



Cisco Active Network Abstraction 3.7.1 Reference Guide

August 30, 2010

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

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 of Cisco Systems, Inc. and/or its affiliates in the U.S. and other countries. A listing of Cisco's trademarks can be found at 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. (1005R)

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 Active Network Abstraction 3.7.1 Reference Guide
© 1999-2010 Cisco Systems, Inc. All rights reserved.



CONTENTS

Preface **xv**

- New and Changed Information **xv**
- Audience **xvi**
- Conventions **xvi**
- Related Documentation **xvii**
- Obtaining Documentation and Submitting a Service Request **xviii**

PART 1

Cisco VNEs

CHAPTER 1

Introduction **1-1**

- Introduction to VNEs **1-1**
- Understanding the Tables **1-1**

CHAPTER 2

Overview—Supported Network Elements in Cisco ANA Version 3.7.1 **2-1**

- Supported Cisco Security Appliances in Cisco ANA Version 3.7.1 **2-2**
- Supported Cisco Access Servers in Cisco ANA Version 3.7.1 **2-2**
- Supported Cisco Gateways in Cisco ANA Version 3.7.1 **2-3**
- Supported Cisco Routers in Cisco ANA Version 3.7.1 **2-3**
- Supported Cisco Switches in Cisco ANA Version 3.7.1 **2-12**
- Supported Generic Devices in Cisco ANA Version 3.7.1 **2-18**

CHAPTER 3

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

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

CHAPTER 4

Support Information for Cisco Access Servers **4-1**

- Cisco Access Server 5800 Series **4-1**
- Supported Technologies on Cisco Access Servers **4-4**

CHAPTER 5

Support Information for Cisco Gateways **5-1**

- Cisco AS5300 Series Universal Gateways **5-1**

Supported Technologies on Cisco Gateways 5-4

CHAPTER 6

Support Information for Cisco Routers 6-1

Cisco 800 Series Routers	6-2
Cisco 1000 Series Routers	6-5
Cisco 1600 Series Routers	6-8
Cisco 1700 Series Modular Access Routers	6-12
Cisco 1800 Series Integrated Services Routers	6-17
Cisco 2500 Series Routers	6-26
Cisco 2600 Series Multiservice Platform Routers	6-30
Cisco 2800 Series Integrated Services Routers	6-35
Cisco 2900 Series Integrated Services Router	6-41
Cisco 3600 Series Multiservice Platform Routers	6-45
Cisco 3700 Series Multiservice Access Routers	6-54
Cisco 3800 Series Integrated Services Routers	6-58
Cisco 3900 Series Integrated Service Routers	6-63
Cisco 4700 Series Routers	6-67
Cisco 7200 Series Routers	6-70
Cisco 7300 Series Routers	6-79
Cisco 7400 Series Routers	6-84
Cisco 7500 Series Routers	6-90
Cisco 7600 Series Routers	6-94
Cisco 10000 Series Routers	6-114
Cisco 12000 Series Routers	6-119
Cisco XR 12000 Series Routers	6-130
Cisco CRS-1 Carrier Routing System	6-142
Cisco ASR 1000 Series Routers	6-154
Cisco ASR 9000 Series Aggregation Services Routers	6-160
Cisco MWR 2900 Series Mobile Wireless Routers	6-166
Cisco Universal Broadband Router 7200 Series	6-172
Cisco Universal Broadband Router 10000 Series	6-176
Supported Technologies on Cisco Routers	6-181

CHAPTER 7

Support Information for Cisco Switches 7-1

Cisco Catalyst 1900 Series Switches	7-2
Cisco Catalyst 2900 Series Switches	7-3

Cisco ME 3400 Series Ethernet Access Switches	7-6
Cisco Catalyst 3500 XL Series Switches	7-10
Cisco Catalyst 3550 Series Switches	7-12
Cisco Catalyst 3560 Series Switches	7-15
Cisco ME 3600X Ethernet Access Switch	7-18
Cisco Catalyst 3750 Series Switches	7-21
Cisco Catalyst 3750 Metro Series Switches	7-24
Cisco ME 3800X Carrier Ethernet Switches	7-29
Cisco Catalyst 4000 Series Switches	7-33
Cisco Catalyst 4500 Series Switches	7-36
Cisco ACE 4700 Series Access Control Engine	7-43
Cisco Catalyst 4900 Series Switches	7-49
Cisco ME 4900 Series Ethernet Switch	7-57
Cisco Catalyst 5000 Series Switches	7-63
Cisco Catalyst 6500 Series (CatOS) