are:

- Adding SIP Adjacency
- Adding SIP Adjacency Outbound AuthRealm
- Adding a Blacklist
- Adding a Blacklist Reason
- Adding a CAC Policy Set
- Adding a CAC Policy Table
- Adding a CAC Rule Entry to a CAC Policy Table
- Adding a Call Policy Set
- Adding a Call Policy Table to a Call Policy Set
- Adding a Call Rule Entry to a Call Policy Table
- Adding a Codec List
- Adding an Entry to a Codec List
- Adding a Media Address
- Adding a QoS Profile
- Adding a SIP Header Profile
- Adding a Header to an Existing SIP Header Profile
- Adding an Entry to a SIP Header Profile Header
- Adding a Condition to a SIP Header Profile Header Entry
- Adding a SIP Option Profile
- Adding a SIP Parameter Profile
- Adding a Parameter to a SIP Parameter Profile
- Adding a Media Address DBE

Adding SIP Adjacency

You can use the Add SIP Adjacency command to add Session Initiation Protocol (SIP) adjacency.

Step 1 In the inventory window, expand the Logical Inventory tree.

Step 2 Expand the Session Border Controller node.

Step 3 Right-click the SBE node and choose **Commands > Add > SIP Adjacency**. The SIP Adjacency dialog box opens.

Step 4 By default, the General tab is selected. Enter values for the following parameters.

Input Parameter	Description
Name	The SIP adjacency name. This parameter is mandatory.
Description	The SIP adjacency description.

Input Parameter	Description
Signaling Address	The local IPv4 signaling address of the SIP adjacency. This parameter is mandatory.
Signaling Port	The local port of signaling address of the SIP adjacency. The range is from 1 to 65535; the default is 5060.
Signaling Peer	The remote signaling peer of the SIP adjacency. This parameter is mandatory.
Signaling Peer Port	The remote signaling peer's port of the SIP adjacency. The range is from 1 to 65535; the default is 5060.
Remote Address	The set of remote signaling peers that can be contacted over the adjacency with the specified IP address prefix. This parameter is mandatory.
Preferred Transport	The preferred transport protocol for SIP signaling on the adjacency.
Vrf	The value used to configure the SIP adjacency for a specific VPN. The adjacency receives incoming signaling from this VPN only. The adjacency's outgoing signaling is routed in the relevant Virtual Routing and Forwarding (VRF) table.
Adjacency group	The adjacency group of the SIP adjacency. The maximum size is 32 characters.
Adjacency Account	The SIP adjacency account on an SBE.
Attach This Adjacency	Check this check box to attach the adjacency to an account on an SBE.

Step 5 Click the **Registration** tab. Enter values for the following parameters.

Input Parameter	Description
Enable Faster Register	Enables or disables fast-path register support on the SIP adjacency.
Faster Register Interval	The fast-path register interval, in seconds.
Register Minimum Expiry	The minimum registration period on the SIP adjacency, in seconds. The default is 3000 seconds.
Registration Target Address	The address to be used when an outbound SIP register request rewriting occurs.
Registration Target Port	The port to be used when an outbound SIP register request rewriting occurs.
Registration Rewrite Register	Enables or disables the SIP register request rewriting.

Step 6 Click the **Signalling Property** tab. Enter values for the following parameters.

Input Parameters	Description
Hold Media Timeout	The amount of time an SBE waits after receiving a media timeout notification from the DBE for an on-hold call before tearing that call down. The time is in milliseconds; the default value is 0.
Redirect Mode	Configures the behavior of the session border controller upon receipt of a 3xx response to an invitation from the SIP adjacency. Values are: • pass-through—Passes all 3xx responses back to the caller. • recurse—On 300, 301, 302, and 305 invite responses, the session border controller resends the invitation to the first listed contact address, or returns the 3xx response.
Redirect Limit	The maximum number of redirections that the session border controller performs on a call. The range is from 0 to 200 redirections; the default is 2.
NAT Force On	Enables NAT assuming.
Passthrough From Header	Enables the From header rewriting.
Passthrough To Header	Enables the To header rewriting.
Force Signaling Peer	Enables forcing the SIP message to go to the configured signaling peer.
SIP-I Passthrough	Enables a SIP adjacency for SIP-I pass-through.
Outbound Flood Rate	The maximum desired rate of outbound request signals on the adjacency, excluding ACK/PRACK requests. The value is in signals per second.
Hunting Trigger	The failure return codes to trigger hunting for the adjacency.
Media Bypass	The SIP adjacency to allow media traffic to bypass the DBE.
Security	The transport-level security to use on a SIP adjacency. Values are: • untrusted—(Default) The adjacency is not secure. • trusted-encrypted—Encrypted signaling is used to ensure security on the adjacency. • untrusted-encrypted—The adjacency is untrusted and uses SSL/TLS encryption. • trusted-unencrypted—A nonencryption mechanism is used to guarantee secure signaling for all messages on the adjacency.
Local Id Host	The local identity name—such as a DNS name—to present on outbound SIP messages.
Resource Priority Set	The name of the resource priority set used with the specified SIP adjacency.

Step 7 Click the **SIP Profile** tab. Enter values for the following parameters.

Input Parameters	Description
Inbound Method Profile	The name of the inbound method profile.
Outbound Method Profile	The name of the outbound method profile.
Inbound Header Profile	The name of the inbound header profile.
Outbound Header Profile	The name of the outbound header profile.

Input Parameters	Description
Proxy Inbound Option Profile	The name of the inbound proxy header profile for white/blacklisting options.
Proxy Outbound Option Profile	The name of the outbound proxy header profile for white/blacklisting options.
UA Inbound Option Profile	The name of the inbound UA header profile for white/blacklisting options.
UA Outbound Option Profile	The name of the outbound UA header profile for white/blacklisting options.

Step 8 Click the **Authentication** tab. Enter values for the following parameters.

Input Parameter	Description
Authentication Realm Inbound	The domain name of inbound authentication realm.
Authentication Mode	Configures the authentication mode for a SIP adjacency.
Authentication Nonce Timeout	The authentication nonce timeout value, in seconds. The range is from 0 to 65535 seconds; the default is 300 seconds. **Note** Nonce is a hash value used to authenticate the user.

Step 9 Click the **UAS Failure Detection** tab. Enter values for the following parameters.

Input Parameters	Description
Enable Ping	Configures the adjacency to: • Poll its remote peer by sending SIP OPTIONS pings to it. • Enter the ping option submode. The default value is disabled.
Ping Interval	The interval between SIP OPTIONS pings that are sent to the remote peer. The range is from 1 to 2147483 seconds; the default is 32 seconds.
Ping Fail Count	The number of consecutive pings that must fail before the adjacency peer is deemed to be unavailable. The range is from 1 to 4294967295; the default value is 3.
Ping Life Time	The duration for which the session border controller waits for a response to an options ping for the adjacency. The default is 32 seconds.

Step 10 Click the **P-CSCF** tab. Enter values for the following parameters.

Input Parameter	Description
Global SIP Inherit Profile	Configures the Proxy-Call Session Control Function (P-CSCF) access inherit profile as the global profile. Values are: • preset-access—Specifies a preset access profile. • preset-core—(Default) Specifies a preset core profile. • preset-ibcf-ext-untrusted—Specifies a preset Interconnection Border Control Function (IBFC) external untrusted profile. • preset-ibcf-external—Specifies a preset IBCF external profile. • preset-ibcf-internal—Specifies a preset IBCF internal profile. • preset-p-cscf-access—Specifies a preset P-CSCF-access profile. • preset-p-cscf-core—Specifies a preset P-CSCF-core profile. • preset-peering—Specifies a preset peering profile. • preset-standard-non-ims—Specified a preset standard non-Information Management System (IMS) profile.
SIP Adjacency Inherit Profile	Configures the SIP adjacency to use the P-CSCF access profile.
Visited Network Identifier	The network name of the SIP adjacency.

Step 11 Click the **IBCF** tab. Enter values for the following parameters.

Input Parameter	Description
Global SIP Home Network Identifier	The specified domain name as the global home network identifier for use in all SIP IBCF adjacencies.
Global SIP Encryption Key	The global encryption key for all SIP IBCF adjacencies.
SIP Adjacency Inherit Profile	Specifies a preset IBCF internal profile.
SIP Adjacency Encryption Key	The encryption key on the SIP IBCF adjacency.
Sip Adjacency Home Network Identifier	The home network identifier on an IBCF adjacency.

Step 12 To see the commands that will be applied on the device, click **Preview**.

You can view the commands in the Result tab. You can go back and make any required changes to the input parameters.

Step 13 To schedule the command, click the Scheduling tab. For more details on scheduling, see Scheduling a Command.

Step 14 To run the commands, click **Execute**.

Any errors are displayed in the Result tab.

Step 15 To close the dialog box, click **Close**.

Adding SIP Adjacency Outbound AuthRealm

Use the Add Sip Adjacency Outbound AuthRealm command to add a SIP adjacency outbound authentication realm.

Step 1 In the inventory window, expand the Logical Inventory tree.

Step 2 Expand the Session Border Controller node.

Step 3 Expand the SBE node.

Step 4 Expand the SIP node.

Step 5 Click the Sip Adjacency node.

Step 6 In the Sip Adjacencies window, right-click the SIP adjacency instance and choose **Commands > Add > SIP Adjacency Outbound AuthRealm**. The SIP Adjacency Outbound AuthRealm dialog box opens.

Step 7 By default, the General tab is selected. Enter values for the following parameters.

Input Parameter	Description
Domain	The domain name for which the authentication credentials are valid.
Username	The username that identifies the SBC in the specified domain.
Password	The password to authenticate the username in the specified domain.

Step 8 To see the commands that will be applied on the device, click **Preview**.

You can view the commands in the Result tab. You can go back and make any required changes to the input parameters.

Step 9 To schedule the command, click the Scheduling tab. For more details on scheduling, see Scheduling a Command.

Step 10 To run the commands, click **Execute**.

Any errors are displayed in the Result tab.

Step 11 To close the dialog box, click **Close**.

Adding a Blacklist

Use the Add Blacklist command to add a blacklist.

Step 1 In the inventory window, expand the Logical Inventory tree.

Step 2 Expand the Session Border Controller node.

Step 3 Right-click the SBE node and choose **Commands > Add > Blacklist**. The Blacklist dialog box opens.

Step 4 By default, the General tab is selected. Enter values for the following parameters.

Input Parameter	Description
VPN	The VPN name. For global VPN, the value is *global*.
Type	The blacklist type. Values are: • NORMAL • CRITICAL
IP Address	The IP address.
Port Type	The port type. Values are: • default-port-limit • TCP • UDP
Port Number	The port number, in the range from 0 to 65535. This field is valid only when the port type is TCP or UDP.
Description	The description of the blacklist.

Step 5 To see the commands that will be applied on the device, click **Preview**.

You can view the commands in the Result tab. You can go back and make any required changes to the input parameters.

Step 6 To schedule the command, click the Scheduling tab. For more details on scheduling, see Scheduling a Command.

Step 7 To run the commands, click **Execute**.

Any errors are displayed in the Result tab.

Step 8 To close the dialog box, click **Close**.

Adding a Blacklist Reason

Use the Add Blacklist Reason command to add a blacklist reason.

Step 1 In the inventory window, expand the Logical Inventory tree.

Step 2 Expand the Session Border Controller node.

Step 3 Expand the SBE node.

Step 4 Expand the Policy node.

Step 5 Click the Blacklist node.

Step 6 In the Blacklists window, right-click the blacklist instance and choose **Commands > Add > Blacklist Reason**. The Blacklist Reason dialog box opens.

Step 7 By default, the General tab is selected. Enter values for the following parameters.

Input Parameter	Description
Blacklist Name	The blacklist name.
Blacklist Type	The blacklist type.
Event Type	The event type. Values are: • authentication-failure • bad-address • corrupt-message • endpoint-registration • policy-rejection • routing-failure • spam
Blacklisting Period	The blacklisting period value.
Trigger Period	The trigger period value.
Trigger Size	The trigger size value.

Step 8 To see the commands that will be applied on the device, click **Preview**.

You can view the commands in the Result tab. You can go back and make any required changes to the input parameters.

Step 9 To schedule the command, click the Scheduling tab. For more details on scheduling, see Scheduling a Command.

Step 10 To run the commands, click **Execute**.

Any errors are displayed in the Result tab.

Step 11 To close the dialog box, click **Close**.

Adding a CAC Policy Set

Use the Add CAC Policy Set command to add a Call Admission Control (CAC) policy set.

Step 1 In the inventory window, expand the Logical Inventory tree.

Step 2 Expand the Session Border Controller node.

Step 3 Right-click the SBE node and choose **Commands > Add > CAC Policy Set**. The CAC Policy Set dialog box opens.

Step 4 By default, the General tab is selected. Enter values for the following parameters.

Input Parameter	Description
Policy Set Number	The set number of the CAC policy set.
Active	The status of the CAC policy set.
Description	The description of the CAC policy set.
First Cac Table	The first policy table of the CAC policy set. The table must be included in this CAC policy set. You can update the policy set's properties only when the policy set is inactive.
First Cac Scope	The first scope of the CAC policy set.

Step 5 Click the **Table 1** tab. Enter values for the following parameters.

Note When you add a CAC policy set for the first time, you can add three CAC policy tables. If you need to add more tables, you can do so after the CAC policy set that you create is discovered.

Input Parameter	Description
Table Name	The CAC policy table name that is included in this CAC policy set.
Match Type	The match type of the CAC policy table.
Number	The entry number for the CAC rule entry.
Action	The action type of the CAC rule entry.
Next table	When the Action field is set to next-table, you must configure this field. If the Action field is set to cac-complete, ignore this field.
Match Value	The match value for the CAC rule entry.

Step 6 To see the commands that will be applied on the device, click **Preview**.

You can view the commands in the Result tab. You can go back and make any required changes to the input parameters.

Step 7 To schedule the command, click the Scheduling tab. For more details on scheduling, see Scheduling a Command.

Step 8 To run the commands, click **Execute**.

Any errors are displayed in the Result tab.

Step 9 To close the dialog box, click **Close**.

Adding a CAC Policy Table

Use the Add CAC Policy Table command to add a CAC policy table to an existing CAC policy set.

Step 1 In the inventory window, expand the Logical Inventory tree.

Step 2 Expand the Session Border Controller node.

Step 3 Expand the SBE node.

Step 4 Expand the Policy node.

Step 5 Click the CAC Policy node.

Step 6 In the CAC Policy Set window, right-click the CAC policy instance and choose **Commands > Add > CAC Policy Table**. The CAC Policy Table dialog box opens.

Step 7 By default, the General tab is selected. Enter values for the following parameters.

Input Parameter	Description
Table Name	The CAC policy table name that is included in this CAC policy set.
Description	The description of the CAC policy table.
Match Type	The match type of the CAC policy table.

Step 8 To see the commands that will be applied on the device, click **Preview**.

You can view the commands in the Result tab. You can go back and make any required changes to the input parameters.

Step 9 To schedule the command, click the Scheduling tab. For more details on scheduling, see Scheduling a Command.

Step 10 To run the commands, click **Execute**.

Any errors are displayed in the Result tab.

Step 11 To close the dialog box, click **Close**.

Adding a CAC Rule Entry to a CAC Policy Table

Use the Add CAC Policy Entry command to add a CAC rule entry to an existing CAC policy table.

Step 1 In the inventory window, expand the Logical Inventory tree.

Step 2 Expand the Session Border Controller node.

Step 3 Expand the SBE node.

Step 4 Expand the Policy node.

Step 5 Click the CAC Policy node.

Step 6 In the CAC Policy Set window, double-click a policy instance. The CAC Policy Set Properties window opens.

Step 7 Right-click a policy table and choose **Commands > Add > CAC Rule Entry**. The CAC Rule Entry dialog box opens.

Step 8 By default, the General tab is selected. Enter values for the following parameters.

Input Parameter	Description
Entry Number	The CAC rule number that is included in this CAC policy table.
Match Value	The match value for the CAC rule entry.
Action	The action type of this CAC rule entry.
Next table	When the Action field is set to next-table, you must configure this field. If the Action field is set to cac-complete, ignore this field.

Step 9 Click the **Callee** tab. Enter values for the following parameters.

Input Parameter	Description
Callee Hold Setting	The callee hold setting. Values are: • hold-c0 • hold-c0-inactive • hold-c0-sendonly • hold-sendonly • standard
Callee Codec List	The codec list of the CAC rule entry.
Callee Privacy	The callee privacy. Values are: • never • always • account-boundary
Callee Sig Qos Profile	The QoS profile to use for signaling packets sent to the original callee.
Callee Video Qos Sig Profile	The QoS profile to use for media packets (video) sent to the original callee.
Callee Voice Qos Sig Profile	The QoS profile to use for media packets (voice) sent to the original callee.

Step 10 Click the **Caller** tab. Enter values for the following parameters.

Input Parameter	Description
Caller Hold Setting	The caller hold setting. Values are: • hold-c0 • hold-c0-inactive • hold-c0-sendonly • hold-sendonly • standard
Caller Codec List	The codec list of the CAC rule entry.
Caller Privacy	The caller privacy. Values are: • never • always • account-boundary
Caller Sig Qos Profile	The QoS profile to use for signaling packets sent to the original caller.
Caller Video Qos Profile	The QoS profile to use for media packets (video) sent to the original caller.
Caller Voice Qos Profile	The QoS profile to use for media packets (voice) sent to the original caller.

Step 11 Click the **Others** tab. Enter values for the following parameters.

Input Parameter	Description
Codec Restrict ToList	The parameter to use to restrict the codecs used in signaling a call to the set of codecs in the specified list.
Early Media	Allows or forbids early media.
Early Media Timeout	The amount of time for which to allow early media before a call is established.
Early Media Type	The direction of early media to allow for an entry in a call admission control table.
Max bandwidth per scope	The maximum bandwidth per scope for an entry in an admission control table.
Max call rate per scope	The maximum call rate for an entry in an admission control table.
Max channels per scope	The maximum number of channels for an entry in an admission control table.
Max In Call Rate	The maximum rate of inbound calls.
Max num calls per scope	The maximum number of calls for an entry in an admission control table.
Max Out Call Rate	The maximum rate of outbound calls.
Max regs per scope	The maximum number of subscriber registrations for an entry in an admission control table.
Max regs rate per scope	The maximum call number of subscriber registrations for an entry in an admission control table.

Input Parameter	Description
Max updates per call	The maximum call updates for an entry in an admission control table.
Media bypass	The SIP adjacency to use to allow media traffic to bypass the DBE.
Transcode	Allows or forbids transcoding for an entry in the admission control table.
Transport	The transport for an entry in an admission control table.

Step 12 To see the commands that will be applied on the device, click **Preview**.

You can view the commands in the Result tab. You can go back and make any required changes to the input parameters.

Step 13 To schedule the command, click the Scheduling tab. For more details on scheduling, see Scheduling a Command.

Step 14 To run the commands, click **Execute**.

Any errors are displayed in the Result tab.

Step 15 To close the dialog box, click **Close**.

Adding a Call Policy Set

Use the Add Call Policy Set command to add a new call policy set.

Note When you add a new call policy set, you can add three call policy tables. You can add more tables after the call policy set you created is discovered.

Step 1 In the inventory window, expand the Logical Inventory tree.

Step 2 Expand the Session Border Controller node.

Step 3 Right-click the SBE node and choose **Commands > Add > Call Policy Set**. The Call Policy Set dialog box opens.

Step 4 By default, the General tab is selected. Enter values for the following parameters.

Input Parameter	Description
Policy Set Number	The set number of the call policy set.
Description	The description of the call policy set.
Active	The status of the call policy set.
First Call Routing Table	The first call routing table of the call policy set. The table must be included in this call policy set. You can update the policy set's properties only when the policy set is inactive.

Step 5 Click the **Table 1** tab. Enter values for the following parameters.

Input Parameter	Description
Table Name	The call policy table name that is included in the call policy set.
Match Type	The match type of the call policy table.
Number	The entry number for the call rule entry.
Action	The action type of the call rule entry
Next table	When the Action field is set to next-table, you must configure this field. If the Action field is set to cac-complete, ignore this field.
Edit action	The dial-string manipulation action in number analysis and routing tables, where entries in the table match the entire dialed number. Enter the: • Edit action type • Edit action value
Edit cic	The carrier identification code (CIC) in number analysis and routing tables. Enter the: • Edit action type • Edit action value

You can add three entries to the call policy table. For details about adding more entries, see Adding a Call Rule Entry to a Call Policy Table.

Step 6 To see the commands that will be applied on the device, click **Preview**.

You can view the commands in the Result tab. You can go back and make any required changes to the input parameters.

Step 7 To schedule the command, click the Scheduling tab. For more details on scheduling, see Scheduling a Command.

Step 8 To run the commands, click **Execute**.

Any errors are displayed in the Result tab.

Step 9 To close the dialog box, click **Close**.

Adding a Call Policy Table to a Call Policy Set

Use the Add Call Policy Table command to add a call policy table to an existing call policy set.

Step 1 In the inventory window, expand the Logical Inventory tree.

Step 2 Expand the Session Border Controller node.

Step 3 Expand the SBE node.

Step 4 Expand the Policy node.

Step 5 Click the Call Policy node.

Step 6 In the Call Policy Set window, right-click the policy set and choose **Commands > Add > Call Policy Table**. The Call Policy Table dialog box opens.

Step 7 By default, the General tab is selected. Enter values for the following parameters.

Input Parameter	Description
Table Name	The call policy table name that is included in the call policy set.
Match Type	The match type of the call policy table.
Description	The description for the call policy table.

Step 8 To see the commands that will be applied on the device, click **Preview**.

You can view the commands in the Result tab. You can go back and make any required changes to the input parameters.

Step 9 To schedule the command, click the Scheduling tab. For more details on scheduling, see Scheduling a Command.

Step 10 To run the commands, click **Execute**.

Any errors are displayed in the Result tab.

Step 11 To close the dialog box, click **Close**.

Adding a Call Rule Entry to a Call Policy Table

Use the Add Call Rule Entry command to add an entry to an existing call policy table.

Step 1 In the inventory window, expand the Logical Inventory tree.

Step 2 Expand the Session Border Controller node.

Step 3 Expand the SBE node.

Step 4 Expand the Policy node.

Step 5 Click the Call Policy node.

Step 6 In the Call Policy Set window, double-click a policy set. The Call Policy Set Properties window opens.

Step 7 Right-click a policy table and choose **Commands > Add > Call Rule Entry**. The Call Rule Entry dialog box opens.

Step 8 By default, the General tab is selected. Enter values for the following parameters.

Input Parameter	Description
Entry Number	The call rule number that is included in this call policy table.
Action	The action type of this call rule entry.
Next table	When the Action field is set to next-table, you must configure this field. If the Action field is set to cac-complete, ignore this field.

Input Parameter	Description
Edit action	The dial-string manipulation action in number analysis and routing tables, where entries in the table match the entire dialed number. Enter the: • Edit action type • Edit action value
Edit cic	The carrier identification code (CIC) in number analysis and routing tables. Enter the: • Edit action type • Edit action value
Edit src	The source number manipulation action in number analysis and routing tables. Enter the: • Edit action type • Edit action value
Match Value	The match value for the call rule entry.
Dst Adjacency	The destination adjacency of an entry in a routing table.
Precedence	The precedence of the routing entry. You must configure this field only when the table type of the call policy table is rtg-time.
Use time offset	Check this check box if the desired time zone is ahead of or behind local time. You must configure this field only when the table type of the call policy table is rtg-time.

Step 9 To see the commands that will be applied on the device, click **Preview**.

You can view the commands in the Result tab. You can go back and make any required changes to the input parameters.

Step 10 To schedule the command, click the Scheduling tab. For more details on scheduling, see Scheduling a Command.

Step 11 To run the commands, click **Execute**.

Any errors are displayed in the Result tab.

Step 12 To close the dialog box, click **Close**.

Adding a Codec List

Use the Add Codec List command to add a codec list.

Step 1 In the inventory window, expand the Logical Inventory tree.

Step 2 Expand the Session Border Controller node.

Step 3 Right-click the SBE node and choose **Commands > Add > Codec List**. The Codec List dialog box opens.

Step 4 By default, the General tab is selected. Enter values for the following parameters.

Input Parameters	Description
Name	The name of the codec list.
Description	The description of the codec list.

Step 5 To see the commands that will be applied on the device, click **Preview**.

You can view the commands in the Result tab. You can go back and make any required changes to the input parameters.

Step 6 To schedule the command, click the Scheduling tab. For more details on scheduling, see Scheduling a Command.

Step 7 To run the commands, click **Execute**.

Any errors are displayed in the Result tab.

Step 8 To close the dialog box, click **Close**.

Adding an Entry to a Codec List

Use the Add Codec List Entry command to add an entry to a codec list.

Step 1 In the inventory window, expand the Logical Inventory tree.

Step 2 Expand the Session Border Controller node.

Step 3 Expand the SBE node.

Step 4 Expand the Policy node.

Step 5 Click the Codec List node.

Step 6 In the Codec List window, right-click the codec list instance and choose **Commands > Add > Codec List Entry**. The Codec List Entry dialog box opens.

Step 7 By default, the General tab is selected. Enter values for the following parameters.

Input Parameter	Description
Name	The name of the codec list.
Codec	The codec list item to add.
Packetization Period	The packetization period value.

Step 8 To see the commands that will be applied on the device, click **Preview**.

You can view the commands in the Result tab. You can go back and make any required changes to the input parameters.

Step 9 To schedule the command, click the Scheduling tab. For more details on scheduling, see Scheduling a Command.

Step 10 To run the commands, click **Execute**.

Any errors are displayed in the Result tab.

Step 11 To close the dialog box, click **Close**.

Adding a Media Address

Use the Add Media Address command to add a media address.

Step 1 In the inventory window, expand the Logical Inventory tree.

Step 2 Expand the Session Border Controller node.

Step 3 Right-click the SBE node and choose **Commands > Add > Media Address**. The Media Address dialog box opens.

Step 4 By default, the General tab is selected. Enter values for the following parameters.

Input Parameter	Description
Address Range	The IP address or IP address range.
Managed By	Indicates whether the media address is managed by the Data Border Element (DBE) or Media Gateway Configuration (MGC).
Nat Mode	The network address translation (NAT) mode of the media address.
Vrf Name	The VRF table name of the media address.
Port Range Lower	The lower limit of the port range.
Port Range Upper	The upper limit of the port range.
Service Class	The service class of the media address.

Step 5 To see the commands that will be applied on the device, click **Preview**.

You can view the commands in the Result tab. You can go back and make any required changes to the input parameters.

Step 6 To schedule the command, click the Scheduling tab. For more details on scheduling, see Scheduling a Command.

Step 7 To run the commands, click **Execute**.

Any errors are displayed in the Result tab.

Step 8 To close the dialog box, click **Close**.

Adding a QoS Profile

Use the Add QoS Profile command to add a QoS profile.

Step 1 In the inventory window, expand the Logical Inventory tree.

Step 2 Expand the Session Border Controller node.

Step 3 Right-click the SBE node and choose **Commands > Add > QoS Profile**. The QoS Profile dialog box opens.

Step 4 By default, the General tab is selected. Enter values for the following parameters.

Input Parameters	Description
Qos Profile Name	The QoS profile name.
Qos Profile Type	The QoS type. Values are: • fax—Fax QoS profile. • sig—Signaling QoS profile. • video—Video QoS profile. • voice—Voice QoS profile.
Marking	The marking type of the QoS profile.
IP Precedence	The IP precedence value. The range is from 0 to 7.
IP ToS	The IP ToS value. The range is from 0 to 15.
DSCP	The DSCP value. The range is from 0 to 63.

Step 5 To see the commands that will be applied on the device, click **Preview**.

You can view the commands in the Result tab. You can go back and make any required changes to the input parameters.

Step 6 To schedule the command, click the Scheduling tab. For more details on scheduling, see Scheduling a Command.

Step 7 To run the commands, click **Execute**.

Any errors are displayed in the Result tab.

Step 8 To close the dialog box, click **Close**.

Adding a SIP Header Profile

Use the Add SIP Header Profile command to add a SIP header profile.

Note When you add a new SIP header profile, you can add three headers to it. You can add more headers to the new SIP header profile after it is discovered.

Step 1 In the inventory window, expand the Logical Inventory tree.

Step 2 Expand the Session Border Controller node.

Step 3 Right-click the SBE node and choose **Commands > Add > SIP Header Profile**. The SIP Header Profile dialog box opens.

Step 4 By default, the General tab is selected. Enter values for the following parameters.

Input Parameter	Description
Name	The name of the SIP header profile.
Description	The description of the SIP header profile.
Profile Type	The type of SIP header profile. Values are: • Whitelist • Blacklist

Step 5 Click the **Header 1** tab. Enter values for the following parameters.

Input Parameter	Description
Header Name	The header name that is included in this header profile.
Entry Number	The entry number for the header.
Action Type	The action type of the entry.
Action Value	The action value for the action type.
Condition Type	The condition type.
Condition Header Name	Compares the content of a different header name.
Condition Content	Compares the content of the header.
Condition Operator	The operator for the condition content comparison.
Condition Value	The value used for comparing the condition content.
Parameter Profile	The parameter profile used by the header entry.

Step 6 To see the commands that will be applied on the device, click **Preview**.

You can view the commands in the Result tab. You can go back and make any required changes to the input parameters.

Step 7 To schedule the command, click the Scheduling tab. For more details on scheduling, see Scheduling a Command.

Step 8 To run the commands, click **Execute**.

Any errors are displayed in the Result tab.

Step 9 To close the dialog box, click **Close**.

Adding a Header to an Existing SIP Header Profile

Use the Add Header command to add a header to an existing header profile.

Step 1 In the inventory window, expand the Logical Inventory tree.

Step 2 Expand the Session Border Controller node.

Step 3 Expand the SBE node.

Step 4 Expand the SIP node.

Step 5 Expand the Sip Profile node.

Step 6 Click the Header Profile node.

Step 7 In the Sip Header Profiles window, right-click the SIP header profile instance and choose **Commands > Add > SIP Header Profile Header**. The SIP Header Profile Header dialog box opens.

Step 8 By default, the General tab is selected. Enter values for the following parameters.

Input Parameter	Description
Header Name	The header name that is included in the header profile.
Entry Number	The entry number for the header.
Action Type	The action type of the entry.
Action Value	The action value for the action type.
Condition Type	The condition type.
Condition Header Name	Compares the content of different header names.
Condition Content	Compares the content of the header.
Condition Operator	The operator for the condition content comparison.
Condition Value	The value used for comparing the condition content.
Parameter Profile	The parameter profile used by the header entry.

Step 9 To see the commands that will be applied on the device, click **Preview**.

You can view the commands in the Result tab. You can go back and make any required changes to the input parameters.

Step 10 To schedule the command, click the Scheduling tab. For more details on scheduling, see Scheduling a Command.

Step 11 To run the commands, click **Execute**.

Any errors are displayed in the Result tab.

Step 12 To close the dialog box, click **Close**.

Adding an Entry to a SIP Header Profile Header

Use the Add SIP Header Profile Entry command to add an entry to an existing SIP header profile header.

Step 1 In the inventory window, expand the Logical Inventory tree.

Step 2 Expand the Session Border Controller node.

Step 3 Expand the SBE node.

Step 4 Expand the SIP node.

Step 5 Expand the Sip Profile node.

Step 6 Click the Header Profile node. The Sip Header Profiles window opens.

Step 7 Double-click a header profile. The Sip Header Profile Properties window opens.

Step 8 Right-click a header and choose **Commands > Add > SIP Header Profile Entry**. The SIP Header Profile Entry dialog box opens.

Step 9 By default, the General tab is selected. Enter values for the following parameters.

Input Parameter	Description
Entry Number	The entry number for the header.
Action Type	The action type of the entry.
Action Value	The action value for the action type.
Condition Type	The condition type.
Condition Header Name	Compares the content of a different header.
Condition Content	Compares the content of the header.
Condition Operator	The operator for the condition content comparison.
Condition Value	The value used for comparing the condition content.
Parameter Profile	The parameter profile used by the header entry.

Step 10 To see the commands that will be applied on the device, click **Preview**.

You can view the commands in the Result tab. You can go back and make any required changes to the input parameters.

Step 11 To schedule the command, click the Scheduling tab. For more details on scheduling, see Scheduling a Command.

Step 12 To run the commands, click **Execute**.

Any errors are displayed in the Result tab.

Step 13 To close the dialog box, click **Close**.

Adding a Condition to a SIP Header Profile Header Entry

Use the Add SIP Header Profile Condition command to add a condition to a SIP header profile header.

Step 1 In the inventory window, expand the Logical Inventory tree.

Step 2 Expand the Session Border Controller node.

Step 3 Expand the SBE node.

Step 4 Expand the SIP node.

Step 5 Expand the Sip Profile node.

Step 6 Click the Header Profile node. The Sip Header Profiles window opens.

Step 7 Double-click a header profile. The Sip Header Profile Properties window opens.

Step 8 Double-click a header. The Sip Header Profile Header Properties window opens.

Step 9 Right-click an entry and choose **Commands > Add > SIP Header Profile Condition**. The SIP Header Profile Condition dialog box opens.

Step 10 By default, the General tab is selected. Enter values for the following parameters.

Input Parameter	Description
Condition Type	The condition type.
Condition Header Name	Compares the content of a different header name.
Condition Content	Compares the content of the header.
Condition Operator	The operator for the condition content comparison.
Condition Value	The value used for comparing the condition content.

Step 11 To see the commands that will be applied on the device, click **Preview**.

You can view the commands in the Result tab. You can go back and make any required changes to the input parameters.

Step 12 To schedule the command, click the Scheduling tab. For more details on scheduling, see Scheduling a Command.

Step 13 To run the commands, click **Execute**.

Any errors are displayed in the Result tab.

Step 14 To close the dialog box, click **Close**.

Adding a SIP Option Profile

Use the Add SIP Option Profile command to add a SIP option profile.

Step 1 In the inventory window, expand the Logical Inventory tree.

Step 2 Expand the Session Border Controller node.

Step 3 Right-click the SBE node and choose **Commands > Add > SIP Option Profile**. The SIP Option Profile dialog box opens.

Step 4 By default, the General tab is selected. Enter values for the following parameters.

Input Parameter	Description
Name	The name of the SIP option profile.
Description	The description of the SIP option profile.
Profile Type	The type of the SIP option profile. Values are: • Whitelist • Blacklist
Profile Options	The options of the SIP option profile. Multiple options are separated by one space; for example, host user-agent

Step 5 To see the commands that will be applied on the device, click **Preview**.

You can view the commands in the Result tab. You can go back and make any required changes to the input parameters.

Step 6 To schedule the command, click the Scheduling tab. For more details on scheduling, see Scheduling a Command.

Step 7 To run the commands, click **Execute**.

Any errors are displayed in the Result tab.

Step 8 To close the dialog box, click **Close**.

Adding a SIP Parameter Profile

Use the Add SIP Parameter Profile command to add a SIP parameter profile.

Step 1 In the inventory window, expand the Logical Inventory tree.

Step 2 Expand the Session Border Controller node.

Step 3 Right-click the SBE node and choose **Commands > Add > SIP Parameter Profile**. The SIP Parameter Profile dialog box opens.

Step 4 By default, the General tab is selected. Enter values for the following parameters.

Input Parameter	Description
Profile Name	The name of the SIP parameter profile.
Description	The description of the SIP parameter profile.

Step 5 To see the commands that will be applied on the device, click **Preview**.

You can view the commands in the Result tab. You can go back and make any required changes to the input parameters.

Step 6 To schedule the command, click the Scheduling tab. For more details on scheduling, see Scheduling a Command.

Step 7 To run the commands, click **Execute**.

Any errors are displayed in the Result tab.

Step 8 To close the dialog box, click **Close**.

Adding a Parameter to a SIP Parameter Profile

Use the Add Parameter command to add a parameter to a SIP parameter profile.

Step 1 In the inventory window, expand the Logical Inventory tree.

Step 2 Expand the Session Border Controller node.

Step 3 Expand the SBE node.

Step 4 Expand the SIP node.

Step 5 Expand the Sip Profile node.

Step 6 Click the Parameter Profile node.

Step 7 In the Sip Parameter Profiles window, right-click the profile instance and choose **Commands > Add > SIP Parameter Profile Parameter**. The SIP Parameter Profile Parameter dialog box opens.

Step 8 By default, the General tab is selected. Enter values for the following parameters.

Input Parameter	Description
Profile Name	The name of the profile to which you want to add the parameter.
Parameter Name	The name of the parameter to update.
Action	The action. Values are: • add-not-present • add-or-replace • strip
Value	The value of the action. Values are: • private-ip-address • public-ip-address • A user-defined word

Step 9 To see the commands that will be applied on the device, click **Preview**.

You can view the commands in the Result tab. You can go back and make any required changes to the input parameters.

Step 10 To schedule the command, click the Scheduling tab. For more details on scheduling, see Scheduling a Command.

Step 11 To run the commands, click **Execute**.

Any errors are displayed in the Result tab.

Step 12 To close the dialog box, click **Close**.

Adding a Media Address DBE

Use the Add Media Address DBE command to add a media address data border element.

Step 1 In the inventory window, expand the Logical Inventory tree.

Step 2 Expand the Session Border Controller node.

Step 3 Right-click the DBE node and choose **Commands > Add > Media Address Dbe**. The Media Address Dbe dialog box opens.

Step 4 By default, the General tab is selected. Enter values for the following parameters.

Input Parameter	Description
Address Range	The IP address or IP address range.
Managed By	Indicates whether the media address is managed by the Data Border Element (DBE) or Media Gateway Configuration (MGC).

Input Parameter	Description
Nat Mode	The network address translation (NAT) mode of the media address.
Vrf Name	The Virtual Routing and Forwarding (VRF) table name of the media address.
Port Range Lower	The lower limit of the port range.
Port Range Upper	The upper limit of the port range.
Service Class	The service class of the media address DBE.

Step 5 To see the commands that will be applied on the device, click **Preview**.You can view the commands in the Result tab. You can go back and make any required changes to the input parameters.

Step 6 To schedule the command, click the Scheduling tab. For more details on scheduling, see Scheduling a Command.

Step 7 To run the commands, click **Execute Now**. Any errors are displayed in the Result tab.

Step 8 To close the dialog box, click **Close**.

Delete Commands

The delete commands that you can use while configuring the SBC components:

- Deleting a Blacklist
- Deleting a Blacklist Reason
- Deleting a CAC Policy Set
- Deleting a CAC Policy Table
- Deleting a CAC Rule Entry
- Deleting a Call Policy Set
- Deleting a Call Policy Table
- Deleting a Call Rule Entry
- Deleting a Codec List
- Deleting an Entry From a Codec List
- Deleting a Media Address
- Deleting a QoS Profile
- Deleting a SIP Header Profile
- Deleting an Entry From a Header of a SIP Header Profile
- Deleting a Header From a SIP Header Profile
- Deleting a SIP Adjacency
- Deleting a SIP Adjacency Authentication Realm
- Deleting a SIP Option Profile
- Deleting a SIP Parameter Profile
- Deleting a Parameter From a SIP Parameter Profile

Deleting a Blacklist

Use the Delete Blacklist command to delete a blacklist.

Step 1 In the inventory window, expand the Logical Inventory tree.

Step 2 Expand the Session Border Controller node.

Step 3 Expand the SBE node.

Step 4 Expand the Policy node.

Step 5 Click the Blacklist node.

Step 6 In the Blacklists window, right-click the blacklist and choose **Commands > Delete > Blacklist**. The Blacklist dialog box opens.

Step 7 By default, the General tab is selected. Enter values for the following parameters.

Input Parameter	Description
Blacklist Name	The name of the blacklist to delete.
Blacklist Type	The blacklist type.

Step 8 To see the commands that will be applied on the device, click **Preview**.

You can view the commands in the Result tab. You can go back and make any required changes to the input parameters.

Step 9 To schedule the command, click the Scheduling tab. For more details on scheduling, see Scheduling a Command.

Step 10 To run the commands, click **Execute**.

Any errors are displayed in the Result tab.

Step 11 To close the dialog box, click **Close**.

Deleting a Blacklist Reason

Use the Delete Blacklist Reason command to delete a blacklist reason.

Step 1 In the inventory window, expand the Logical Inventory tree.

Step 2 Expand the Session Border Controller node.

Step 3 Expand the SBE node.

Step 4 Expand the Policy node.

Step 5 Click the Blacklist node.

Step 6 In the Blacklists window, double-click a blacklist instance. The Configured Blacklist Properties window opens.

Step 7 Right-click a blacklist reason and choose **Commands > Delete > Blacklist Reason**. The Blacklist Reason dialog box opens.

Step 8 By default, the General tab is selected. Enter a value for the following parameter.

Input Parameter	Description
Event Type	The reason type to delete.

Step 9 To see the commands that will be applied on the device, click **Preview**.

You can view the commands in the Result tab. You can go back and make any required changes to the input parameters.

Step 10 To schedule the command, click the Scheduling tab. For more details on scheduling, see Scheduling a Command.

Step 11 To run the commands, click **Execute**.

Any errors are displayed in the Result tab.

Step 12 To close the dialog box, click **Close**.

Deleting a CAC Policy Set

Use the Delete CAC Policy Set command to delete a CAC policy set.

Step 1 In the inventory window, expand the Logical Inventory tree.

Step 2 Expand the Session Border Controller node.

Step 3 Expand the SBE node.

Step 4 Expand the Policy node.

Step 5 Click the CAC Policy node.

Step 6 In the CAC Policy Set window, right-click the policy set instance and choose **Commands > Delete > CAC Policy Set**. The CAC Policy Set dialog box opens.

Step 7 By default, the General tab is selected. Enter a value for the following parameter.

Input Parameter	Description
Policy Set Number	The number of the CAC policy set to delete.

Step 8 To see the commands that will be applied on the device, click **Preview**.

You can view the commands in the Result tab. You can go back and make any required changes to the input parameters.

Step 9 To schedule the command, click the Scheduling tab. For more details on scheduling, see Scheduling a Command.

Step 10 To run the commands, click **Execute**.

Any errors are displayed in the Result tab.

Step 11 To close the dialog box, click **Close**.

Deleting a CAC Policy Table

Use the Delete CAC Policy Table command to delete a CAC policy table.

Step 1 In the inventory window, expand the Logical Inventory tree.

Step 2 Expand the Session Border Controller node.

Step 3 Expand the SBE node.

Step 4 Expand the Policy node.

Step 5 Click the CAC Policy node.

Step 6 In the CAC Policy Set window, double-click a policy instance. The Cac Policy Set Properties window opens.

Step 7 Right-click a policy table and choose **Commands > Delete > CAC Policy Table**. The CAC Policy Table dialog box opens.

Step 8 By default, the General tab is selected. Enter a value for the following parameter.

Input Parameter	Description
Table Name	The name of the CAC policy table to delete.

Step 9 To see the commands that will be applied on the device, click **Preview**.

You can view the commands in the Result tab. You can go back and make any required changes to the input parameters.

Step 10 To schedule the command, click the Scheduling tab. For more details on scheduling, see Scheduling a Command.

Step 11 To run the commands, click **Execute**.

Any errors are displayed in the Result tab.

Step 12 To close the dialog box, click **Close**.

Deleting a CAC Rule Entry

Use the Delete CAC Rule Entry command to delete a CAC rule entry.

Step 1 In the inventory window, expand the Logical Inventory tree.

Step 2 Expand the Session Border Controller node.

Step 3 Expand the SBE node.

Step 4 Expand the Policy node.

Step 5 Click the CAC Policy node.

Step 6 In the CAC Policy Set window, double-click a policy instance. The Cac Policy Set Properties window opens.

Step 7 Double-click a policy table. The Cac Policy Table Properties window opens.

Step 8 In the CAC Rule Entry tab, right-click an entry and choose **Commands > Delete > CAC Rule Entry**. The CAC Rule Entry dialog box opens.

Step 9 By default, the General tab is selected. Enter a value for the following parameter.

Input Parameter	Description
Entry Number	The number of the CAC rule entry to delete.

Step 10 To see the commands that will be applied on the device, click **Preview**.

You can view the commands in the Result tab. You can go back and make any required changes to the input parameters.

Step 11 To schedule the command, click the Scheduling tab. For more details on scheduling, see Scheduling a Command.

Step 12 To run the commands, click **Execute**.

Any errors are displayed in the Result tab.

Step 13 To close the dialog box, click **Close**.

Deleting a Call Policy Set

Use the Delete Call Policy Set command to delete a call policy set.

Step 1 In the inventory window, expand the Logical Inventory tree.

Step 2 Expand the Session Border Controller node.

Step 3 Expand the SBE node.

Step 4 Expand the Policy node.

Step 5 Click the Call Policy node.

Step 6 In the Call Policy Set window, right-click a policy set and choose **Commands > Delete > Call Policy Set**. The Call Policy Set dialog box opens.

Step 7 By default, the General tab is selected. Enter a value for the following parameter.

Input Parameter	Description
Policy Set Number	The number of the call policy set to delete.

Step 8 To see the commands that will be applied on the device, click **Preview**.

You can view the commands in the Result tab. You can go back and make any required changes to the input parameters.

Step 9 To schedule the command, click the Scheduling tab. For more details on scheduling, see Scheduling a Command.

Step 10 To run the commands, click **Execute**.

Any errors are displayed in the Result tab.

Step 11 To close the dialog box, click **Close**.

Deleting a Call Policy Table

Use the Delete Call Policy Table command to delete a call policy table.

Step 1 In the inventory window, expand the Logical Inventory tree.

Step 2 Expand the Session Border Controller node.

Step 3 Expand the SBE node.

Step 4 Expand the Policy node.

Step 5 Click the Call Policy node.

Step 6 In the Call Policy Set window, double-click a policy set. The Call Policy Set Properties window opens.

Step 7 Right-click a policy table and choose **Commands > Delete > Call Policy Table**. The Call Policy Table dialog box opens.

Step 8 By default, the General tab is selected. Enter a value for the following parameter.

Input Parameter	Description
Table Name	The name of the call policy table to delete.

Step 9 To see the commands that will be applied on the device, click **Preview**.

You can view the commands in the Result tab. You can go back and make any required changes to the input parameter.

Step 10 To schedule the command, click the Scheduling tab. For more details on scheduling, see Scheduling a Command.

Step 11 To run the commands, click **Execute**.

Any errors are displayed in the Result tab.

Step 12 To close the dialog box, click **Close**.

Deleting a Call Rule Entry

Use the Delete Call Rule Entry command to delete a call rule entry.

Step 1 In the inventory window, expand the Logical Inventory tree.

Step 2 Expand the Session Border Controller node.

Step 3 Expand the SBE node.

Step 4 Expand the Policy node.

Step 5 Click the Call Policy node.

Step 6 In the Call Policy Set window, double-click a policy set. The Call Policy Set Properties window opens.

Step 7 Right-click a policy table and choose **Commands > Delete > Call Rule Entry**. The Call Rule Entry dialog box opens.

Step 8 By default, the General tab is selected. Enter a value for the following parameter.

Input Parameter	Description
Entry Number	The number of the call rule entry to delete.

Step 9 To see the commands that will be applied on the device, click **Preview**.

You can view the commands in the Result tab. You can go back and make any required changes to the input parameter.

Step 10 To schedule the command, click the Scheduling tab. For more details on scheduling, see Scheduling a Command.

Step 11 To run the commands, click **Execute**.

Any errors are displayed in the Result tab.

Step 12 To close the dialog box, click **Close**.

Deleting a Codec List

Use the Delete Codec List command to delete a codec list.

Step 1 In the inventory window, expand the Logical Inventory tree.

Step 2 Expand the Session Border Controller node.

Step 3 Expand the SBE node.

Step 4 Expand the Policy node.

Step 5 Click the Codec List node.

Step 6 In the Codec List window, right-click a codec list instance and choose **Commands > Delete > Codec List**. The Codec List dialog box opens.

Step 7 By default, the General tab is selected. Enter a value for the following parameter.

Input Parameter	Description
Name	The name of the codec list to delete.

Step 8 To see the commands that will be applied on the device, click **Preview**.

You can view the commands in the Result tab. You can go back and make any required changes to the input parameter.

Step 9 To schedule the command, click the Scheduling tab. For more details on scheduling, see Scheduling a Command.

Step 10 To run the commands, click **Execute**.

Any errors are displayed in the Result tab.

Step 11 To close the dialog box, click **Close**.

Deleting an Entry From a Codec List

Use the Delete Codec List Entry command to delete an entry from a codec list.

Step 1 In the inventory window, expand the Logical Inventory tree.

Step 2 Expand the Session Border Controller node.

Step 3 Expand the SBE node.

Step 4 Expand the Policy node.

Step 5 Click the Codec List node.

Step 6 In the Codec List window, double-click a codec list. The Codec List Properties window opens.

Step 7 Right-click a codec and choose **Commands > Delete > Codec List Entry**. The Codec List Entry dialog box opens.

Step 8 By default, the General tab is selected. Enter a value for the following parameter.

Input Parameter	Description
Codec	The codec to delete.

Step 9 To see the commands that will be applied on the device, click **Preview**.

You can view the commands in the Result tab. You can go back and make any required changes to the input parameter.

Step 10 To schedule the command, click the Scheduling tab. For more details on scheduling, see Scheduling a Command.

Step 11 To run the commands, click **Execute**.

Any errors are displayed in the Result tab.

Step 12 To close the dialog box, click **Close**.

Deleting a Media Address

Use the Delete Media Address command to delete a media address.

Step 1 In the inventory window, expand the Logical Inventory tree.

Step 2 Expand the Session Border Controller node.

Step 3 Expand the DBE node.

Step 4 Click the Media Address node.

Step 5 In the Media Address window, right-click a media address and choose **Commands > Delete > Media Address**. The Media Address dialog box opens.

Step 6 By default, the General tab is selected. Enter values for the following parameters.

Input Parameter	Description
Address Range	The IP address or IP address range.
Managed By	Indicates whether the media address is managed by the Data Border Element (DBE) or Media Gateway Configuration (MGC).
Nat Mode	The network address translation (NAT) mode of the media address.
Vrf Name	The VRF name of the media address.

Step 7 To see the commands that will be applied on the device, click **Preview**.

You can view the commands in the Result tab. You can go back and make any required changes to the input parameters.

Step 8 To schedule the command, click the Scheduling tab. For more details on scheduling, see Scheduling a Command.

Step 9 To run the commands, click **Execute**.

Any errors are displayed in the Result tab.

Step 10 To close the dialog box, click **Close**.

Deleting a QoS Profile

Use the Delete QoS Profile command to delete a QoS profile.

Step 1 In the inventory window, expand the Logical Inventory tree.

Step 2 Expand the Session Border Controller node.

Step 3 Expand the SBE node.

Step 4 Expand the Policy node.

Step 5 Click the QoS Profile node.

Step 6 In the Qos Profile window, right-click a QoS profile and choose **Commands > Delete > QoS Profile**. The QoS Profile dialog box opens.

Step 7 By default, the General tab is selected. Enter values for the following parameters.

Input Parameter	Description
Qos Profile Name	The name of the QoS profile to delete.
Qos Profile Type	The type of QoS profile. Values are: • sig • voice • video

Step 8 To see the commands that will be applied on the device, click **Preview**.

You can view the commands in the Result tab. You can go back and make any required changes to the input parameters.

Step 9 To schedule the command, click the Scheduling tab. For more details on scheduling, see Scheduling a Command.

Step 10 To run the commands, click **Execute**.

Any errors are displayed in the Result tab.

Step 11 To close the dialog box, click **Close**.

Deleting a SIP Header Profile

Use the Delete SIP Header Profile command to delete a SIP header profile.

Step 1 In the inventory window, expand the Logical Inventory tree.

Step 2 Expand the Session Border Controller node.

Step 3 Expand the SBE node.

Step 4 Expand the SIP node.

Step 5 Expand the Sip Profile node.

Step 6 Click the Header Profile node.

Step 7 In the Sip Header Profiles window, right-click a header profile and choose **Commands > Delete > SIP Header Profile**. The SIP Header Profile dialog box opens.

Step 8 By default, the General tab is selected. Enter a value for the following parameter.

Input Parameter	Description
Name	The name of the SIP header profile to delete.

Step 9 To see the commands that will be applied on the device, click **Preview**.

You can view the commands in the Result tab. You can go back and make any required changes to the input parameter.

Step 10 To schedule the command, click the Scheduling tab. For more details on scheduling, see Scheduling a Command.

Step 11 To run the commands, click **Execute**.

Any errors are displayed in the Result tab.

Step 12 To close the dialog box, click **Close**.

Deleting an Entry From a Header of a SIP Header Profile

Use the Delete SIP Header Profile Entry command to delete an entry from a header of a SIP header profile.

Step 1 In the inventory window, expand the Logical Inventory tree.

Step 2 Expand the Session Border Controller node.

Step 3 Expand the SBE node.

Step 4 Expand the SIP node.

Step 5 Expand the Sip Profile node.

Step 6 Click the Header Profile node. The Sip Header Profiles window opens.

Step 7 Double-click a header profile. The Sip Header Profile Properties window opens.

Step 8 Double-click a header. The Sip Header Profile Header Properties window opens.

Step 9 Right-click an entry and choose **Commands > Delete > SIP Header Profile Entry**. The SIP Header Profile Entry dialog box opens.

Step 10 By default, the General tab is selected. Enter a value for the following parameter.

Input Parameter	Description
Entry Number	The number of the entry to delete.

Step 11 To see the commands that will be applied on the device, click **Preview**.

You can view the commands in the Result tab. You can go back and make any required changes to the input parameter.

Step 12 To schedule the command, click the Scheduling tab. For more details on scheduling, see Scheduling a Command.

Step 13 To run the commands, click **Execute**.

Any errors are displayed in the Result tab.

Step 14 To close the dialog box, click **Close**.

Deleting a Header From a SIP Header Profile

Use the Delete SIP Header Profile Header command to delete a header from a SIP header profile.

Step 1 In the inventory window, expand the Logical Inventory tree.

Step 2 Expand the Session Border Controller node.

Step 3 Expand the SBE node.

Step 4 Expand the SIP node.

Step 5 Expand the Sip Profile node.

Step 6 Click the Header Profile node. The Sip Header Profiles window opens.

Step 7 Double-click a header profile. The Sip Header Profile Properties window opens.

Step 8 Right-click a header and choose **Commands > Delete > SIP Header Profile Header**. The SIP Header Profile Header dialog box opens.

Step 9 By default, the General tab is selected. Enter a value for the following parameter.

Input Parameter	Description
Name	The name of the header to delete from the SIP header profile.

Step 10 To see the commands that will be applied on the device, click **Preview**.

You can view the commands in the Result tab. You can go back and make any required changes to the input parameter.

Step 11 To schedule the command, click the Scheduling tab. For more details on scheduling, see Scheduling a Command.

Step 12 To run the commands, click **Execute**.

Any errors are displayed in the Result tab.

Step 13 To close the dialog box, click **Close**.

Deleting a SIP Adjacency

Use the Delete SIP Adjacency command to delete a SIP adjacency.

Step 1 In the inventory window, expand the Logical Inventory tree.

Step 2 Expand the Session Border Controller node.

Step 3 Expand the SBE node.

Step 4 Expand the SIP node.

Step 5 Click the Sip Adjacency node.

Step 6 In the Sip Adjacencies window, right-click a SIP adjacency and choose **Commands > Delete > SIP Adjacency**. The SIP Adjacency dialog box opens.

Step 7 By default, the General tab is selected. Enter a value for the following parameter.

Input Parameter	Description
Adj Name	The name of the SIP adjacency to delete.

Step 8 To see the commands that will be applied on the device, click **Preview**.

You can view the commands in the Result tab. You can go back and make any required changes to the input parameter.

Step 9 To schedule the command, click the Scheduling tab. For more details on scheduling, see Scheduling a Command.

Step 10 To run the commands, click **Execute**. If the adjacency is attached, it will be detached and then deleted.

Any errors are displayed in the Result tab.

Step 11 To close the dialog box, click **Close**.

Deleting a SIP Adjacency Authentication Realm

Use the Delete SIP Adjacency Outbound AuthRealm command to delete a SIP adjacency outbound authentication realm.

Step 1 In the inventory window, expand the Logical Inventory tree.

Step 2 Expand the Session Border Controller node.

Step 3 Expand the SBE node.

Step 4 Expand the SIP node.

Step 5 Click the Sip Adjacency node.

Step 6 In the Sip Adjacencies window, right-click the SIP adjacency instance and choose **Commands > Delete > SIP Adjacency Outbound AuthRealm**. The SIP Adjacency Outbound AuthRealm dialog box opens.

Step 7 By default, the General tab is selected. Enter a value for the following parameter.

Input Parameter	Description
Domain	The domain name of the outbound authentication realm to delete.

Step 8 To see the commands that will be applied on the device, click **Preview**.

You can view the commands in the Result tab. You can go back and make any required changes to the input parameters.

Step 9 To schedule the command, click the Scheduling tab. For more details on scheduling, see Scheduling a Command.

Step 10 To run the commands, click **Execute**. If the adjacency is attached, it will be detached and then deleted.

Any errors are displayed in the Result tab.

Step 11 To close the dialog box, click **Close**.

Deleting a SIP Option Profile

Use the Delete SIP Option Profile command to delete a SIP option profile.

Step 1 In the inventory window, expand the Logical Inventory tree.

Step 2 Expand the Session Border Controller node.

Step 3 Expand the SBE node.

Step 4 Expand the SIP node.

Step 5 Expand the Sip Profile node.

Step 6 Click the Option Profile node.

Step 7 In the Sip Option Profiles window, right-click a profile and choose **Commands > Delete > SIP Option Profile**. The SIP Option Profile dialog box opens.

Step 8 By default, the General tab is selected. Enter a value for the following parameter.

Input Parameter	Description
Name	The name of the SIP option profile to delete.

Step 9 To see the commands that will be applied on the device, click **Preview**.

You can view the commands in the Result tab. You can go back and make any required changes to the input parameter.

Step 10 To schedule the command, click the Scheduling tab. For more details on scheduling, see Scheduling a Command.

Step 11 To run the commands, click **Execute**.

Any errors are displayed in the Result tab.

Step 12 To close the dialog box, click **Close**.

Deleting a SIP Parameter Profile

Use the Delete SIP Parameter Profile command to delete a SIP parameter profile.

Step 1 In the inventory window, expand the Logical Inventory tree.

Step 2 Expand the Session Border Controller node.

Step 3 Expand the SBE node.

Step 4 Expand the SIP node.

Step 5 Expand the Sip Profile node.

Step 6 Click the Parameter Profile node.

Step 7 In the Sip Parameter Profiles window, right-click a profile and choose **Commands > Delete > SIP Parameter Profile**. The SIP Parameter Profile dialog box opens.

Step 8 By default, the General tab is selected. Enter a value for the following parameter.

Input Parameter	Description
Profile Name	The name of the SIP parameter profile to delete.

Step 9 To see the commands that will be applied on the device, click **Preview**.

You can view the commands in the Result tab. You can go back and make any required changes to the input parameter.

Step 10 To schedule the command, click the Scheduling tab. For more details on scheduling, see Scheduling a Command.

Step 11 To run the commands, click **Execute**.

Any errors are displayed in the Result tab.

Step 12 To close the dialog box, click **Close**.

Deleting a Parameter From a SIP Parameter Profile

Use the Delete SIP Parameter Profile Parameter command to delete a parameter from a SIP parameter profile.

Step 1 In the inventory window, expand the Logical Inventory tree.

Step 2 Expand the Session Border Controller node.

Step 3 Expand the SBE node.

Step 4 Expand the SIP node.

Step 5 Expand the Sip Profile node.

Step 6 Click the Parameter Profile node.

Step 7 In the Sip Parameter Profiles window, double-click a profile. The Sip Parameter Profile Properties window opens.

Step 8 Right-click a parameter and choose **Commands > Delete > SIP Parameter Profile Parameter**. The SIP Parameter Profile Parameter dialog box opens.

Step 9 By default, the General tab is selected. Enter a value for the following parameter.

Input Parameter	Description
Parameter Name	The name parameter to delete.

Step 10 To see the commands that will be applied on the device, click **Preview**.

You can view the commands in the Result tab. You can go back and make any required changes to the input parameter.

Step 11 To schedule the command, click the Scheduling tab. For more details on scheduling, see Scheduling a Command.

Step 12 To run the commands, click **Execute**.

Any errors are displayed in the Result tab.

Step 13 To close the dialog box, click **Close**.

Update Commands

The update commands that you can use while configuring the SBC components:

- Updating a Blacklist Reason
- Updating a CAC Policy Set
- Updating a CAC Policy Table
- Updating a CAC Rule Entry
- Updating a Call Policy Set
- Updating a Call Policy Table
- Updating a Call Rule Entry
- Updating a Codec List Entry
- Updating a QoS Profile
- Updating a SIP Adjacency
- Updating a SIP Header Profile
- Updating a SIP Header Profile Entry
- Updating a SIP Option Profile
- Updating a Parameter in a SIP Parameter Profile
- Updating SIP Adjacency Outbound AuthRealm

Updating a Blacklist Reason

Use the Update Blacklist Reason command to update a blacklist reason.

Step 1 In the inventory window, expand the Logical Inventory tree.

Step 2 Expand the Session Border Controller node.

Step 3 Expand the SBE node.

Step 4 Expand the Policy node.

Step 5 Click the Blacklist node.

Step 6 In the Blacklists window, double-click a blacklist instance. The Configured Blacklist Properties window opens.

Step 7 Right-click a blacklist reason and choose **Commands > Update > Blacklist Reason**. The Blacklist Reason dialog box opens.

Step 8 By default, the General tab is selected. Enter values for the following parameters.

Input Parameter	Description
Blacklisting Period	The blacklisting period value.
Trigger Period	The trigger period value.
Trigger Size	The trigger size value.

Step 9 To see the commands that will be applied on the device, click **Preview**.

You can view the commands in the Result tab. You can go back and make any required changes to the input parameters.

Step 10 To schedule the command, click the Scheduling tab. For more details on scheduling, see Scheduling a Command.

Step 11 To run the commands, click **Execute**.

Any errors are displayed in the Result tab.

Step 12 To close the dialog box, click **Close**.

Updating a CAC Policy Set

Use the Update CAC Policy Set command to update a CAC policy set.

Step 1 In the inventory window, expand the Logical Inventory tree.

Step 2 Expand the Session Border Controller node.

Step 3 Expand the SBE node.

Step 4 Expand the Policy node.

Step 5 Click the CAC Policy node.

Step 6 In the CAC Policy Set window, right-click the policy set instance and choose **Commands > Update > CAC Policy Set**. The CAC Policy Set dialog box opens.

Step 7 By default, the General tab is selected. Enter values for the following parameters.

Input Parameter	Description
Active	The status of the CAC policy set.
Description	The description of the CAC policy set.
First Cac Table	The first policy table of the CAC policy set. The table must be included in this CAC policy set. You can update the policy set's properties only when the policy set is inactive.
First Cac Scope	The first scope of the CAC policy set.

Step 8 To see the commands that will be applied on the device, click **Preview**.

You can view the commands in the Result tab. You can go back and make any required changes to the input parameters.

Step 9 To schedule the command, click the Scheduling tab. For more details on scheduling, see Scheduling a Command.

Step 10 To run the commands, click **Execute**.

Any errors are displayed in the Result tab.

Step 11 To close the dialog box, click **Close**.

Updating a CAC Policy Table

Use the Update Cac Policy Table command to update a CAC policy table.

Step 1 In the inventory window, expand the Logical Inventory tree.

Step 2 Expand the Session Border Controller node.

Step 3 Expand the SBE node.

Step 4 Expand the Policy node.

Step 5 Click the CAC Policy node.

Step 6 In the CAC Policy Set window, double-click a policy instance. The Cac Policy Set Properties window opens.

Step 7 Right-click a policy table and choose **Commands > Update > CAC Policy Table**. The CAC Policy Table dialog box opens.

Step 8 By default, the General tab is selected. Enter values for the following parameters.

Input Parameter	Description
Description	The description of the CAC policy table.
Match Type	The match type of the CAC policy table. You cannot update the match type if there are entries in the policy table.

Step 9 To see the commands that will be applied on the device, click **Preview**.

You can view the commands in the Result tab. You can go back and make any required changes to the input parameters.

Step 10 To schedule the command, click the Scheduling tab. For more details on scheduling, see Scheduling a Command.

Step 11 To run the commands, click **Execute**.

Any errors are displayed in the Result tab.

Step 12 To close the dialog box, click **Close**.

Updating a CAC Rule Entry

Use the Update CAC Rule Entry command to update a CAC rule entry.

Step 1 In the inventory window, expand the Logical Inventory tree.

Step 2 Expand the Session Border Controller node.

Step 3 Expand the SBE node.

Step 4 Expand the Policy node.

Step 5 Click the CAC Policy node.

Step 6 In the CAC Policy Set window, double-click a policy instance. The Cac Policy Set Properties window opens.

Step 7 Double-click a policy table. The Cac Policy Table Properties window opens.

Step 8 In the CAC Rule Entry tab, right-click an entry and choose **Commands > Update > CAC Rule Entry**. The CAC Rule Entry dialog box opens.

Step 9 By default, the General tab is selected. Enter values for the following parameters.

Input Parameter	Description
Match Value	The match value for the CAC rule entry.
Action	The action type of the CAC rule entry. Values are: • next-table • cac-complete
Next table	When the Action field is set to “next-table,” you must configure this field. If the Action field is set to “cac-complete,” ignore this field.

Step 10 Click the **Callee** tab. Enter values for the following parameters.

Input Parameter	Description
Callee Hold Setting	The callee hold setting. Values are: • hold-c0 • hold-c0-inactive • hold-c0-sendonly • hold-sendonly • standard
Callee Codec List	The codec list of the CAC rule entry.
Callee Privacy	The callee privacy. Values are: • never • always • account-boundary
Callee Sig Qos Profile	The QoS profile to use for signaling packets sent to the original callee.

Input Parameter	Description
Callee Video Qos Profile	The QoS profile to use for media packets (video) sent to the original callee.
Callee Voice Qos Profile	The QoS profile to use for media packets (voice) sent to the original callee.

Step 11 Click the **Caller** tab. Enter values for the following parameters.

Input Parameter	Description
Caller Hold Setting	The caller hold setting. Values are: • hold-c0 • hold-c0-inactive • hold-c0-sendonly • hold-sendonly • standard
Caller Codec List	The codec list of the CAC rule entry.
Caller Privacy	The caller privacy. Values are: • never • always • account-boundary
Caller Sig Qos Profile	The QoS profile to use for signaling packets sent to the original caller.
Caller Video Qos Profile	The QoS profile to use for media packets (video) sent to the original caller.
Caller Voice Qos Profile	The QoS profile to use for media packets (voice) sent to the original caller.

Step 12 Click the **Others** tab. Enter values for the following parameters.

Input Parameter	Description
Codec Restrict ToList	The parameter to use to restrict the codecs used in signaling a call to the set of codecs in the specified list.
Early Media	Allows or forbids early media.
Early Media Timeout	The amount of time for which to allow early media before a call is established.
Early Media Type	The direction of early media to allow for an entry in a call admission control table.
Max bandwidth per scope	The maximum bandwidth per scope for an entry in an admission control table.
Max call rate per scope	The maximum call rate for an entry in an admission control table.
Max channels per scope	The maximum number of channels for an entry in an admission control table.
Max In Call Rate	The maximum rate of inbound calls.
Max num calls per scope	The maximum number of calls in an entry in an admission control table.
Max Out Call Rate	The maximum rate of outbound calls.

Input Parameter	Description
Max regs per scope	The maximum number of subscriber registrations for an entry in an admission control table.
Max regs rate per scope	The maximum call number of subscriber registrations for an entry in an admission control table.
Max updates per call	The maximum number of call updates for an entry in an admission control table.
Media bypass	The SIP adjacency to use to allow media traffic to bypass the DBE.
Transcode	Allows or forbids transcoding for an entry in the admission control table.
Transport	The transport for an entry in an admission control table.

Step 13 To see the commands that will be applied on the device, click **Preview**.

You can view the commands in the Result tab. You can go back and make any required changes to the input parameters.

Step 14 To schedule the command, click the Scheduling tab. For more details on scheduling, see Scheduling a Command.

Step 15 To run the commands, click **Execute**.

Any errors are displayed in the Result tab.

Step 16 To close the dialog box, click **Close**.

Updating a Call Policy Set

Use the Update Call Policy Set command to update a call policy set.

Step 1 In the inventory window, expand the Logical Inventory tree.

Step 2 Expand the Session Border Controller node.

Step 3 Expand the SBE node.

Step 4 Expand the Policy node.

Step 5 Click the Call Policy node.

Step 6 In the Call Policy Set window, right-click a policy set and choose **Commands > Update > Call Policy Set**. The Call Policy Set dialog box opens.

Step 7 By default, the General tab is selected. Enter values for the following parameters.

Input Parameter	Description
Active	The status of the call policy set. Values are: • true—The call policy set is active. • false—The call policy set is inactive.
Description	The description of the call policy set.
First Call Routing Table	The first call routing table of the call policy set. The table must be included in this call policy set. You can update the propeerties of the policy set only when the policy set is inactive.

Step 8 To see the commands that will be applied on the device, click **Preview**.

You can view the commands in the Result tab. You can go back and make any required changes to the input parameters.

Step 9 To schedule the command, click the Scheduling tab. For more details on scheduling, see Scheduling a Command.

Step 10 To run the commands, click **Execute**.

Any errors are displayed in the Result tab.

Step 11 To close the dialog box, click **Close**.

Updating a Call Policy Table

Use the Update Call Policy Table command to update a call policy table.

Step 1 In the inventory window, expand the Logical Inventory tree.

Step 2 Expand the Session Border Controller node.

Step 3 Expand the SBE node.

Step 4 Expand the Policy node.

Step 5 Click the Call Policy node.

Step 6 In the Call Policy Set window, double-click a policy set. The Call Policy Set Properties window opens.

Step 7 Right-click a policy table and choose **Commands > Update > Call Policy Table**. The Call Policy Table dialog box opens.

Step 8 By default, the General tab is selected. Enter a value for the following parameter.

Input Parameter	Description
Description	The description of the call policy table.

Step 9 To see the commands that will be applied on the device, click **Preview**.

You can view the commands in the Result tab. You can go back and make any required changes to the input parameter.

Step 10 To schedule the command, click the Scheduling tab. For more details on scheduling, see Scheduling a Command.

Step 11 To run the commands, click **Execute**.

Any errors are displayed in the Result tab.

Step 12 To close the dialog box, click **Close**.

Updating a Call Rule Entry

Use the Update Call Rule Entry command to update a call rule entry.

Step 1 In the inventory window, expand the Logical Inventory tree.

Step 2 Expand the Session Border Controller node.

Step 3 Expand the SBE node.

Step 4 Expand the Policy node.

Step 5 Click the Call Policy node.

Step 6 In the Call Policy Set window, double-click a policy set. The Call Policy Set Properties window opens.

Step 7 Double-click a policy table. The Call Policy Table Properties window opens.

Step 8 In the Call Rule Entry tab, right-click an entry and choose **Commands > Update > Call Rule Entry**. The Call Rule Entry dialog box opens.

Step 9 By default, the General tab is selected. Enter values for the following parameters.

Input Parameter	Description
Action	The action type of the call rule entry. Values are: • next-table • cac-complete
Next table	When the Action field is set to “next-table,” you must configure this field. If the Action field is set to “cac-complete,” ignore this field.
Edit action type	The dial-string manipulation action in number analysis and routing tables, where entries in the table match the entire dialed number.
Edit action value	Enter a value for the action value.
Edit cic type	The carrier identification code (CIC) in number analysis and routing tables.
Edit cic value	Enter a value for the CIC value.
Edit src type	The source number manipulation action in number analysis and routing tables.
Edit src value	Enter a value for the source value.
Match value	The match value for the call rule entry.
Dst adjacency	The destination adjacency of an entry in a routing table.

Input Parameter	Description
Precedence	The precedence of the routing entry. You must configure this field only when the table type of the call policy table is rtg-time.
Use time offset	Check this check box if the desired time zone is ahead of or behind local time. You must configure this field only when the table type of the call policy table is rtg-time.

Step 10 To see the commands that will be applied on the device, click **Preview**.

You can view the commands in the Result tab. You can go back and make any required changes to the input parameters.

Step 11 To schedule the command, click the Scheduling tab. For more details on scheduling, see Scheduling a Command.

Step 12 To run the commands, click **Execute**.

Any errors are displayed in the Result tab.

Step 13 To close the dialog box, click **Close**.

Updating a Codec List Entry

Use the Update Codec List Entry command to update an entry in a codec list.

Step 1 In the inventory window, expand the Logical Inventory tree.

Step 2 Expand the Session Border Controller node.

Step 3 Expand the SBE node.

Step 4 Expand the Policy node.

Step 5 Click the Codec List node.

Step 6 In the Codec List window, double-click a codec. The Codec List Properties window opens.

Step 7 Right-click a codec list instance and choose **Commands > Update > Codec List Entry**. The Codec List Entry dialog box opens.

Step 8 By default, the General tab is selected. Enter values for the following parameters.

Input Parameter	Description
Codec	The codec list item to delete.
Packetization Period	The packetization period value.

Step 9 To see the commands that will be applied on the device, click **Preview**.

You can view the commands in the Result tab. You can go back and make any required changes to the input parameters.

Step 10 To schedule the command, click the Scheduling tab. For more details on scheduling, see Scheduling a Command.

Step 11 To run the commands, click **Execute**.

Any errors are displayed in the Result tab.

Step 12 To close the dialog box, click **Close**.

Updating a QoS Profile

Use the Update Qos Profile command to update a QoS profile.

Step 1 In the inventory window, expand the Logical Inventory tree.

Step 2 Expand the Session Border Controller node.

Step 3 Expand the SBE node.

Step 4 Expand the Policy node.

Step 5 Click the QoS Profile node.

Step 6 In the Qos Profile window, right-click a QoS profile and choose **Commands > Update > QoS Profile**. The QoS Profile dialog box opens.

Step 7 By default, the General tab is selected. Enter values for the following parameters.

Input Parameter	Description
Qos Profile Name	The QoS profile name.
Qos Profile Type	The QoS profile type. Values are: • sig • voice • video
Marking	The marking type of the QoS profile.
IP Precedence	The IP precedence value. The range is from 0 to 7.
IP ToS	The IP ToS value. The range is from 0 to 15.
DSCP	The DSCP value. The range is from 0 to 63.

Step 8 To see the commands that will be applied on the device, click **Preview**.

You can view the commands in the Result tab. You can go back and make any required changes to the input parameters.

Step 9 To schedule the command, click the Scheduling tab. For more details on scheduling, see Scheduling a Command.

Step 10 To run the commands, click **Execute**.

Any errors are displayed in the Result tab.

Step 11 To close the dialog box, click **Close**.

Updating a SIP Adjacency

Use the Update SIP Adjacency command to update a SIP adjacency.

Step 1 In the inventory window, expand the Logical Inventory tree.

Step 2 Expand the Session Border Controller node.

Step 3 Expand the SBE node.

Step 4 Expand the SIP node.

Step 5 Click the Sip Adjacency node.

Step 6 In the Sip Adjacencies window, right-click a SIP adjacency and choose **Commands > Update > SIP Adjacency**. The SIP Adjacency dialog box opens.

Step 7 By default, the General tab is selected. Enter values for the following parameters.

Input Parameter	Description
Name	The name of the SIP adjacency.
Description	The description of the SIP adjacency.
Signaling Address	The local IPv4 signaling address of the SIP adjacency.
Signaling Port	The local signaling address port of the SIP adjacency. The range is from 1 to 65535; the default is 5060.
Signaling Peer	The remote signaling peer of the SIP adjacency.
Signaling Peer Port	The remote signaling peer's port of the SIP adjacency. The range is from 1 to 65535; the default is 5060.
Remote Address	The set of remote signaling peers that can be contacted over the adjacency with the specified IP address prefix.
Preferred Transport	The preferred transport protocol for SIP signaling on the adjacency.
Vrf	The value used to configure a SIP adjacency for a specific VPN. The adjacency receives incoming signaling from this VPN only. The adjacency's outgoing signaling is routed to the relevant Virtual Routing and Forwarding table (VRF).
Adjacency group	The adjacency group of the SIP adjacency. The maximum size is 32 characters.
Adjacency Account	The SIP adjacency account on an SBE.
Attach This Adjacency	Check this check box to attach the adjacency to an account on an SBE.

Step 8 Click the **Registration** tab. Enter values for the following parameters.

Input Parameter	Description
Enable Faster Register	Enables or disables fast-path register support on the SIP adjacency.
Faster Register Interval	The fast-path register interval, in seconds.
Register Minimum Expiry	The minimum registration period on the SIP adjacency, in seconds. The default is 3000 seconds.

Input Parameter	Description
Registration Target Address	The address to use when an outbound SIP register request rewriting occurs.
Registration Target Port	The port to use when an outbound SIP register request rewriting occurs.
Registration Rewrite Register	Enables or disables the SIP register request rewriting.

Step 9 Click the **Signalling Property** tab. Enter values for the following parameters.

Input Parameters	Description
Hold Media Timeout	The amount of time an SBE waits after receiving a media timeout notification from the DBE for an on-hold call before tearing that call down. The time is in milliseconds; the default value is 0.
Redirect Mode	Configures the behavior of the session border controller upon receipt of a 3xx response to an invitation from the SIP adjacency. Values are: • pass-through—Passes all 3xx responses back to the caller. • recurse—On 300, 301, 302, and 305 invite responses, the session border controller resends the invitation to the first listed contact address, or returns the 3xx response.
Redirect Limit	The maximum number of redirections that the session border controller performs on a call. The range is from 0 to 200 redirections; the default is 2.
NAT Force On	Enables NAT assuming.
Passthrough From Header	Enables the From header rewriting.
Passthrough To Header	Enables the To header rewriting.
Force Signaling Peer	Enables forcing the SIP message to go to the configured signaling peer.
SIP-I Passthrough	Enables a SIP adjacency for a SIP-I pass-through.
Outbound Flood Rate	The maximum desired rate of outbound request signals on the adjacency, excluding ACK/PRACK requests. The value is in signals per second.
Hunting Trigger	The failure return codes to trigger hunting for the adjacency.
Media Bypass	The SIP adjacency to allow media traffic to bypass the Data Border Element (DBE).
Security	The transport-level security to use on a SIP adjacency. Values are: • untrusted—(Default) The adjacency is not secure. • trusted-encrypted—Encrypted signaling is used to ensure security on the adjacency. • untrusted-encrypted—The adjacency is untrusted and uses SSL/TLS encryption. • trusted-unencrypted—A nonencryption mechanism is used to guarantee secure signaling for all messages on the adjacency.
Local Id Host	The local identity name—such as a DNS name—to present on outbound SIP messages.
Resource Priority Set	The name of the resource priority set used with the specified SIP adjacency.

Step 10 Click the **SIP Profile** tab. Enter values for the following parameters.

Input Parameters	Description
Inbound Method Profile	The name of the inbound method profile.
Outbound Method Profile	The name of the outbound method profile.
Inbound Header Profile	The name of the inbound header profile.
Outbound Header Profile	The name of the outbound header profile.
Proxy Inbound Option Profile	The name of the inbound proxy header profile for white/blacklisting options.
Proxy Outbound Option Profile	The name of the outbound proxy header profile for white/blacklisting options.
UA Inbound Option Profile	The name of the inbound UA header profile for white/blacklisting options.
UA Outbound Option Profile	The name of the outbound UA header profile for white/blacklisting options.

Step 11 Click the **Authentication** tab. Enter values for the following parameters.

Input Parameter	Description
Authentication Realm Inbound	The domain name of the inbound authentication realm.
Authentication Mode	Configures the authentication mode for a SIP adjacency.
Authentication Nonce Timeout	The authentication nonce timeout value, in seconds. The range is from 0 to 65535 seconds; the default is 300 seconds. **Note** Nonce is a hash value used to authenticate the user.

Step 12 Click the **UAS Failure Detection** tab. Enter values for the following parameters.

Input Parameters	Description
Enable Ping	Configures the adjacency to: • Poll its remote peer by sending SIP OPTIONS pings to it. • Enter the ping option submode. The default value is disabled.
Ping Interval	The interval between SIP OPTIONS pings that are sent to the remote peer. The range is from 1 to 2147483 seconds; the default is 32 seconds.
Ping Fail Count	The number of consecutive pings that must fail before the adjacencies peer is deemed to be unavailable. The range is from 1 to 4294967295; the default value is 3.
Ping Life Time	The duration for which the session border controller waits for a response to an options ping for the adjacency. The default is 32 seconds.

Step 13 Click the **P-CSCF** tab. Enter values for the following parameters.

Input Parameter	Description
Global SIP Inherit Profile	Configures the P-CSCF access inherit profile as the global profile. Values are: • preset-access—Specifies a preset access profile. • preset-core—(Default) Specifies a preset core profile. • preset-ibcf-ext-untrusted—Specifies a preset IBCF external untrusted profile. • preset-ibcf-external—Specifies a preset IBCF external profile. • preset-ibcf-internal—Specifies a preset IBCF internal profile. • preset-p-cscf-access—Specifies a preset P-CSCF access profile. • preset-p-cscf-core—Specifies a preset P-CSCF core profile. • preset-peering—Specifies a preset peering profile. • preset-standard-non-ims—Specifies a preset standard non-IMS profile.
SIP Adjacency Inherit Profile	Configures the SIP adjacency to use the P-CSCF access profile.
Visited Network Identifier	The network name of SIP adjacency.

Step 14 Click the **IBCF** tab. Enter values for the following parameters.

Input Parameter	Description
Global SIP Home Network Identifier	The specified domain name as the global home network identifier for use in all SIP IBCF adjacencies.
Global SIP Encryption Key	The global encryption key for all SIP IBCF adjacencies.
SIP Adjacency Inherit Profile	Specifies a preset IBCF internal profile.
SIP Adjacency Encryption Key	The encryption key on the SIP IBCF adjacency.
Sip Adjacency Home Network Identifier	The home network identifier on an IBCF adjacency.

Step 15 To see the commands that will be applied on the device, click **Preview**.

You can view the commands in the Result tab. You can go back and make any required changes to the input parameters.

Step 16 To schedule the command, click the Scheduling tab. For more details on scheduling, see Scheduling a Command.

Step 17 To run the commands, click **Execute**.

Any errors are displayed in the Result tab.

Step 18 To close the dialog box, click **Close**.

Updating a SIP Header Profile

Use the Update SIP Header Profile command to update a SIP header profile.

Step 1 In the inventory window, expand the Logical Inventory tree.

Step 2 Expand the Session Border Controller node.

Step 3 Expand the SBE node.

Step 4 Expand the SIP node.

Step 5 Expand the Sip Profile node.

Step 6 Click the Header Profile node.

Step 7 In the Sip Header Profiles window, right-click a header profile and choose **Commands > Update > SIP Header Profile**. The SIP Header Profile dialog box opens.

Step 8 By default, the General tab is selected. Enter values for the following parameters.

Input Parameter	Description
Name	The name of the SIP header profile to update.
Description	The description of the SIP header profile.
Profile Type	The type of SIP header profile. Values are: • Whitelist • Blacklist

Step 9 To see the commands that will be applied on the device, click **Preview**.

You can view the commands in the Result tab. You can go back and make any required changes to the input parameters.

Step 10 To schedule the command, click the Scheduling tab. For more details on scheduling, see Scheduling a Command.

Step 11 To run the commands, click **Execute**.

Any errors are displayed in the Result tab.

Step 12 To close the dialog box, click **Close**.

Updating a SIP Header Profile Entry

Use the Update SIP Header Profile Entry command to update an entry in a SIP header profile.

Step 1 In the inventory window, expand the Logical Inventory tree.

Step 2 Expand the Session Border Controller node.

Step 3 Expand the SBE node.

Step 4 Expand the SIP node.

Step 5 Expand the Sip Profile node.

Step 6 Click the Header Profile node. The Sip Header Profiles window opens.

Step 7 Double-click a header profile. The Sip Header Profile Properties window opens.

Step 8 Double-click a header. The Sip Header Profile Header Properties window opens.

Step 9 Right-click an entry and choose **Commands > Update > SIP Header Profile Entry**. The SIP Header Profile Entry dialog box opens.

Step 10 By default, the General tab is selected. Enter values for the following parameters.

Input Parameter	Description
Entry Number	The entry number for the header profile.
Action Type	The action type of the entry.
Action Value	The action value for the action type.
Conditions	The condition type.
Parameter Profile	The parameter profile used by the header entry.

Step 11 To see the commands that will be applied on the device, click **Preview**.

You can view the commands in the Result tab. You can go back and make any required changes to the input parameters.

Step 12 To schedule the command, click the Scheduling tab. For more details on scheduling, see Scheduling a Command.

Step 13 To run the commands, click **Execute**.

Any errors are displayed in the Result tab.

Step 14 To close the dialog box, click **Close**.

Updating a SIP Option Profile

Use the Update SIP Option Profile command to update a SIP option profile.

Step 1 In the inventory window, expand the Logical Inventory tree.

Step 2 Expand the Session Border Controller node.

Step 3 Expand the SBE node.

Step 4 Expand the SIP node.

Step 5 Expand the Sip Profile node.

Step 6 Click the Option Profile node.

Step 7 In the Sip Option Profiles window, right-click a profile and choose **Commands > Update > SIP Option Profile**. The SIP Option Profile dialog box opens.

Step 8 By default, the General tab is selected. Enter values for the following parameters.

Input Parameter	Description
Name	The name of the SIP option profile to update.
Description	The description of the SIP option profile.
Profile Type	The type of SIP option profile. Values are: • Whitelist • Blacklist
Profile Options	The options of the SIP option profile. Multiple options are separated by one space; for example: host user-agent

Step 9 To see the commands that will be applied on the device, click **Preview**.

You can view the commands in the Result tab. You can go back and make any required changes to the input parameters.

Step 10 To schedule the command, click the Scheduling tab. For more details on scheduling, see Scheduling a Command.

Step 11 To run the commands, click **Execute**.

Any errors are displayed in the Result tab.

Step 12 To close the dialog box, click **Close**.

Updating a Parameter in a SIP Parameter Profile

Use the Update SIP Parameter Profile Parameter command to update a parameter in a SIP parameter profile.

Step 1 In the inventory window, expand the Logical Inventory tree.

Step 2 Expand the Session Border Controller node.

Step 3 Expand the SBE node.

Step 4 Expand the SIP node.

Step 5 Expand the Sip Profile node.

Step 6 Click the Parameter Profile node.

Step 7 In the Sip Parameter Profiles window, double-click a profile. The Sip Parameter Profile Properties window opens.

Step 8 Right-click a parameter and choose **Commands > Update > SIP Parameter Profile Parameter**. The SIP Parameter Profile Parameter dialog box opens.

Step 9 By default, the General tab is selected. Enter values for the following parameters.

Input Parameter	Description
Parameter Name	The name of the parameter to update.
Action	The action. Values are: • add-not-present • add-or-replace • strip
Value	The value of the action. Values are: • private-ip-address • public-ip-address • A user-defined word

Step 10 To see the commands that will be applied on the device, click **Preview**.

You can view the commands in the Result tab. You can go back and make any required changes to the input parameters.

Step 11 To schedule the command, click the Scheduling tab. For more details on scheduling, see Scheduling a Command.

Step 12 To run the commands, click **Execute**.

Any errors are displayed in the Result tab.

Step 13 To close the dialog box, click **Close**.

Updating SIP Adjacency Outbound AuthRealm

Use the Update Sip Adjacency Outbound AuthRealm command to update a SIP adjacency outbound authentication realm.

Step 1 In the inventory window, expand the Logical Inventory tree.

Step 2 Expand the Session Border Controller node.

Step 3 Expand the SBE node.

Step 4 Expand the SIP node.

Step 5 Click the Sip Adjacency node.

Step 6 In the Sip Adjacencies window, right-click the SIP adjacency instance and choose **Commands > Update > SIP Adjacency Outbound AuthRealm**. The SIP Adjacency Outbound AuthRealm dialog box opens.

Step 7 By default, the General tab is selected. Enter values for the following parameters.

Input Parameter	Description
Domain	The domain name for which the authentication credentials are valid.
Username	The username that identifies the SBC in the specified domain.
Password	The password to authenticate the username in the specified domain.

Step 8 To see the commands that will be applied on the device, click **Preview**.You can view the commands in the Result tab. You can go back and make any required changes to the input parameters.

Step 9 To schedule the command, click the Scheduling tab. For more details on scheduling, see Scheduling a Command.

Step 10 To run the commands, click **Execute**.Any errors are displayed in the Result tab.

Step 11 To close the dialog box, click **Close**.

Monitoring the Performance of SBC Components

The following commands facilitate performance monitoring of SBC components.

- Showing SBC CPS Data
- Showing SBC Components
- Showing SBC Current 15 Minute Stats
- Showing SBC Current 5 Minute Stats
- Showing SBC Current Day Stats
- Showing SBC Current Hour Stats
- Showing SBC H248 Stats
- Showing SBC Previous 15 Minute Stats
- Showing SBC Previous 5 Minute Stats
- Showing SBC Previous Day Stats
- Showing SBC Previous Hour Stats
- Showing SBC Media Stats

Note In the GUI, parameters that are displayed in bold text are mandatory.

Showing SBC CPS Data

Step 1 In the inventory window, expand the Logical Inventory tree.

Step 2 Expand the Session Border Controller node.

Step 3 Right-click the SBE node and choose **Commands > Show > PM > CPS Data**. The Show CPS Controller dialog box opens and displays values for current, minimum, maximum, and average CPS.

Step 4 To see the commands that will be applied on the device, click **Preview**.

You can view the commands in the Result tab. You can go back and make any required changes to the input parameters.

Step 5 To schedule the command, click the Scheduling tab. For more details on scheduling, see Scheduling a Command.

Step 6 To run the commands, click **Execute**.

Any errors are displayed in the Result tab.

Step 7 To close the dialog box, click **Close**.

Showing SBC Components

Step 1 In the inventory window, expand the Logical Inventory tree.

Step 2 Expand the Session Border Controller node.

Step 3 Right-click the SBE node and choose **Commands > Show > Components**. The Components dialog box opens and lets you select the component type.

Step 4 To see the commands that will be applied on the device, click **Preview**.

You can view the commands in the Result tab. You can go back and make any required changes to the input parameters.

Step 5 To schedule the command, click the Scheduling tab. For more details on scheduling, see Scheduling a Command.

Step 6 To run the commands, click **Execute**.

Any errors are displayed in the Result tab.

Step 7 To close the dialog box, click **Close**.

Showing SBC Current 15 Minute Stats

Step 1 In the inventory window, expand the Logical Inventory tree.

Step 2 Expand the Session Border Controller node.

Step 3 Right-click the SBE node and choose **Commands > Show > PM > Current 15 Min Statistics**.

Step 4 To see the commands that will be applied on the device, click **Preview**.

You can view the commands in the Result tab. You can go back and make any required changes to the input parameters.

Step 5 To schedule the command, click the Scheduling tab. For more details on scheduling, see Scheduling a Command.

Step 6 To run the commands, click **Execute**.

Any errors are displayed in the Result tab.

Step 7 To close the dialog box, click **Close**.

Showing SBC Current 5 Minute Stats

Step 1 In the inventory window, expand the Logical Inventory tree.

Step 2 Expand the Session Border Controller node.

Step 3 Right-click the SBE node and choose **Commands > Show > PM > Current 5 Min Statistics**.

Step 4 To see the commands that will be applied on the device, click **Preview**.

You can view the commands in the Result tab. You can go back and make any required changes to the input parameters.

Step 5 To schedule the command, click the Scheduling tab. For more details on scheduling, see Scheduling a Command.

Step 6 To run the commands, click **Execute**.

Any errors are displayed in the Result tab.

Step 7 To close the dialog box, click **Close**.

Showing SBC Current Day Stats

Step 1 In the inventory window, expand the Logical Inventory tree.

Step 2 Expand the Session Border Controller node.

Step 3 Right-click the SBE node and choose **Commands > Show > PM > Current Day Statistics**.

Step 4 To see the commands that will be applied on the device, click **Preview**.

You can view the commands in the Result tab. You can go back and make any required changes to the input parameters.

Step 5 To schedule the command, click the Scheduling tab. For more details on scheduling, see Scheduling a Command.

Step 6 To run the commands, click **Execute**.

Any errors are displayed in the Result tab.

Step 7 To close the dialog box, click **Close**.

Showing SBC Current Hour Stats

Step 1 In the inventory window, expand the Logical Inventory tree.

Step 2 Expand the Session Border Controller node.

Step 3 Right-click the SBE node and choose **Commands > Show > PM > Current Hour Statistics**.

Step 4 To see the commands that will be applied on the device, click **Preview**.You can view the commands in the Result tab. You can go back and make any required changes to the input parameters.

Step 5 To schedule the command, click the Scheduling tab. For more details on scheduling, see Scheduling a Command.

Step 6 To run the commands, click **Execute**. Any errors are displayed in the Result tab.

Step 7 To close the dialog box, click **Close**.

Showing SBC H248 Stats

Step 1 In the inventory window, expand the Logical Inventory tree.

Step 2 Expand the Session Border Controller node.

Step 3 Right-click the SBE node and choose **Commands > Show > PM > H.248 Statistics**. The Show Stats H248 Controller dialog box opens and displays the number of:

- Requests sent
- Requests received
- Requests failed
- Requests retried
- Replies sent
- Replies received
- Replies retried

Step 4 To see the commands that will be applied on the device, click **Preview**.

You can view the commands in the Result tab. You can go back and make any required changes to the input parameters.

Step 5 To schedule the command, click the Scheduling tab. For more details on scheduling, see Scheduling a Command.

Step 6 To run the commands, click **Execute**.

Any errors are displayed in the Result tab.

Step 7 To close the dialog box, click **Close**.

Showing SBC Previous 15 Minute Stats

Step 1 In the inventory window, expand the Logical Inventory tree.

Step 2 Expand the Session Border Controller node.

Step 3 Right-click the SBE node and choose **Commands > Show > PM > Previous 15 Minutes Statistics**.

Step 4 To see the commands that will be applied on the device, click **Preview**.

You can view the commands in the Result tab. You can go back and make any required changes to the input parameters.

Step 5 To schedule the command, click the Scheduling tab. For more details on scheduling, see Scheduling a Command.

Step 6 To run the commands, click **Execute**.

Any errors are displayed in the Result tab.

Step 7 To close the dialog box, click **Close**.

Showing SBC Previous 5 Minute Stats

Step 1 In the inventory window, expand the Logical Inventory tree.

Step 2 Expand the Session Border Controller node.

Step 3 Right-click the SBE node and choose **Commands > Show > PM > Previous 5 Minutes Statistics**.

Step 4 To see the commands that will be applied on the device, click **Preview**.

You can view the commands in the Result tab. You can go back and make any required changes to the input parameters.

Step 5 To schedule the command, click the Scheduling tab. For more details on scheduling, see Scheduling a Command.

Step 6 To run the commands, click **Execute**.

Any errors are displayed in the Result tab.

Step 7 To close the dialog box, click **Close**.

Showing SBC Previous Day Stats

Step 1 In the inventory window, expand the Logical Inventory tree.

Step 2 Expand the Session Border Controller node.

Step 3 Right-click the SBE node and choose **Commands > Show > PM > Previous Day Statistics**.

Step 4 To see the commands that will be applied on the device, click **Preview**.

You can view the commands in the Result tab. You can go back and make any required changes to the input parameters.

Step 5 To schedule the command, click the Scheduling tab. For more details on scheduling, see Scheduling a Command.

Step 6 To run the commands, click **Execute**.

Any errors are displayed in the Result tab.

Step 7 To close the dialog box, click **Close**.

Showing SBC Previous Hour Stats

Step 1 In the inventory window, expand the Logical Inventory tree.

Step 2 Expand the Session Border Controller node.

Step 3 Right-click the SBE node and choose **Commands > Show > PM > Previous Hour Statistics**.

Step 4 To see the commands that will be applied on the device, click **Preview**.

You can view the commands in the Result tab. You can go back and make any required changes to the input parameters.

Step 5 To schedule the command, click the Scheduling tab. For more details on scheduling, see Scheduling a Command.

Step 6 To run the commands, click **Execute**.

Any errors are displayed in the Result tab.

Step 7 To close the dialog box, click **Close**.

Showing SBC Media Stats

Step 1 In the inventory window, expand the Logical Inventory tree.

Step 2 Expand the Session Border Controller node.

Step 3 Right-click the SBE node and choose **Commands > Show > Media Statistics**. The Show Stats Media Controller dialog box opens and displays values for available bandwidth, available flows, and media count numbers.

Step 4 To see the commands that will be applied on the device, click **Preview**.

You can view the commands in the Result tab. You can go back and make any required changes to the input parameters.

Step 5 To schedule the command, click the Scheduling tab. For more details on scheduling, see Scheduling a Command.

Step 6 To run the commands, click **Execute**.

Any errors are displayed in the Result tab.

Step 7 To close the dialog box, click **Close**.



CHAPTER 27

Using the DWDM and SONET Commands

The Cisco IP over dense wavelength division multiplexing (IPoDWDM) solution enables the convergence of the IP and DWDM core networks of the service providers. It increases service flexibility, operational efficiency and reliability while lowering operating expenses (OpEx) and capital expenditures (CapEx).

Cisco Prime Network discovers and displays the following DWDM attributes in the Physical Inventory tree of the Cisco Prime Network Vision

- DWDM controllers. The controller location is same as the DWDM interface.
- Loopback information for the DWDM controller.
- DWDM controller status.
- DWDM port properties—Wavelength, Laser Status, Tx Power, and Rx Power.
- DWDM controller card status (G.709 status).

See the *Cisco Prime Network 3.9 User Guide* for more details on the physical and logical inventory information for the device.

Prime Network provides commands that support DWDM and Synchronous Optical Network (SONET) controllers. These commands help in configuring the device and in displaying device details.

Supported Network Elements

You can run the DWDM commands on the following network elements:

- Cisco 7600 Series Routers
- Cisco CRS Carrier Routing System

  Cisco CRS series includes Cisco CRS-1 and Cisco CRS-3 Carrier Routing Systems.
- Cisco IOS 12000 Series Gigabit Switch Router (GSR)

You can run the SONET commands on the following network elements:

- Cisco 7600 Series Routers
- Cisco CRS Carrier Routing System

  Cisco CRS series includes Cisco CRS-1 and Cisco CRS-3 Carrier Routing Systems.
- Cisco IOS 12000 Series GSR

See the “Cisco VNEs” section in this guide for details on the network element software versions that Prime Network supports. To run the DWDM and SONET commands, the software on the network element must support the DWDM and SONET technology.

Running SONET Commands

The following sections provide details about the tasks that you can perform by running the SONET commands:

Note In the GUI, parameters that are displayed in bold text are mandatory.

- Displaying BER Threshold, page 27-2
- Displaying SONET Controller Data, page 27-3
- Displaying TCA Threshold, page 27-3
- Displaying Line PM Counters, page 27-3
- Displaying Medium PM Counters, page 27-4
- Displaying Path PM Counters, page 27-4
- Displaying Section PM Counters, page 27-5
- Displaying Trace Details, page 27-6
- Clearing SONET Counters, page 27-6
- Setting BER Threshold, page 27-7
- Setting Clock Source, page 27-7
- Setting TCA Threshold, page 27-8

Displaying BER Threshold

Use the BER Threshold command to display the bit error rate (BER) threshold details.

Step 1 In the inventory window, expand the Physical Inventory tree, then right-click the SONET port.

Step 2 Choose **Commands > SONET > Show > BER Threshold** from the popup menu.

The BER Threshold window is displayed.

Step 3 To see how the command, including variables, looks before it is executed, click **Preview**.

Step 4 To schedule the command, click the Scheduling tab. For more details on scheduling, see Scheduling a Command.

Step 5 To run the command, click **Execute**.

The Result tab displays the actual interaction of the command in the output console.

Step 6 To close the window, click **Close**.

Displaying SONET Controller Data

Use the show SONET Controller Data command to display SONET controller data.

Step 1 In the inventory window, expand the Physical Inventory tree, then right-click the SONET port.

Step 2 Choose **Commands > SONET > Show > Controller Data** from the popup menu.

The Controller Data window is displayed.

Step 3 To see how the command, including variables, looks before it is executed, click **Preview**.

Step 4 To schedule the command, click the Scheduling tab. For more details on scheduling, see Scheduling a Command.

Step 5 To run the command, click **Execute**.

The Result tab displays the actual interaction of the command in the output console.

Step 6 To close the window, click **Close**.

Displaying TCA Threshold

Use the show SONET TCA Threshold command to display SONET threshold crossing alert (TCA) thresholds.

Step 1 In the inventory window, expand the Physical Inventory tree, then right-click the SONET port.

Step 2 Choose **Commands > SONET > Show > TCA Threshold** from the popup menu.

The TCA Threshold window is displayed.

Step 3 To see how the command, including variables, looks before it is executed, click **Preview**.

Step 4 To schedule the command, click the Scheduling tab. For more details on scheduling, see Scheduling a Command.

Step 5 To run the command, click **Execute**.

The Result tab displays the actual interaction of the command in the output console.

Step 6 To close the window, click **Close**.

Displaying Line PM Counters

Use the show SONET Line Performance Measurement (PM) Counters command to display SONET Line PM counters.

Step 1 In the inventory window, expand the Physical Inventory tree, then right-click the SONET port.

Step 2 Choose **Commands > SONET > Show > PM > Line Counters** from the popup menu.

The Line Counters dialog box is displayed.

Step 3 Enter values for the following parameters.

Input Parameter	Description
Line Option	The line type. Values are: • farendline • farendline-history • line • line-history
History Interval (1 to 96, or 0 for all)	The interval for the history. Value in the range from 1 to 96 (to view the details of a particular interval), or 0 (to view the details of all intervals).

Step 4 To see how the command, including variables, looks before it is executed, click **Preview**.

Step 5 To schedule the command, click the Scheduling tab. For more details on scheduling, see Scheduling a Command.

Step 6 To run the command, click **Execute**.

The Result tab displays the actual interaction of the command in the output console.

Step 7 To close the window, click **Close**.

Displaying Medium PM Counters

Use the show SONET Medium PM Counters command to display the SONET Medium PM counters.

Step 1 In the inventory window, expand the Physical Inventory tree, then right-click the SONET port.

Step 2 Choose **Commands > SONET > Show > PM > Medium Counters** from the popup menu.

The Medium Counters window is displayed.

Step 3 To see how the command, including variables, looks before it is executed, click **Preview**.

Step 4 To schedule the command, click the Scheduling tab. For more details on scheduling, see Scheduling a Command.

Step 5 To run the command, click **Execute**.

The Result tab displays the actual interaction of the command in the output console.

Step 6 To close the window, click **Close**.

Displaying Path PM Counters

Use the show SONET Path PM Counters command to display the SONET Path PM counters.

Step 1 In the inventory window, expand the Physical Inventory tree, then right-click the SONET port.

Step 2 Choose **Commands > SONET > Show > PM > Path Counters** from the popup menu.

The Path Counters window is displayed.

Step 3 Enter values for the following parameters.

Input Parameter	Description
Path Option	The path type. Values are: • farendpath • farendpath-history • path • path-history
Channelized Path Index (1 to 48, or 0 for all)	The channel number. Value in the range from 1 to 48 (to view the details of a particular channel), or 0 (to view the details of all channels).
History Interval (1 to 96, or 0 for all)	The interval for the history. Value in the range from 1 to 96 (to view the details of a particular interval), or 0 (to view the details of all intervals).

Step 4 To see how the command, including variables, looks before it is executed, click **Preview**.

Step 5 To schedule the command, click the Scheduling tab. For more details on scheduling, see Scheduling a Command.

Step 6 To run the command, click **Execute**.

The Result tab displays the actual interaction of the command in the output console.

Step 7 To close the window, click **Close**.

Displaying Section PM Counters

Use the show SONET Section PM Counters command to display the SONET Section PM counters.

Step 1 In the inventory window, expand the Physical Inventory tree, then right-click the SONET port.

Step 2 Choose **Commands > SONET > Show > PM > Section Counters** from the popup menu.

The Section Counters window is displayed.

Step 3 Enter values for the following parameters.

Input Parameter	Description
Section Option	The section type. Values are: • section • section-history
History Interval (1 to 96, or 0 for all)	The interval for the history. Value in the range from 1 to 96 (to view the details of a particular interval), or 0 (to view the details of all intervals).

Step 4 To see how the command, including variables, looks before it is executed, click **Preview**.

Step 5 To schedule the command, click the Scheduling tab. For more details on scheduling, see Scheduling a Command.

Step 6 To run the command, click **Execute**.

The Result tab displays the actual interaction of the command in the output console.

Step 7 To close the window, click **Close**.

Displaying Trace Details

Use the show SONET Trace details command to display the SONET trace details for card location.

Note You can run this command only if the device is managed by Prime Network with device admin privilege.

Step 1 In the inventory window, expand the Physical Inventory tree, then right-click the SONET port.

Step 2 Choose **Commands > SONET > Show > Trace Details** from the popup menu.

The Trace Details window is displayed.

Step 3 Enter a value for the following parameter.

Input Parameter	Description
Location	The card location; for example, 0/5/CPU0

Step 4 To see how the command, including variables, looks before it is executed, click **Preview**.

Step 5 To schedule the command, click the Scheduling tab. For more details on scheduling, see Scheduling a Command.

Step 6 To run the command, click **Execute**.

The Result tab displays the actual interaction of the command in the output console.

Step 7 To close the window, click **Close**.

Clearing SONET Counters

Use the Clear SONET Counters command to clear the SONET counters.

Step 1 In the inventory window, expand the Physical Inventory tree, then right-click the SONET port.

Step 2 Choose **Commands > SONET > Clear > SONET > SDH Counters** from the popup menu.

The SDH Counters window is displayed.

Step 3 To see how the command, including variables, looks before it is executed, click **Preview**.

Step 4 To schedule the command, click the Scheduling tab. For more details on scheduling, see Scheduling a Command.

Step 5 To run the command, click **Execute**.

The Result tab displays the actual interaction of the command in the output console.

Step 6 To close the window, click **Close**.

Setting BER Threshold

Use the Configure SONET BER Threshold command to set the BER threshold values of the specified alarms for a SONET controller.

Step 1 In the inventory window, expand the Physical Inventory tree, then right-click the SONET port.

Step 2 Choose **Commands > SONET > Configure > BER Threshold** from the popup menu.

The BER Threshold dialog box is displayed.

Step 3 Enter values for the following parameters.

Input Parameter	Description
BER Threshold	The BER threshold value. Values are: • sf-ber—Sets the signal degrade BER threshold. Value in the range from 3 to 9. The default value is 6. • sd-ber—Sets the signal failure BER threshold. Value in the range from 3 through 9. The default value is 3.
Bit Error Rate (3 to 9)	Bit error rate. Value in the range from 3 to 9, or default. • The default value for sd-ber is 6. • The default value for sf-ber is 3.

Step 4 To see how the command, including variables, looks before it is executed, click **Preview**.

Step 5 To schedule the command, click the Scheduling tab. For more details on scheduling, see Scheduling a Command.

Step 6 To run the command, click **Execute**.The Result tab displays the actual interaction of the command in the output console.

Step 7 To close the window, click **Close**.

Setting Clock Source

Use the Configure SONET Clock Source command to set the clock source of the sent signal on SONET ports.

Step 1 In the inventory window, expand the Physical Inventory tree, then right-click the SONET port.

Step 2 Choose **Commands > SONET > Configure > Clock Source** from the popup menu.

The Clock Source dialog box is displayed.

Step 3 Enter a value for the following parameter.

Input Parameter	Description
Clock Source	The clock source of the sent signal on SONET ports. Values are: • internal—Specifies that the controller will clock its sent data from its internal clock. • line—(Default) Specifies that the controller will clock its sent data from a clock recovered from the receive data stream of the line. • default—Cancels a clock source setting.

Step 4 To see how the command, including variables, looks before it is executed, click **Preview**.

Step 5 To schedule the command, click the Scheduling tab. For more details on scheduling, see Scheduling a Command.

Step 6 To run the command, click **Execute**.

The Result tab displays the actual interaction of the command in the output console.

Step 7 To close the window, click **Close**.

Setting TCA Threshold

Use the Configure SONET TCA Threshold command to set the BER TCA values of the specified alarms for a SONET controller.

Step 1 In the inventory window, expand the Physical Inventory tree, then right-click the SONET port.

Step 2 Choose **Commands > SONET > Configure > TCA Threshold** from the popup menu.

The TCA Threshold dialog box is displayed.

Step 3 Enter values for the following parameters.

Input Parameters	Description
TCA Threshold	The TCA threshold. Values are: • b1-tca—Sets the B1 BER TCA. Value in the range from 3 to 9. The default value is 6. • b2-tca—Sets the B2 BER TCA. Value in the range from 3 to 9. The default value is 6.
Bit Error Rate (3 to 9)	The bit error rate. Value in the range from 3 to 9 (10 to the minus *x*), or default.

Step 4 To see how the command, including variables, looks before it is executed, click **Preview**.

Step 5 To schedule the command, click the Scheduling tab. For more details on scheduling, see Scheduling a Command.

Step 6 To run the command, click **Execute**.

The Result tab displays the actual interaction of the command in the output console.

Step 7 To close the window, click **Close**.

Running DWDM Commands

The following sections provide details about the tasks that you can perform by running the DWDM commands:

Note In the GUI, parameters that are displayed in bold text are mandatory.

- Displaying DWDM Controller Data, page 27-10
- Displaying DWDM PM History Data, page 27-10
- Displaying DWDM RTPM Counters, page 27-11
- Displaying DWDM RTPM Threshold, page 27-11
- Displaying DWDM Wavelength Map, page 27-12
- Clearing DWDM Counters, page 27-12
- Setting DWDM Channel, page 27-13
- Setting DWDM FEC Mode, page 27-13
- Setting DWDM G.709 ODU, page 27-14
- Setting DWDM G.709 OTU, page 27-14
- Setting DWDM G.709 TTI, page 27-15
- Setting DWDM G.709 Wrapper, page 27-16
- Setting DWDM Laser State, page 27-17
- Setting DWDM Loopback, page 27-17
- Setting DWDM PM FEC Data, page 27-18
- Setting DWDM PM Optics Data, page 27-19
- Setting DWDM PM OTN Data, page 27-20
- Setting DWDM Transmit Power, page 27-21
- Setting Rx LOS Threshold, page 27-22
- Displaying IM Trace Details, page 27-23
- Displaying Device Log, page 27-23

Displaying DWDM Controller Data

Use the Show DWDM Controller Data command to display the complete details about the DWDM controller.

Step 1 In the inventory window, expand the Physical Inventory tree, then right-click the DWDM port.

Step 2 Choose **Commands > IPODWDM > Show > Controller Data** from the popup menu.

The Controller Data window is displayed.

Step 3 To see how the command, including variables, looks before it is executed, click **Preview**.

Step 4 To schedule the command, click the Scheduling tab. For more details on scheduling, see Scheduling a Command.

Step 5 To run the command, click **Execute**.

The Result tab displays the actual interaction of the command in the output console.

Step 6 To close the window, click **Close**.

Displaying DWDM PM History Data

Use the Show DWDM Controller Data to display PM history in 15-minute or 24-hour buckets.

Step 1 In the inventory window, expand the Physical Inventory tree, then right-click the DWDM port.

Step 2 Choose **Commands > IPODWDM > Show > PM History Data** from the popup menu.

The PM History Data window is displayed.

Step 3 Enter values for the following parameters.

Input Parameter	Description
PM Interval	PM interval type. Values are: • 15-min • 24-hour
Interval	The interval number.

Step 4 To see how the command, including variables, looks before it is executed, click **Preview**.

Step 5 To schedule the command, click the Scheduling tab. For more details on scheduling, see Scheduling a Command.

Step 6 To run the command, click **Execute**.

The Result tab displays the actual interaction of the command in the output console.

Step 7 To close the window, click **Close**.

Displaying DWDM RTPM Counters

Use the Show DWDM RTPM Counters command to display PM counters for Forward Error Correction (FEC), optical, and Optical Transport Network (OTN) layers.

Step 1 In the inventory window, expand the Physical Inventory tree, then right-click the DWDM port.

Step 2 Choose **Commands > IPODWDM > Show > RTPM Counters** from the popup menu.

The RTPM Counters window is displayed.

Step 3 Enter values for the following parameter.

Input Parameter	Description
PM Interval	The PM interval type. Values are: • 15-min • 24-hour

Step 4 To see how the command, including variables, looks before it is executed, click **Preview**.

Step 5 To schedule the command, click the Scheduling tab. For more details on scheduling, see Scheduling a Command.

Step 6 To run the command, click **Execute**.

The Result tab displays the actual interaction of the command in the output console.

Step 7 To close the window, click **Close**.

Displaying DWDM RTPM Threshold

Use the DWDM RTPM Threshold command to display TCA thresholds for FEC, optical, and OTN layers.

Step 1 In the inventory window, expand the Physical Inventory tree, then right-click the DWDM port.

Step 2 Choose **Commands > IPODWDM > Show > RTPM Threshold** from the popup menu.

The RTPM Threshold window is displayed.

Step 3 Enter values for the following parameter.

Input Parameter	Description
PM Interval	The PM interval type. Values are: • 15-min • 24-hour

Step 4 To see how the command, including variables, looks before it is executed, click **Preview**.

Step 5 To schedule the command, click the Scheduling tab. For more details on scheduling, see Scheduling a Command.

Step 6 To run the command, click **Execute**.

The Result tab displays the actual interaction of the command in the output console.

Step 7 To close the window, click **Close**.

Displaying DWDM Wavelength Map

Use the Show DWDM Wavelength Map command to display the available wavelength map for the DWDM controller.

Step 1 In the inventory window, expand the Physical Inventory tree, then right-click the DWDM port.

Step 2 Choose **Commands > IPODWDM > Show > Wavelength Map** from the popup menu.

The Wavelength Map window is displayed.

Step 3 To see how the command, including variables, looks before it is executed, click **Preview**.

Step 4 To schedule the command, click the Scheduling tab. For more details on scheduling, see Scheduling a Command.

Step 5 To run the command, click **Execute**.

The Result tab displays the actual interaction of the command in the output console.

Step 6 To close the window, click **Close**.

Clearing DWDM Counters

Use the Clear DWDM Counters command to clear the DWDM counters.

Step 1 In the inventory window, expand the Physical Inventory tree, then right-click the DWDM port.

Step 2 Choose **Commands > IPODWDM > Clear > Counters** from the popup menu.

The Counters window is displayed.

Step 3 To see how the command, including variables, looks before it is executed, click **Preview**.

Step 4 To schedule the command, click the Scheduling tab. For more details on scheduling, see Scheduling a Command.

Step 5 To run the command, click **Execute**.

The Result tab displays the actual interaction of the command in the output console.

Step 6 To close the window, click **Close**.

Setting DWDM Channel

Use the Configure DWDM Channel command to configure the channel number corresponding to the first wavelength and to reset the channel back to the default.

Step 1 In the inventory window, expand the Physical Inventory tree, then right-click the DWDM port.

Step 2 Choose **Commands > IPODWDM > Configure > Channel** from the popup menu.

The Channel dialog box is displayed.

Step 3 Enter values for the following parameters.

Input parameters	Description
Channel Number	The channel number.
Option	Specifies whether to set or reset the channel.

Step 4 To see how the command, including variables, looks before it is executed, click **Preview**.

Step 5 To schedule the command, click the Scheduling tab. For more details on scheduling, see Scheduling a Command.

Step 6 To run the command, click **Execute**.

The Result tab displays the actual interaction of the command in the output console.

Step 7 To close the window, click **Close**.

Setting DWDM FEC Mode

Use the Configure DWDM FEC Mode to configure forward error correction (FEC) mode.

Step 1 In the inventory window, expand the Physical Inventory tree, then right-click the DWDM port.

Step 2 Choose **Commands > IPODWDM > Configure > FEC Mode** from the popup menu.

The FEC Mode dialog box is displayed.

Step 3 Enter the value for the following parameter.

Input Parameter	Description
G709 FEC Mode	The G709 FEC mode. Values are: • Disabled • Enhanced • Standard

Step 4 To see how the command, including variables, looks before it is executed, click **Preview**.

Step 5 To schedule the command, click the Scheduling tab. For more details on scheduling, see Scheduling a Command.

Step 6 To run the command, click **Execute**.

The Result tab displays the actual interaction of the command in the output console.

Step 7 To close the window, click **Close**.

Setting DWDM G.709 ODU

Use the Configure DWDM G.709 ODU command to configure the logging of selected optical channel data unit (ODU) alarms to the console.

Step 1 In the inventory window, expand the Physical Inventory tree, then right-click the DWDM port.

Step 2 Choose **Commands > IPODWDM > Configure > G.709 ODU** from the popup menu.

The G.709 ODU dialog box is displayed.

Step 3 Enter the values for the following parameters.

Input Parameter	Description
ODU Alarm Type	The ODU alarm type. Values are: • ais • bdi • lck • oci • ptim • oci • tim
Option	Specifies whether to enable or disable the alarm type.

Step 4 To see how the command, including variables, looks before it is executed, click **Preview**.

Step 5 To schedule the command, click the Scheduling tab. For more details on scheduling, see Scheduling a Command.

Step 6 To run the command, click **Execute**.

The Result tab displays the actual interaction of the command in the output console.

Step 7 To close the window, click **Close**.

Setting DWDM G.709 OTU

Use the Configure DWDM G.709 OTU command to configure the logging of selected optical channel transport unit (OTU) alarms to the console.

Step 1 In the inventory window, expand the Physical Inventory tree, then right-click the DWDM port.

Step 2 Choose **Commands > IPODWDM > Configure > G.709 OTU** from the popup menu.

The G.709 OTU dialog box is displayed.

Step 3 Enter values for the following parameters.

Input Parameter	Description
OTU Alarm Type	The OTU alarm type. Values are: • bdi • fecmismatch • iae • lof • lom • los • sd-ber • sf-ber • tim
Option	Specifies whether to enable or disable the alarm type.

Step 4 To see how the command, including variables, looks before it is executed, click **Preview**.

Step 5 To schedule the command, click the Scheduling tab. For more details on scheduling, see Scheduling a Command.

Step 6 To run the command, click **Execute**.

The Result tab displays the actual interaction of the command in the output console.

Step 7 To close the window, click **Close**.

Setting DWDM G.709 TTI

Use the Configure DWDM G.709 TTI command to configure a transmit or expected Trail Trace Identifier (TTI).

Step 1 In the inventory window, expand the Physical Inventory tree, then right-click the DWDM port.

Step 2 Choose **Commands > IPODWDM > Configure > G.709 TTI** from the popup menu.

The G.709 TTI dialog box is displayed.

Step 3 Enter values for the following parameters.

Input Parameter	Description
Optical Channel Unit Type	The optical channel unit type. Values are: • ODU • OTU
TTI Type	The TTI type. Values are: • Expected • Sent
TTI String Type	The TTI string type. Values are: • ASCII • HEX
TTI String	The TTI string.
Option	Specifies whether to set or reset the TTI string. Values are: • Reset TTI string • Set TTI String

Step 4 To see how the command, including variables, looks before it is executed, click **Preview**.

Step 5 To schedule the command, click the Scheduling tab. For more details on scheduling, see Scheduling a Command.

Step 6 To run the command, click **Execute**.

The Result tab displays the actual interaction of the command in the output console.

Step 7 To close the window, click **Close**.

Setting DWDM G.709 Wrapper

Use the Configure DWDM G.709 Wrapper command to disable the G.709 wrapper and re-enable it.

Step 1 In the inventory window, expand the Physical Inventory tree, then right-click the DWDM port.

Step 2 Choose **Commands > IPODWDM > Configure > G.709 Wrapper** from the popup menu.

The G.709 Wrapper dialog box is displayed.

Step 3 Enter the value for the following parameter.

Input Parameter	Description
Option	Specifies whether to disable or enable G.709 wrapper. Values are: • Disable G.709 wrapper • Enable G.709 wrapper

Step 4 To see how the command, including variables, looks before it is executed, click **Preview**.

Step 5 To schedule the command, click the Scheduling tab. For more details on scheduling, see Scheduling a Command.

Step 6 To run the command, click **Execute**.

The Result tab displays the actual interaction of the command in the output console.

Step 7 To close the window, click **Close**.

Setting DWDM Laser State

Use the Configure DWDM Laser State command to configure the laser state.

Step 1 In the inventory window, expand the Physical Inventory tree, then right-click the DWDM port.

Step 2 Choose **Commands > IPODWDM > Configure > Laser State** from the popup menu.

The Laser State dialog box is displayed.

Step 3 Enter the value for the following parameter.

Input Parameter	Descriptions
Laser State	Specifies whether to switch off or switch on the laser. Values are: • Off • On

Step 4 To see how the command, including variables, looks before it is executed, click **Preview**.

Step 5 To schedule the command, click the Scheduling tab. For more details on scheduling, see Scheduling a Command.

Step 6 To run the command, click **Execute**.

The Result tab displays the actual interaction of the command in the output console.

Step 7 To close the window, click **Close**.

Setting DWDM Loopback

Use the Configure DWDM Loopback command to configure loopback and reset loopback back to none.

Step 1 In the inventory window, expand the Physical Inventory tree, then right-click the DWDM port.

Step 2 Choose **Commands > IPODWDM > Configure > Loopback** from the popup menu.

The Loopback dialog box is displayed.

Step 3 Enter values for the following parameters.

Input Parameter	Description
Loopback	The loopback type. Values are: • Internal • Line
Option	Specifies whether to set or remove loopback.

Step 4 To see how the command, including variables, looks before it is executed, click **Preview**.

Step 5 To schedule the command, click the Scheduling tab. For more details on scheduling, see Scheduling a Command.

Step 6 To run the command, click **Execute**.

The Result tab displays the actual interaction of the command in the output console.

Step 7 To close the window, click **Close**.

Setting DWDM PM FEC Data

Use the Configure DWDM PM FEC Data command to configure TCA generation and PM counters on the FEC layer.

Step 1 In the inventory window, expand the Physical Inventory tree, then right-click the DWDM port.

Step 2 Choose **Commands > IPODWDM > Configure > PM FEC Data** from the popup menu.

The PM FEC Data dialog box is displayed.

Step 3 Enter values for the following parameters.

Input Parameter	Description
PM Interval	The PM interval type.
FEC Alarm Type	The FEC alarm type. Values are: • Ec-bits—Bit errors corrected (BIEC). Indicates the number of bit errors corrected in the DWDM trunk line during the performance monitoring time interval. • Uc-words—Uncorrectable words. Indicates the number of uncorrectable words detected in the DWDM trunk line during the performance monitoring time interval.
TCA Option	Specifies whether to enable or disable the TCA generation.
Threshold Option	Sets or resets the threshold option. If you select Set, the threshold value that is entered is set on the device; otherwise, the threshold value is reset. If you select blank, the threshold value is not used.
Threshold	The threshold value.

Step 4 To see how the command, including variables, looks before it is executed, click **Preview**.

Step 5 To schedule the command, click the Scheduling tab. For more details on scheduling, see Scheduling a Command.

Step 6 To run the command, click **Execute**.

The Result tab displays the actual interaction of the command in the output console.

Step 7 To close the window, click **Close**.

Setting DWDM PM Optics Data

Use the Configure DWDM PM Optics Data command to configure TCA generation and PM counters on the optical layer.

Step 1 In the inventory window, expand the Physical Inventory tree, then right-click the DWDM port.

Step 2 Choose **Commands > IPODWDM > Configure > PM Optics Data** from the popup menu.

The PM Optics Data dialog box is displayed.

Step 3 Enter values for the following parameters.

Input Parameter	Description
PM Interval	The PM interval type. Values are: • 15-min • 24- hour
Optics Alarm Type	The alarm type. Values are: • lbc—Laser bias current. • opr—Optical power on the unidirectional port. • opt—Transmit optical power in dBm.
Max TCA Option	Specifies whether to enable or disable the maximum threshold option.
Max Threshold Option	Sets or resets the maximum threshold option. If you select Set, the maximum threshold value that is entered is set on the device; otherwise, the threshold value is reset. If you select blank, the maximum threshold value is not used.
Max Threshold	The maximum threshold value.
Min-TCA Option	Specifies whether to disable or enable the minimum threshold option.
Min Threshold Option	Sets or resets the minimum threshold option. If you select Set, the minimum threshold value that is entered is set on the device; otherwise, the threshold value is reset. If you select blank, the minimum threshold value is not used.
Min Threshold	The minimum threshold value.

Step 4 To see how the command, including variables, looks before it is executed, click **Preview**.

Step 5 To schedule the command, click the Scheduling tab. For more details on scheduling, see Scheduling a Command.

Step 6 To run the command, click **Execute**.

The Result tab displays the actual interaction of the command in the output console.

Step 7 To close the window, click **Close**.

Setting DWDM PM OTN Data

Use the Configure DWDM PM OTN Data to configure TCA generation and PM counters on the OTN layer.

Step 1 In the inventory window, expand the Physical Inventory tree, then right-click the DWDM port.

Step 2 Choose **Commands > IPODWDM > Configure > PM OTN Data** from the popup menu.

The PM OTN Data dialog box is displayed.

Step 3 Enter values for the following parameters.

Input Parameter	Descriptions
PM Interval	The interval type. Values are: • 15-min • 24- hour
OTN Alarm Type	The OTN alarm type. Values are: • bbe-pm-fe—Far-end path monitoring background block errors (BBE-PM). • bbe-pm-ne—Near-end BBE-PM. • bbe-sm-fe—Far-end section monitoring background block errors (BBE-SM). • bbe-sm-ne—Near-end BBE-SM. • bber-pm-fe—Far-end path monitoring background block errors ratio (BBER-PM). • bber-pm-ne—Near-end BBER-PM. • bber-sm-fe—Far-end section monitoring background block errors ratio (BBER-SM). • bber-sm-ne—Near-end BBER-SM. • es-pm-fe—Far-end path monitoring errored seconds (ES-PM). • es-pm-ne—Near-end ES-PM. • es-sm-fe—Far-end section monitoring errored seconds (ES-SM). • es-sm-ne—Near-end ES-SM. • esr-pm-fe—Far-end path monitoring errored seconds ratio (ESR-PM). • esr-pm-ne—Near-end ESR-PM.

Input Parameter	Descriptions
OTN Alarm Type (continued)	• esr-sm-fe—Far-end section monitoring errored seconds ratio (ESR-SM). • esr-sm-ne—Near-end ESR-SM. • fc-pm-fe—Far-end path monitoring failure counts (FC-PM). • fc-pm-ne—Near-end FC-PM. • fc-sm-fe—Far-end section monitoring failure counts (FC-SM). • fc-sm-ne—Near-end FC-SM. • ses-pm-fe—Far-end path monitoring severely errored seconds (SES-PM). • ses-pm-ne—Near-end SES-PM. • ses-sm-fe—Far-end section monitoring severely errored seconds (SES-SM). • ses-sm-ne—Near-end SES-SM. • sesr-pm-fe—Far-end path monitoring severely errored seconds ratio (SESR-PM). • sesr-pm-ne—Near-end SESR-PM. • sesr-sm-fe—Far-end section monitoring severely errored seconds ratio (SESR-SM). • sesr-sm-ne—Near-end SESR-SM. • uas-pm-fe—Far-end path monitoring unavailable seconds (UAS-PM). • uas-pm-ne—Near-end UAS-PM. • uas-sm-fe—Far-end section monitoring unavailable seconds (UAS-SM). • uas-sm-ne—Near-end UAS-SM.
TCA Option	Specifies whether to disable or enable.
Threshold Option	Sets or resets the threshold option. If you select Set, the threshold value that is entered is set on the device; otherwise, the threshold value is reset. If you select blank, the threshold value is not used.
Threshold	The threshold value.

Step 4 To see how the command, including variables, looks before it is executed, click **Preview**.

Step 5 To schedule the command, click the Scheduling tab. For more details on scheduling, see Scheduling a Command.

Step 6 To run the command, click **Execute**.

The Result tab displays the actual interaction of the command in the output console.

Step 7 To close the window, click **Close**.

Setting DWDM Transmit Power

Use the Configure DWDM Transmit Power command to configure transponder Tx threshold and reset it to the default.

Step 1 In the inventory window, expand the Physical Inventory tree, then right-click the DWDM port.

Step 2 Choose **Commands > IPODWDM > Configure > Transmit Power** from the popup menu.

The Transmit Power dialog box is displayed.

Step 3 Enter values for the following parameters.

Input Parameter	Description
Transmit Power	The transmit power in dBm.
Option	Specifies whether to set or reset the transponder Tx threshold.

Step 4 To see how the command, including variables, looks before it is executed, click **Preview**.

Step 5 To schedule the command, click the Scheduling tab. For more details on scheduling, see Scheduling a Command.

Step 6 To run the command, click **Execute**.

The Result tab displays the actual interaction of the command in the output console.

Step 7 To close the window, click **Close**.

Setting Rx LOS Threshold

Use the Configure Rx LOS Threshold command to configure transponder Rx threshold and reset it to the default.

Step 1 In the inventory window, expand the Physical Inventory tree, then right-click the DWDM port.

Step 2 Choose **Commands > IPODWDM > Configure > Rx LOS Threshold** from the popup menu.

The Rx LOS Threshold dialog box is displayed.

Step 3 Enter values for the following parameters.

Input Parameter	Description
Rx Los Threshold	The Rx LOS threshold value.
Option	Specifies whether to set or reset the transponder Rx threshold.

Step 4 To see how the command, including variables, looks before it is executed, click **Preview**.

Step 5 To schedule the command, click the Scheduling tab. For more details on scheduling, see Scheduling a Command.

Step 6 To run the command, click **Execute**.

The Result tab displays the actual interaction of the command in the output console.

Step 7 To close the window, click **Close**.

Displaying IM Trace Details

Use the Show DWDM Interface Manager Trace Details command to display Interface Manager trace details for the card.

Step 1 In the inventory window, expand the Physical Inventory tree, then right-click the module.

Step 2 Choose **Commands > IPODWDM > Show > IM Trace Details** from the popup menu.

The IM Trace Details dialog box is displayed.

Step 3 Enter a value for the following parameter.

Input Parameter	Description
Location	The card location; for example, 0/5/CPU0

Step 4 To see how the command, including variables, looks before it is executed, click **Preview**.

Step 5 To schedule the command, click the Scheduling tab. For more details on scheduling, see Scheduling a Command.

Step 6 To run the command, click **Execute**.

The Result tab displays the actual interaction of the command in the output console.

Step 7 To close the window, click **Close**.

Displaying Device Log

Use the Show DWDM Device Log command to display device logs.

Step 1 In the inventory window, right-click the VNE.

Step 2 Choose **Commands > IPODWDM > Show > Device Log**.

The Device Log window is displayed.

Step 3 To see how the command, including variables, looks before it is executed, click **Preview**.

Step 4 To schedule the command, click the Scheduling tab. For more details on scheduling, see Scheduling a Command.

Step 5 To run the command, click **Execute**.

The Result tab displays the actual interaction of the command in the output console.

Step 6 To close the window, click **Close**.



CHAPTER 28

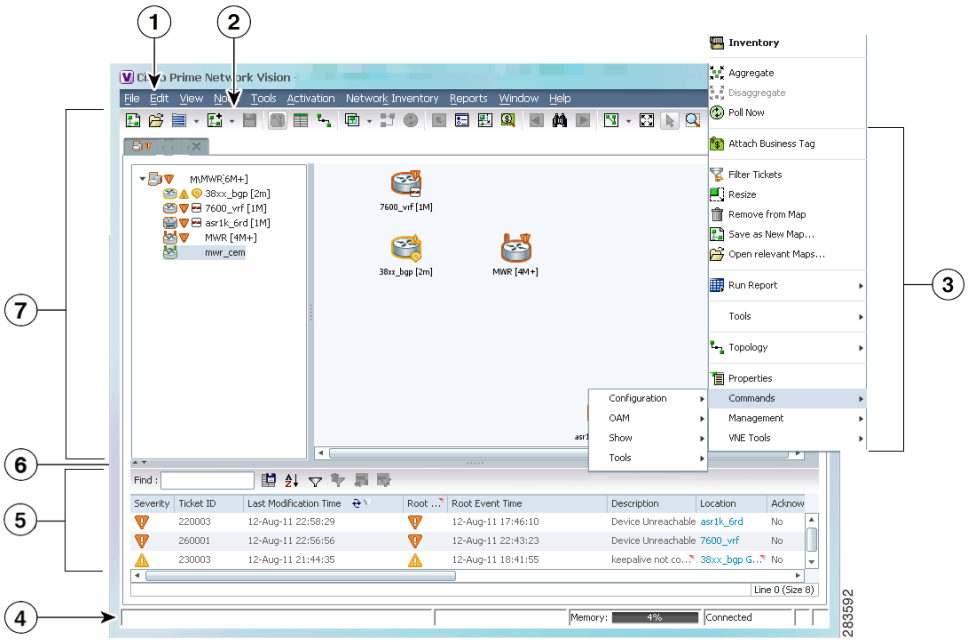
Using the Prime Network Basic Operation Commands

Prime Network allows you to perform basic operations on a selected network element. To perform the basic operation commands, you can launch it in a network element from the Prime Network Vision List or Map View. Figure 28-1 shows what happens when you right-click a network element. From here, you can choose **Commands**.

Note To view the basic operation commands in the Cisco Carrier Packet Transport (CPT) System, you must right-click the Cisco Carrier Packet Transport (CPT) System in the Prime Network Vision List or Map View and click **Logical Inventory > CPT Context Container**.

Note The basic operation commands in this chapter can be executed by all network elements that run on Cisco IOS software, Cisco IOS XR software, and Cisco NX OS software. You will not be able to execute these commands on network elements that have Cisco Catalyst OS software.

Figure 28-1 Basic Operation Commands



1	Menu Bar	**5**	Ticket Pane
2	Tool bar	**6**	Hide/display Ticket Pane
3	Device Right-click Menu	**7**	Navigation Pane
4	Status Bar		

The basic operation commands that you can perform include:

- Configuration Commands, page 28-2
- Show Commands, page 28-24
- Tools Commands, page 28-27
- OAM Commands, page 28-30

Configuration Commands

The configuration commands allow you to configure the selected network element. The commands include:

- Add Interface Configuration, page 28-3
- Remove Interface Configuration, page 28-4
- Update Interface Configuration, page 28-4
- Add Loopback Interface, page 28-5
- Add Port Description, page 28-6
- Remove Port Description, page 28-6

- Update Port Description, page 28-7
- Change Port Status, page 28-8
- Enable traps, page 28-8
- Remove Access List, page 28-9
- Remove Access List Entry, page 28-9
- Remove Rate Limit, page 28-10
- Write Memory, page 28-10
- Disable Interface, page 28-11
- Enable Interface, page 28-11
- Assign Port To Vlan, page 28-11
- DeAssign Port To Vlan, page 28-12
- Add Host Name, page 28-12
- Remove Host Name, page 28-13
- Add DNS Server, page 28-13
- Remove DNS Server, page 28-14
- Add NTP Server, page 28-15
- Remove NTP Server, page 28-15
- Syslog Host Logging, page 28-16
- Add Traps, page 28-16
- Remove Traps, page 28-17
- Add Radius Server, page 28-18
- Remove Radius Server, page 28-18
- Add Tacacs Server, page 28-19
- Remove Tacacs Server, page 28-20
- Add Tacacs+ Server, page 28-20
- Remove Tacacs+ Server, page 28-21
- Add SNMP Configuration, page 28-21
- Remove SNMP Configuration, page 28-22
- Update SNMP Configuration, page 28-23

Add Interface Configuration

Use the **Add Interface Configuration** command to add an interface configuration to the selected network element.

Step 1 In the Network Vision List or Map View, right-click the network element.

Step 2 Choose **Physical Inventory**.

Step 3 Choose the corresponding interface and right-click, choose **Commands > Configuration > Add Interface Configuration**.

Step 4 Enter the value for the following parameters.

Input Parameter	Description
IP Address Type	The IP address family- can be IPv4 or IPv6
IP Address	The IP address - can be IPv4 or IPv6
Mask	The subnet mask IP address.
Description	The description of the interface.

Step 5 To see the commands that will be applied on the device, click **Preview**.

Step 6 You can view the commands in the Result tab. You can go back and make any required changes to the input parameters.

Step 7 To schedule the command, click the Scheduling tab. For more details on scheduling, see Scheduling a Command.

Step 8 To run the commands, click **Execute Now**.

You can view errors in the Result tab, if there are any.

Step 9 To close the dialog box, click **Close**.

Remove Interface Configuration

Use the **Remove Interface Configuration** command to remove an interface configuration from the selected network element.

Step 1 In the Network Vision List or Map View, right-click the network element.

Step 2 Choose **Logical Inventory > Routing Entities.** Choose the corresponding interface and right-click.

Step 3 Choose **Commands > Configuration > Remove Interface Configuration.**

Step 4 To see the commands that will be applied on the device, click **Preview**.

Step 5 You can view the commands in the Result tab. You can go back and make any required changes to the input parameters.

Step 6 To schedule the command, click the Scheduling tab. For more details on scheduling, see Scheduling a Command.

Step 7 To run the commands, click **Execute Now**.

You can view errors in the Result tab, if there are any.

Step 8 To close the dialog box, click **Close**.

Update Interface Configuration

Use the **Update Interface Configuration** command to update an interface configuration on the selected network element.

Step 1 In the Network Vision List or Map View, right-click the network element.

Step 2 Choose **Logical Inventory > Routing Entities.** Choose the corresponding interface and right-click.

Step 3 Choose **Commands > Configuration > Update Interface Configuration**.

Step 4 Enter the value for the following parameter.

Input Parameter	Description
Description	The description of the interface.

Step 5 To see the commands that will be applied on the device, click **Preview**.

Step 6 You can view the commands in the Result tab. You can go back and make any required changes to the input parameters.

Step 7 To schedule the command, click the Scheduling tab. For more details on scheduling, see Scheduling a Command.

Step 8 To run the commands, click **Execute Now**.

You can view errors in the Result tab, if there are any.

Step 9 To close the dialog box, click **Close**.

Add Loopback Interface

Use the **Add Loopback Interface** command to add a loop back interface on the selected network element.

Step 1 In the Network Vision List or Map View, right-click the network element.

Step 2 Choose **Commands > Configuration > Add Loopback Interface**.

Step 3 Enter the value for the following parameter

Input Parameter	Description
IPAddress Type	The IP address family- can be IPv4 or IPv6
Address	The IP address - can be IPv4 or IPv6
Loopback ID	The loopback identifier of the IP address.
Mask	The subnet mask IP address - can be IPv4 or IPv6

Step 4 To see the commands that will be applied on the device, click **Preview**.

Step 5 You can view the commands in the Result tab. You can go back and make any required changes to the input parameters.

Step 6 To schedule the command, click the Scheduling tab. For more details on scheduling, see Scheduling a Command.

Step 7 To run the commands, click **Execute Now**.

You can view errors in the Result tab, if there are any.

Step 8 To close the dialog box, click **Close**.

Add Port Description

Use the **Add port description** command to add a port description on the selected network element.

Note This command is unavailable on the Cisco Carrier Packet Transport (CPT) System.

Step 1 In the Network Vision List or Map View, right-click the network element.

Step 2 Choose Physical Inventory.

Step 3 Choose the corresponding interface and right-click, choose **Commands > Configuration > Add port description**.

Step 4 Enter the value for the following parameter.

Input Parameter	Description
Description	The description of the port.

Step 5 To see the commands that will be applied on the device, click **Preview**.

Step 6 You can view the commands in the Result tab. You can go back and make any required changes to the input parameters.

Step 7 To schedule the command, click the Scheduling tab. For more details on scheduling, see Scheduling a Command.

Step 8 To run the commands, click **Execute Now**.

You can view errors in the Result tab, if there are any.

Step 9 To close the dialog box, click **Close**.

Remove Port Description

Use the **Remove port description** command to remove a port description on the selected network element.

Note This command is unavailable on the Cisco Carrier Packet Transport (CPT) System.

Step 1 In the Network Vision List or Map View, right-click the network element.

Step 2 Choose Physical Inventory.

Step 3 Choose the corresponding interface and right-click, choose **Commands > Configuration > Remove port description.**

Step 4 To see the commands that will be applied on the device, click **Preview**.

Step 5 You can view the commands in the Result tab. You can go back and make any required changes to the input parameters.

Step 6 To schedule the command, click the Scheduling tab. For more details on scheduling, see Scheduling a Command.

Step 7 To run the commands, click **Execute Now**.

You can view errors in the Result tab, if there are any.

Step 8 To close the dialog box, click **Close**.

Update Port Description

Use the **Update port description** command to update the port description on the selected network element.

Note This command is unavailable on the Cisco Carrier Packet Transport (CPT) System.

Step 1 In the Network Vision List or Map View, right-click the network element.

Step 2 Choose Physical Inventory.

Step 3 Choose the corresponding interface and right-click, choose **Commands > Configuration > Update port description**.

Step 4 Enter the value for the following parameter.

Input Parameter	Description
Description	The description of the port.

Step 5 To see the commands that will be applied on the device, click **Preview**.

Step 6 You can view the commands in the Result tab. You can go back and make any required changes to the input parameters.

Step 7 To schedule the command, click the Scheduling tab. For more details on scheduling, see Scheduling a Command.

Step 8 To run the commands, click **Execute Now**.

You can view errors in the Result tab, if there are any.

Step 9 To close the dialog box, click **Close**.

Change Port Status

Use the **Change port status** command to add a loop back interface on the selected network element.

Note This command is unavailable on the Cisco Carrier Packet Transport (CPT) System.

Step 1 In the Network Vision List or Map View, right-click the network element.

Step 2 Choose Physical Inventory.

Step 3 Choose the corresponding interface and right-click, choose **Commands > Configuration > Change Port Status**.

Step 4 Enter the value for the following parameter.

Input Parameter	Description
Status	The status of the port.

Step 5 To see the commands that will be applied on the device, click **Preview**.

Step 6 You can view the commands in the Result tab. You can go back and make any required changes to the input parameters.

Step 7 To schedule the command, click the Scheduling tab. For more details on scheduling, see Scheduling a Command.

Step 8 To run the commands, click **Execute Now**.

You can view errors in the Result tab, if there are any.

Step 9 To close the dialog box, click **Close**.

Enable traps

Use the **Enable traps** command to enable traps on the selected network element.

Step 1 In the Network Vision List or Map View, right-click the network element.

Step 2 Choose **Commands > Configuration > System > SNMP > Enable traps**.

Step 3 Enter the value for the following parameter

Input Parameter	Description
Community	The community name.
Host address	The host address.

Step 4 To see the commands that will be applied on the device, click **Preview**.

Step 5 You can view the commands in the Result tab. You can go back and make any required changes to the input parameters.

Step 6 To schedule the command, click the Scheduling tab. For more details on scheduling, see Scheduling a Command.

Step 7 To run the commands, click **Execute Now**.

You can view errors in the Result tab, if there are any.

Step 8 To close the dialog box, click **Close**.

Remove Access List

Use the **Remove access list** command to remove the access list on the selected network element.

Note You can not execute this command on network elements that run on Cisco IOS XR software.

Step 1 In the Network Vision List or Map View, right-click the network element.

Step 2 Choose **Commands > Configuration > System > Remove access list**.

Step 3 To see the commands that will be applied on the device, click **Preview**.

Step 4 You can view the commands in the Result tab. You can go back and make any required changes to the input parameters.

Step 5 To schedule the command, click the Scheduling tab. For more details on scheduling, see Scheduling a Command.

Step 6 To run the commands, click **Execute Now**.

You can view errors in the Result tab, if there are any.

Step 7 To close the dialog box, click **Close**.

Remove Access List Entry

Use the **Remove access list entry** command to remve access list entry on the selected network element.

Note You can not execute this command on network elements that run on Cisco IOS XR software.

Step 1 In the Network Vision List or Map View, right-click the network element.

Step 2 Choose **Commands > Configuration > System > Remove access list entry**.

Step 3 To see the commands that will be applied on the device, click **Preview**.

Step 4 You can view the commands in the Result tab. You can go back and make any required changes to the input parameters.

Step 5 To schedule the command, click the Scheduling tab. For more details on scheduling, see Scheduling a Command.

Step 6 To run the commands, click **Execute Now**.

You can view errors in the Result tab, if there are any.

Step 7 To close the dialog box, click **Close**.

Remove Rate Limit

Use the **Remove rate limit** command to remove the rate limit on the selected network element.

Note You can not execute this command on network elements that run on Cisco IOS XR software.

Step 1 In the Network Vision List or Map View, right-click the network element.

Step 2 Choose **Commands > Configuration > System > Remove rate limit**.

Step 3 To see the commands that will be applied on the device, click **Preview**.

Step 4 You can view the commands in the Result tab. You can go back and make any required changes to the input parameters.

Step 5 To schedule the command, click the Scheduling tab. For more details on scheduling, see Scheduling a Command.

Step 6 To run the commands, click **Execute Now**.

You can view errors in the Result tab, if there are any.

Step 7 To close the dialog box, click **Close**.

Write Memory

Use the **Write memory** command to write memory on the selected network element.

Note You can not execute this command on network elements that run on Cisco IOS XR software.

Step 1 In the Network Vision List or Map View, right-click the network element.

Step 2 Choose **Commands > Configuration > Write memory.**

Step 3 To see the commands that will be applied on the device, click **Preview**.

Step 4 You can view the commands in the Result tab. You can go back and make any required changes to the input parameters.

Step 5 To schedule the command, click the Scheduling tab. For more details on scheduling, see Scheduling a Command.

Step 6 To run the commands, click **Execute Now**.

You can view errors in the Result tab, if there are any.

Step 7 To close the dialog box, click **Close**.

Disable Interface

Use the **Disable Interface** command to disable the interface on the selected network element.

Step 1 In the Network Vision List or Map View, right-click the network element.

Step 2 Choose Logical Inventory > Routing Entities. Choose the corresponding interface and right-click.

Step 3 Choose **Commands > Configuration > Disable Interface.**

Step 4 To see the commands that will be applied on the device, click **Preview**.

Step 5 You can view the commands in the Result tab. You can go back and make any required changes to the input parameters.

Step 6 To schedule the command, click the Scheduling tab. For more details on scheduling, see Scheduling a Command.

Step 7 To run the commands, click **Execute Now**.

You can view errors in the Result tab, if there are any.

Step 8 To close the dialog box, click **Close**.

Enable Interface

Use the **Enable Interface** command to enable the interface on the selected network element.

Step 1 In the Network Vision List or Map View, right-click the network element.

Step 2 Choose Logical Inventory > Routing Entities. Choose the corresponding interface and right-click.

Step 3 Choose **Commands > Configuration > Enable Interface.**

Step 4 To see the commands that will be applied on the device, click **Preview**.

Step 5 You can view the commands in the Result tab. You can go back and make any required changes to the input parameters.

Step 6 To schedule the command, click the Scheduling tab. For more details on scheduling, see Scheduling a Command.

Step 7 To run the commands, click **Execute Now**.

You can view errors in the Result tab, if there are any.

Step 8 To close the dialog box, click **Close**.

Assign Port To Vlan

Use the **Assign Port To Vlan** command to assign a port to VLAN on the selected network element.

Step 1 In the Network Vision List or Map View, right-click the network element.

Step 2 Choose Logical Inventory > Routing Entities. Choose the corresponding interface and right-click.

Step 3 Choose **Commands > Configuration > Assign Port To Vlan.**

Step 4 Enter the folowing parameter.

\

Input Parameter	Description
VLAN ID	The VLAN identifier. Value should be with in the range 1 to 4094.

Step 5 To see the commands that will be applied on the device, click **Preview**.

Step 6 You can view the commands in the Result tab. You can go back and make any required changes to the input parameters.

Step 7 To schedule the command, click the Scheduling tab. For more details on scheduling, see Scheduling a Command.

Step 8 To run the commands, click **Execute Now**.

You can view errors in the Result tab, if there are any.

Step 9 To close the dialog box, click **Close**.

DeAssign Port To Vlan

Use the **DeAssign Port To Vlan** command to de-assign a port to VLAN on the selected network element.

Step 1 In the Network Vision List or Map View, right-click the network element.

Step 2 Choose Logical Inventory > Routing Entities. Choose the corresponding interface and right-click.

Step 3 Choose **Commands > Configuration > DeAssign Port To Vlan.**

Step 4 To see the commands that will be applied on the device, click **Preview**.

Step 5 You can view the commands in the Result tab. You can go back and make any required changes to the input parameters.

Step 6 To schedule the command, click the Scheduling tab. For more details on scheduling, see Scheduling a Command.

Step 7 To run the commands, click **Execute Now**.

You can view errors in the Result tab, if there are any.

Step 8 To close the dialog box, click **Close**.

Add Host Name

Use the **Add Host Name** command to add a host name on the selected network element.

Step 1 In the Network Vision List or Map View, right-click the network element.

Step 2 Choose **Commands > Configuration > System > Add Host Name.**

Step 3 Enter the value for the following parameter.

Input Parameter	Description
Host name	The name of the host.

Step 4 To see the commands that will be applied on the device, click **Preview**.

Step 5 You can view the commands in the Result tab. You can go back and make any required changes to the input parameters.

Step 6 To schedule the command, click the Scheduling tab. For more details on scheduling, see Scheduling a Command.

Step 7 To run the commands, click **Execute Now**.

You can view errors in the Result tab, if there are any.

Step 8 To close the dialog box, click **Close**.

Remove Host Name

Use the **Remove Host Name** command to remove a host name on the selected network element.

Step 1 In the Network Vision List or Map View, right-click the network element.

Step 2 Choose **Commands > Configuration > System > Remove Host Name.**

Step 3 To see the commands that will be applied on the device, click **Preview**.

Step 4 You can view the commands in the Result tab. You can go back and make any required changes to the input parameters.

Step 5 To schedule the command, click the Scheduling tab. For more details on scheduling, see Scheduling a Command.

Step 6 To run the commands, click **Execute Now**.

You can view errors in the Result tab, if there are any.

Step 7 To close the dialog box, click **Close**.

Add DNS Server

Use the **Add DNS Server** command to add a DNS server to the selected network element.

Step 1 In the Network Vision List or Map View, right-click the network element.

Step 2 Choose **Commands > Configuration > System > DNS > Add DNS Server.**

Step 3 Enter the values for the following parameters

Input Parameter	Description
Domain Name	The name of the domain.
Domain List	The name of the domain list.
Domain Name Server Address 1 ([A.B.C.D])	The domain name server address 1.

Step 4 To see the commands that will be applied on the device, click **Preview**.

Step 5 You can view the commands in the Result tab. You can go back and make any required changes to the input parameters.

Step 6 To schedule the command, click the Scheduling tab. For more details on scheduling, see Scheduling a Command.

Step 7 To run the commands, click **Execute Now**.

You can view errors in the Result tab, if there are any.

Step 8 To close the dialog box, click **Close**.

Remove DNS Server

Use the **Remove DNS Server** command to add a DNS server from the selected network element.

Step 1 In the Network Vision List or Map View, right-click the network element.

Step 2 Choose **Commands > Configuration > System > DNS > Remove DNS Server.**

Step 3 Enter the values for the following parameters

Input Parameter	Description
Domain Name	The name of the domain
Domain List	The name of the domain list
Domain Name Server Address 1 ([A.B.C.D])	The domain name server address 1.

Step 4 To see the commands that will be applied on the device, click **Preview**.

Step 5 You can view the commands in the Result tab. You can go back and make any required changes to the input parameters.

Step 6 To schedule the command, click the Scheduling tab. For more details on scheduling, see Scheduling a Command.

Step 7 To run the commands, click **Execute Now**.

You can view errors in the Result tab, if there are any.

Step 8 To close the dialog box, click **Close**.

Add NTP Server

Use the **Add NTP Server** command to add a NTP server from the selected network element.

Step 1 In the Network Vision List or Map View, right-click the network element.

Step 2 Choose **Commands > Configuration > System > NTP > Add NTP Server.**

Step 3 Enter the values for the following parameters

Input Parameter	Description
IPAddress Type	The address family- IPV4 or IPV6 values.
NTP Server Address	The NTP server IP address.
Version Number	The version number.
Key Id	The key identifier. The range should be from 0 to 4294967295.
Interface Name	The name of the interface.

Step 4 To see the commands that will be applied on the device, click **Preview**.

Step 5 You can view the commands in the Result tab. You can go back and make any required changes to the input parameters.

Step 6 To schedule the command, click the Scheduling tab. For more details on scheduling, see Scheduling a Command.

Step 7 To run the commands, click **Execute Now**.

You can view errors in the Result tab, if there are any.

Step 8 To close the dialog box, click **Close**.

Remove NTP Server

Use the **Remove NTP Server** command to remove a NTP server from the selected network element.

Step 1 In the Network Vision List or Map View, right-click the network element.

Step 2 Choose **Commands > Configuration > System > NTP > Remove NTP Server.**

Step 3 Enter the values for the following parameter.

NTP Server Address, The NTP server IP address.

Step 4 To see the commands that will be applied on the device, click **Preview**.

Step 5 You can view the commands in the Result tab. You can go back and make any required changes to the input parameters.

Step 6 To schedule the command, click the Scheduling tab. For more details on scheduling, see Scheduling a Command.

Step 7 To run the commands, click **Execute Now**.

You can view errors in the Result tab, if there are any.

Step 8 To close the dialog box, click **Close**.

Syslog Host Logging

Use the **Syslog Host Logging** command to view the syslogs of host logging on the selected network element.

Step 1 In the Network Vision List or Map View, right-click the network element.

Step 2 Choose **Commands > Configuration > System > Syslog Host Logging**.

Step 3 Enter the values for the following parameters

Input Parameter	Description
Host Type	The host type- IPV4 or IPV6 host.
Logging Host	The IP address of the logging host.
Logging Buffer Size	Logging buffer size. Value should be in the range from 4096 to 2147483647.
Logging Buffered	Logging Buffered
Logging Facility	Logging Facility
Logging Severity Level	Logging Severity Level
Logging History	Logging History

Step 4 To see the commands that will be applied on the device, click **Preview**.

Step 5 You can view the commands in the Result tab. You can go back and make any required changes to the input parameters.

Step 6 To schedule the command, click the Scheduling tab. For more details on scheduling, see Scheduling a Command.

Step 7 To run the commands, click **Execute Now**.

You can view errors in the Result tab, if there are any.

Step 8 To close the dialog box, click **Close**.

Add Traps

Use the **Add Traps** command to add traps on the selected network element.

Step 1 In the Network Vision List or Map View, right-click the network element.

Step 2 Choose **Commands > Configuration > System > Snmp > Add Traps**.

Step 3 Enter the values for the following parameters

Input Parameter	Description
Trap 1	Trap list 1
Trap 2	Trap list 2
Trap 3	Trap list 3
Trap 4	Trap list 4
Trap 5	Trap list 5
Trap 6	Trap list 6
Trap 7	Trap list 7

Step 4 To see the commands that will be applied on the device, click **Preview**.

Step 5 You can view the commands in the Result tab. You can go back and make any required changes to the input parameters.

Step 6 To schedule the command, click the Scheduling tab. For more details on scheduling, see Scheduling a Command.

Step 7 To run the commands, click **Execute Now**.

You can view errors in the Result tab, if there are any.

Step 8 To close the dialog box, click **Close**.

Remove Traps

Use the **Remove Traps** command to remove traps on the selected network element.

Step 1 In the Network Vision List or Map View, right-click the network element.

Step 2 Choose **Commands > Configuration > System > Snmp > Remove Traps**.

Step 3 Enter the values for the following parameters.

Input Parameter	Description
Trap 1	Trap list 1
Trap 2	Trap list 2
Trap 3	Trap list 3
Trap 4	Trap list 4
Trap 5	Trap list 5
Trap 6	Trap list 6
Trap 7	Trap list 7

Step 4 To see the commands that will be applied on the device, click **Preview**.

Step 5 You can view the commands in the Result tab. You can go back and make any required changes to the input parameters.

Step 6 To schedule the command, click the Scheduling tab. For more details on scheduling, see Scheduling a Command.

Step 7 To run the commands, click **Execute Now**.

You can view errors in the Result tab, if there are any.

Step 8 To close the dialog box, click **Close**.

Add Radius Server

Use the **Add Radius Server** command to add a radius server on the selected network element.

Step 1 In the Network Vision List or Map View, right-click the network element.

Step 2 Choose **Commands > Configuration > System > RADIUS > Add Radius Server**.

Step 3 Enter the values for the following parameters

Input Parameter	Description
Radius Server Host Address	The radius server host IP address
Authentication port value	The authentication port. Value should be in the range 0 to 65535.
key-value	The key-value of th radius server??
Authentication List Name	The authentication list name.
Group Name	The name of the group.

Step 4 To see the commands that will be applied on the device, click **Preview**.

Step 5 You can view the commands in the Result tab. You can go back and make any required changes to the input parameters.

Step 6 To schedule the command, click the Scheduling tab. For more details on scheduling, see Scheduling a Command.

Step 7 To run the commands, click **Execute Now**.

You can view errors in the Result tab, if there are any.

Step 8 To close the dialog box, click **Close**.

Remove Radius Server

Use the **Remove Radius Server** command to remove a radius server on the selected network element.

Step 1 In the Network Vision List or Map View, right-click the network element.

Step 2 Choose **Commands > Configuration > System > RADIUS > Remove Radius Server**.

Step 3 Enter the values for the following parameters

Input Parameter	Description
Radius Server Host Address	The radius server host IP address
Authentication List Name	The authentication list name.

Step 4 To see the commands that will be applied on the device, click **Preview**.

Step 5 You can view the commands in the Result tab. You can go back and make any required changes to the input parameters.

Step 6 To schedule the command, click the Scheduling tab. For more details on scheduling, see Scheduling a Command.

Step 7 To run the commands, click **Execute Now**.

You can view errors in the Result tab, if there are any.

Step 8 To close the dialog box, click **Close**.

Add Tacacs Server

Use the **Add Tacacs Server** command to add a TACAS server on the selected network element.

Step 1 In the Network Vision List or Map View, right-click the network element.

Step 2 Choose **Commands > Configuration > System > TACACS > Add Tacacs Server**.

Step 3 Enter the values for the following parameters

Input Parameter	Description
Tacacs Server Host Address	The TACAS Server Host IP Address.
Retransmit Value	The retransmit value. Values should be in the range 0 to 100.
Timeout Value	The timeout value. Value should be in the range 1 to 1000.

Step 4 To see the commands that will be applied on the device, click **Preview**.

Step 5 You can view the commands in the Result tab. You can go back and make any required changes to the input parameters.

Step 6 To schedule the command, click the Scheduling tab. For more details on scheduling, see Scheduling a Command.

Step 7 To run the commands, click **Execute Now**.

You can view errors in the Result tab, if there are any.

Step 8 To close the dialog box, click **Close**.

Remove Tacacs Server

Use the **Remove Tacacs Server** command to remove a TACAS server on the selected network element.

Step 1 In the Network Vision List or Map View, right-click the network element.

Step 2 Choose **Commands > Configuration > System > TACACS > Remove Tacacs Server**.

Step 3 Enter the values for the following parameters

Input Parameter	Description
Tacacs Server Host Address	The TACAS Server Host IP Address.

Step 4 To see the commands that will be applied on the device, click **Preview**.

Step 5 You can view the commands in the Result tab. You can go back and make any required changes to the input parameters.

Step 6 To schedule the command, click the Scheduling tab. For more details on scheduling, see Scheduling a Command.

Step 7 To run the commands, click **Execute Now**.

You can view errors in the Result tab, if there are any.

Step 8 To close the dialog box, click **Close**.

Add Tacacs+ Server

Use the **Add Tacacs Server** command to add a TACAS+ server on the selected network element.

Step 1 In the Network Vision List or Map View, right-click the network element.

Step 2 Choose **Commands > Configuration > System > TACACS+ > Add Tacacs+ Server**.

Step 3 Enter the values for the following parameters

Input Parameter	Description
Tacacs+ Server Host Address	The TACACS+ server host IP address.
key-value	The key-value.
Authentication List Name	The authentication list name.
Group Name	The name of the group.

Step 4 To see the commands that will be applied on the device, click **Preview**.

Step 5 You can view the commands in the Result tab. You can go back and make any required changes to the input parameters.

Step 6 To schedule the command, click the Scheduling tab. For more details on scheduling, see Scheduling a Command.

Step 7 To run the commands, click **Execute Now**.

You can view errors in the Result tab, if there are any.

Step 8 To close the dialog box, click **Close**.

Remove Tacacs+ Server

Use the **Add Tacacs Server** command to remove a TACAS+ server on the selected network element.

Step 1 In the Network Vision List or Map View, right-click the network element.

Step 2 Choose **Commands > Configuration > System > TACACS+ > Remove Tacacs+ Server**.

Step 3 Enter the values for the following parameters.

Input Parameter	Description
Tacacs+ Server Host Address	The TACACS+ server host IP address.
Authentication List Name	The authentication list name.

Step 4 To see the commands that will be applied on the device, click **Preview**.

Step 5 You can view the commands in the Result tab. You can go back and make any required changes to the input parameters.

Step 6 To schedule the command, click the Scheduling tab. For more details on scheduling, see Scheduling a Command.

Step 7 To run the commands, click **Execute Now**.

You can view errors in the Result tab, if there are any.

Step 8 To close the dialog box, click **Close**.

Add SNMP Configuration

Use the **Add Snmp Configuration** command to add an SNMP configuration on the selected network element.

Step 1 In the Network Vision List or Map View, right-click the network element.

Step 2 Choose **Commands > Configuration > System > Snmp > Add Snmp Configuration.**

Step 3 Enter the values for the following parameters.

Input Parameter	Description
Host address	The host address.
Community String	The community string.

Input Parameter	Description
Community Access Type	Community Access Type
Trap community Type	The trap community type.
Snmp Engine ID	The SNMP engine identifier.
Snmp Server View Name	The SNMP server view name.
MIB View Family Name	The MIB view family name.
MIB family Included/Excluded from the view	The MIB family Included/Excluded from the view.
Snmp Server Group Name	The SNMP server group name.
SNMPv3 Group Security Model	The SNMPv3 group security model.
Group Read View Name	The group read view name.
Group Write View Name	The group write view nam.e
Group Notify View Name	The group notify view name.
Snmp Server User Name	The SNMP server user name.
SNMPv3 User Security Model	The SNMPv3 user security model.
Authentication Password	The authentication password.

Step 4 To see the commands that will be applied on the device, click **Preview**.

Step 5 You can view the commands in the Result tab. You can go back and make any required changes to the input parameters.

Step 6 To schedule the command, click the Scheduling tab. For more details on scheduling, see Scheduling a Command.

Step 7 To run the commands, click **Execute Now**.

You can view errors in the Result tab, if there are any.

Step 8 To close the dialog box, click **Close**.

Remove SNMP Configuration

Use the **Remove Snmp Configuration** command to remove an SNMP configuration on the selected network element.

Step 1 In the Network Vision List or Map View, right-click the network element.

Step 2 Choose **Commands > Configuration > System > Snmp > Remove Snmp Configuration.**

Step 3 Enter the values for the following parameters

Input Parameter	Description
Host address	The host address.
Community String	The community string.

Input Parameter	Description
Trap community Type	The trap community type.
Snmp Server View Name	The SNMP server view name.
Snmp Server Group Name	The SNMP server group name.
SNMPv3 Group Security Model	The SNMPv3 group security model.
Snmp Server User Name	The SNMP server user name.

Step 4 To see the commands that will be applied on the device, click **Preview**.

Step 5 You can view the commands in the Result tab. You can go back and make any required changes to the input parameters.

Step 6 To schedule the command, click the Scheduling tab. For more details on scheduling, see Scheduling a Command.

Step 7 To run the commands, click **Execute Now**.

You can view errors in the Result tab, if there are any.

Step 8 To close the dialog box, click **Close**.

Update SNMP Configuration

Use the **Update Snmp Configuration** command to add an SNMP configuration on the selected network element.

Step 1 In the Network Vision List or Map View, right-click the network element.

Step 2 Choose **Commands > Configuration > System > Snmp > Update Snmp Configuration.**

Step 3 Enter the values for the following parameters.

Input Parameter	Description
Host address	The host address.
Community String	The community string.
Community Access Type	Community Access Type
Trap community Type	The trap community type.
Snmp Server View Name	The SNMP server view name.
MIB View Family Name	The MIB view family name.
MIB family Included/Excluded from the view	The MIB family Included/Excluded from the view.
Snmp Server Group Name	The SNMP server group name.
SNMPv3 Group Security Model	The SNMPv3 group security model.
Group Read View Name	The group read view name.
Group Write View Name	The group write view name.

Input Parameter	Description
Group Notify View Name	The group notify view name.
Snmp Server User Name	The SNMP server user name.
SNMPv3 User Security Model	The SNMPv3 user security model.
Authentication Password	The authentication password.

Step 4 To see the commands that will be applied on the device, click **Preview**.

Step 5 You can view the commands in the Result tab. You can go back and make any required changes to the input parameters.

Step 6 To schedule the command, click the Scheduling tab. For more details on scheduling, see Scheduling a Command.

Step 7 To run the commands, click **Execute Now**.

You can view errors in the Result tab, if there are any.

Step 8 To close the dialog box, click **Close**.

Show Commands

The show commands allow you to show the details of the selected network element. The commands include:

- Interface Brief, page 28-24
- IP Route, page 28-25
- VRF IP Route, page 28-25
- Running Config, page 28-26
- Running Config from File, page 28-26
- Startup Config, page 28-26
- Users (Telnet Sessions), page 28-27

Interface Brief

Use the **Interface Brief** command to provide more brief information on the selected network element.

Step 1 In the Network Vision List or Map View, right-click the network element.

Step 2 Choose **Commands > Show > IP > Interface Brief.**

Step 3 To see the commands that will be applied on the device, click **Preview**.

Step 4 You can view the commands in the Result tab. You can go back and make any required changes to the input parameters.

Step 5 To schedule the command, click the Scheduling tab. For more details on scheduling, see Scheduling a Command.

Step 6 To run the commands, click **Execute Now**.

You can view errors in the Result tab, if there are any.

Step 7 To close the dialog box, click **Close**.

IP Route

Use the **IP route** command to provide more brief information of the IP route of the selected network element.

Step 1 In the Network Vision List or Map View, right-click the network element.

Step 2 Choose **Commands > Show > IP route.**

Step 3 To see the commands that will be applied on the device, click **Preview**.

Step 4 You can view the commands in the Result tab. You can go back and make any required changes to the input parameters.

Step 5 To schedule the command, click the Scheduling tab. For more details on scheduling, see Scheduling a Command.

Step 6 To run the commands, click **Execute Now**.

You can view errors in the Result tab, if there are any.

Step 7 To close the dialog box, click **Close**.

VRF IP Route

Use the **VRF IP route** command to provide information on the VRF IP route of the selected network element.

Step 1 In the Network Vision List or Map View, right-click the network element.

Step 2 Choose **Commands > Show > VRF IP route.**

Step 3 To see the commands that will be applied on the device, click **Preview**.

Step 4 You can view the commands in the Result tab. You can go back and make any required changes to the input parameters.

Step 5 To schedule the command, click the Scheduling tab. For more details on scheduling, see Scheduling a Command.

Step 6 To run the commands, click **Execute Now**.

You can view errors in the Result tab, if there are any.

Step 7 To close the dialog box, click **Close**.

Running Config

Use the **Running Config** command to view the running configuration of the selected network element.

Step 1 In the Network Vision List or Map View, right-click the network element.

Step 2 Choose **Commands > Show > Running Config.**

Step 3 To see the commands that will be applied on the device, click **Preview**.

Step 4 You can view the commands in the Result tab. You can go back and make any required changes to the input parameters.

Step 5 To schedule the command, click the Scheduling tab. For more details on scheduling, see Scheduling a Command.

Step 6 To run the commands, click **Execute Now**.

You can view errors in the Result tab, if there are any.

Step 7 To close the dialog box, click **Close**.

Running Config from File

Use the **Running Config from file** command to view the running configuration of the selected network element from the file.

Step 1 In the Network Vision List or Map View, right-click the network element.

Step 2 Choose **Commands > Show > Running Config from file.**

Step 3 To see the commands that will be applied on the device, click **Preview**.

Step 4 You can view the commands in the Result tab. You can go back and make any required changes to the input parameters.

Step 5 To schedule the command, click the Scheduling tab. For more details on scheduling, see Scheduling a Command.

Step 6 To run the commands, click **Execute Now**.

You can view errors in the Result tab, if there are any.

Step 7 To close the dialog box, click **Close**.

Startup Config

Use the **Startup Config** command to view the start-up configuration of the selected network element.

Step 1 In the Network Vision List or Map View, right-click the network element.

Step 2 Choose **Commands > Show > Startup Config.**

Step 3 To see the commands that will be applied on the device, click **Preview**.

Step 4 You can view the commands in the Result tab. You can go back and make any required changes to the input parameters.

Step 5 To schedule the command, click the Scheduling tab. For more details on scheduling, see Scheduling a Command.

Step 6 To run the commands, click **Execute Now**.

You can view errors in the Result tab, if there are any.

Step 7 To close the dialog box, click **Close**.

Users (Telnet Sessions)

Use the **Users (Telnet Sessions)** command to view the details of the telnet sessions of the selected network element.

Step 1 In the Network Vision List or Map View, right-click the network element.

Step 2 Choose **Commands > Show > Users (Telnet Sessions).**

Step 3 To see the commands that will be applied on the device, click **Preview**.

Step 4 You can view the commands in the Result tab. You can go back and make any required changes to the input parameters.

Step 5 To schedule the command, click the Scheduling tab. For more details on scheduling, see Scheduling a Command.

Step 6 To run the commands, click **Execute Now**.

You can view errors in the Result tab, if there are any.

Step 7 To close the dialog box, click **Close**.

Tools Commands

The tools commands allow you to transfer files from the selected network element. The commands include:

- From FTP, page 28-28
- From TFTP, page 28-28
- To FTP, page 28-29
- To TFTP, page 28-29

Note The tools commands are unavailable on the Cisco Carrier Packet Transport (CPT) System.

From FTP

Use the **From FTP** command to perform FTP on the selected network element.

Step 1 In the Network Vision List or Map View, right-click the network element.

Step 2 Choose **Commands > Tools > File copy > From FTP**.

Step 3 Enter the value for the following parameter.

Input Parameter	Description
Source File	The configuration source file type.
Dest file	The destination configuration file type- running config or start-up config.
Password	The FTP password.
Source IP	The source IP address
Source file	The configuration source file type.
User	The FTP user name

Step 4 To see the commands that will be applied on the device, click **Preview**.

Step 5 You can view the commands in the Result tab. You can go back and make any required changes to the input parameters.

Step 6 To schedule the command, click the Scheduling tab. For more details on scheduling, see Scheduling a Command.

Step 7 To run the commands, click **Execute Now**.

You can view errors in the Result tab, if there are any.

Step 8 To close the dialog box, click **Close**.

From TFTP

Use the **From TFTP** command to perform TFTP on the selected network element.

Step 1 In the Network Vision List or Map View, right-click the network element.

Step 2 Choose **Commands > Tools > File copy > From TFTP**.

Step 3 Enter the value for the following parameter.

Input Parameter	Description
Dest file	The destination configuration file type.
Source IP	The source IP address.
Source file	The configuration source file type.

Step 4 To see the commands that will be applied on the device, click **Preview**.

Step 5 You can view the commands in the Result tab. You can go back and make any required changes to the input parameters.

Step 6 To schedule the command, click the Scheduling tab. For more details on scheduling, see Scheduling a Command.

Step 7 To run the commands, click **Execute Now**.

You can view errors in the Result tab, if there are any.

Step 8 To close the dialog box, click **Close**.

To FTP

Use the **To FTP** command to perform FTP on the selected network element.

Step 1 In the Network Vision List or Map View, right-click the network element.

Step 2 Choose **Commands > Tools > File copy > To FTP**.

Step 3 Enter the value for the following parameter

Input Parameter	Description
Destination IP	The destination IP address.
Destination file	The destination file.
Password	The FTP password.
Source file	The source configuration file type.
User	The FTP user name.

Step 4 To see the commands that will be applied on the device, click **Preview**.

Step 5 You can view the commands in the Result tab. You can go back and make any required changes to the input parameters.

Step 6 To schedule the command, click the Scheduling tab. For more details on scheduling, see Scheduling a Command.

Step 7 To run the commands, click **Execute Now**.

You can view errors in the Result tab, if there are any.

Step 8 To close the dialog box, click **Close**.

To TFTP

Use the **To TFTP** command to perform TFTP on the selected network element.

Step 1 In the Network Vision List or Map View, right-click the network element.

Step 2 Choose **Commands > Tools > File copy > To FTP**.

Step 3 Enter the value for the following parameter.

Input Parameter	Description
Destination IP	The destination IP address
Destination file	The destination file
Source file	The source configuration file type

Step 4 To see the commands that will be applied on the device, click **Preview**.

Step 5 You can view the commands in the Result tab. You can go back and make any required changes to the input parameters.

Step 6 To schedule the command, click the Scheduling tab. For more details on scheduling, see Scheduling a Command.

Step 7 To run the commands, click **Execute Now**.

You can view errors in the Result tab, if there are any.

Step 8 To close the dialog box, click **Close**.

OAM Commands

TheOAM commands allow you to perform operations, administration, and maintanence operations on the selected network element. The commands include:

- Destination From Device, page 28-30
- Ping VRF, page 28-31
- Trace Route From Device, page 28-31
- Trace Route VRF, page 28-32

Destination From Device

Use the **Destination From Device** command to view the destination from device on the selected network element.

Step 1 In the Network Vision List or Map View, right-click the network element.

Step 2 Choose **Commands > OAM > Ping > Destination From Device**.

Step 3 Enter the value for the following parameter.

Input Parameter	Description
Destination address	The destination address.

Step 4 To see the commands that will be applied on the device, click **Preview**.

Step 5 You can view the commands in the Result tab. You can go back and make any required changes to the input parameters.

Step 6 To schedule the command, click the Scheduling tab. For more details on scheduling, see Scheduling a Command.

Step 7 To run the commands, click **Execute Now**.

You can view errors in the Result tab, if there are any.

Step 8 To close the dialog box, click **Close**.

Ping VRF

Use the **Ping VRF** command to perform ping VRF on the selected network element.

Step 1 In the Network Vision List or Map View, right-click the network element.

Step 2 Choose **Commands > OAM > Ping VRF**.

Step 3 Enter the value for the following parameter

Input Parameter	Description
Destination address	The destination address.

Step 4 To see the commands that will be applied on the device, click **Preview**.

Step 5 You can view the commands in the Result tab. You can go back and make any required changes to the input parameters.

Step 6 To schedule the command, click the Scheduling tab. For more details on scheduling, see Scheduling a Command.

Step 7 To run the commands, click **Execute Now**.

You can view errors in the Result tab, if there are any.

Step 8 To close the dialog box, click **Close**.

Trace Route From Device

Use the **Trace Route From Device** command to view the trace route from the selected network element.

Step 1 In the Network Vision List or Map View, right-click the network element.

Step 2 Choose **Commands > OAM > Trace Route From Device.**

Step 3 Enter the value for the following parameter

Input Parameter	Description
Destination address	The destination address.

Step 4 To see the commands that will be applied on the device, click **Preview**.

Step 5 You can view the commands in the Result tab. You can go back and make any required changes to the input parameters.

Step 6 To schedule the command, click the Scheduling tab. For more details on scheduling, see Scheduling a Command.

Step 7 To run the commands, click **Execute Now**.

You can view errors in the Result tab, if there are any.

Step 8 To close the dialog box, click **Close**.

Trace Route VRF

Use the **Trace Route VRF** command to view the trace route VRF from the selected network element.

Step 1 In the Network Vision List or Map View, right-click the network element.

Step 2 Choose **Commands > OAM > Trace Route VRF.**

Step 3 Enter the value for the following parameter.

Input Parameter	Description
Destination address	The destination address.

Step 4 To see the commands that will be applied on the device, click **Preview**.

Step 5 You can view the commands in the Result tab. You can go back and make any required changes to the input parameters.

Step 6 To schedule the command, click the Scheduling tab. For more details on scheduling, see Scheduling a Command.

Step 7 To run the commands, click **Execute Now**.

You can view errors in the Result tab, if there are any.

Step 8 To close the dialog box, click **Close**.

Scheduling a Command

You can specify when you want to execute a command using the Scheduling tab of the commands window.

To schedule a command, you must:

Step 1 In the Network Vision List or Map View, right-click the network element.

Step 2 Choose **Commands** and then select the desired command**.**

Step 3 Click the Scheduling tab.

Step 4 Choose Execute Now to execute the command at that instance.

Step 5 Choose Schedule Job to schedule the command to execute later.

a. Click Once to specify the command to execute only once. You must specify the date and the time you want the command to execute.

b. Click Recurring to specify that you want the command to be executed in a recurring manner. You must specify the from and to date and time. You can execute the command:

- Every specific time. For example every twenty minutes.
- Daily– You can select Daily if you want the selected command to be executed every day.
- Weekly– You can select which day of the week you want to execute the command.
- Monthly– You can select which day of the month you want to execute the comand.

Step 6 Enter the values for the comment.

Step 7 To preview the executed command, click **Preview**.

Step 8 To execute the command as specified in the command window, click **Execute Now**.

Step 9 To close the window, click **Close**.



INDEX

A

adaptive polling
  alarm description 15-4
  registry parameters 15-67
All IP Interfaces Down alarm 15-5, 15-69
ATM
  VNE topology type 12-2
ATM IMA Down
  event registry 15-70
ATM IMA Service
  alarm description 15-5, 15-49, 15-158

B

BGP
  VNE topology type 12-2
BGP alarms
  BGP Link Down 15-7, 15-76, 15-210
  BGP Neighbor Loss 15-9, 15-10, 15-16, 15-17, 15-18, 15-19, 15-20, 15-21, 15-48, 15-55, 15-56, 15-78
  BGP Process Down 15-10, 15-11, 15-81
Broken LSP Discovered alarm 15-11, 15-13, 15-82
business, VNE topology type 12-2

C

Card Down alarm 15-14, 15-82
Card Out alarm 15-14, 15-15, 15-83
CDP
  VNE topology type 12-8
CFM Domain Fault
  registry 15-95
Chassis Disconnected 15-22
Chassis Disconnected Alarm 15-22
cloud VNE
  Cloud Problem alarm 15-22, 15-23, 15-99
Component Unreachable alarm 15-23, 15-100
CPU usage
  CPU Utilization alarm 15-15, 15-26, 15-101

D

Device Unsupported alarm 15-27, 15-102
Discard Packets alarm 15-27, 15-103
Dropped Packets alarm 15-28, 15-29, 15-104
DS0 Bundle alarm
  event registry 15-105
DS1 Path Link Down
  alarm 15-29
  event registry 15-107
DS1 Path Port Down
  alarm 15-30
  event registry 15-111
DS3 Path Link Down
  alarm 15-30
  event registry 15-113
DS3 Path Port Down
  alarm 15-31
  event registry 15-117
Dual Stack IP Changed
  event registry 15-119
Dual Stack IP Changed alarm 15-31
DWDM Service alarm 15-32, 15-35
  event registry 15-121, 15-122

E

EFP Down alarm 15-33, 15-124
esmc process down alarm 15-33
Ethernet
  VNE topology type 12-2
events
  security 14-1

F

Frame Relay
  VNE topology type 12-3

G

GRE
  GRE Keepalive alarm 15-35
    subtype event registry 15-130
  GRE Tunnel Down alarm 15-35, 15-131
  GRE Tunnel endpoint OID structure 15-210
GRE Tunnel, VNE topology type 12-5

H

HDLC
  VNE topology type 12-4
HSRP
  HSRP Group Status Changed alarm 15-36, 15-132

I

Interface Status alarm 15-37, 15-134
Investigation State alarm 15-39, 15-137
ISyncEOID 15-206

K

keepalive message (GRE tunnel) 15-35

L

L2TP Peer Not Established alarm 15-39, 15-137
L2TP Sessions Threshold alarm 15-40, 15-139
Layer 2 MPLS Tunnel Endpoint, OID structure 15-210
Layer 2 Tunnel Down alarm 15-42, 15-144
LDP Neighbor Loss alarm 15-43, 15-145
links
  Link Down alarm 15-44, 15-146
  Link Down alarm endpoint OID structure 15-209
  Link Utilization alarm 15-149
Link Utilization alarm 15-45
Logical Port Down alarm 15-46, 15-152
lsp down alarm 15-47
lsp end point OID 15-202

M

Memory Utilization alarm 15-49, 15-157
MPLS
  VNE topology type 12-4
MPLS alarms
  MPLS Black Hole Found alarm 15-50, 15-162
  MPLS Interface Removed alarm 15-51, 15-163
  MPLS TE Tunnel Down alarm 15-53, 15-166
  MPLS TE Tunnel OID structure 15-206
MPLS TE FRR State Changed
  alarm 15-52
  registry entries 15-164
MPLS-TP Commands 24-2
mpls tp tunnel down alarm 15-54

N

network clock synchronization 15-55

O

obtaining documentation 1-xxxiii
ospf neighbour state change 15-56
ospf neighbour state change OID 15-207

P

physical layer, VNE topology type 12-5
port alarms
  Port Down alarm 15-56, 15-174
  REP Port Role Change 15-58
PWE3
  VNE topology type 12-5

Q

QinQ
  Subinterface Down alarm 15-62

R

registry parameters, service alarms 15-65
related documentation 1-xxxiii
Rx Dormant alarm 15-59, 15-181
Rx Utilization alarm 15-60, 15-182

S

security
  events 14-1
service alarms
  list of supported alarms 15-2
  overview 15-1
  registry parameters 15-65
  source OIDs 15-196
Shelf Out alarm 15-60, 15-183
source OIDs (object identifiers) 15-196
  BGP Neighbor Entry OID 15-197
  Chassis OID 15-198
  DWDM Controller OID 15-199
  EFP OID 15-199
  IP Interface OID 15-200
  L2TP Peer OID 15-201
  Logical Port OID 15-202
  LSE (Label Switching Entity) OID 15-203
  LSE Entry OID 15-203
  Managed Element OID 15-204
  Module OID 15-205
  MP-BGP OID 15-205
  MPLS TE Tunnel OID 15-206
  Physical Layer OID 15-207
  Shelf OID 15-208
  Topological Link OID 15-208, 15-209
  VLAN Tagged Interface OID 15-211
  VSI OID 15-211
Subinterface Down alarm 15-62, 15-190
submitting a service request 1-xxxiii

T

technologies, supported 11-1
tp tunnel endpoint OID 15-206
Tx Dormant alarm 15-63, 15-192
Tx Utilization alarm 15-64, 15-193

V

VNE topology
  CDP 12-8
  physical layer 12-10
  traffic signature 12-7

types
ATM 12-2
BGP 12-2
business 12-2
Ethernet 12-2
Frame Relay 12-3
GRE Tunnel 12-5
HDLC 12-4
MPLS 12-4
physical layer 12-5
PPP 12-4
PWE3 12-5
VPN 12-5
VPN
VNE topology type 12-5
VSI Down alarm 15-64, 15-194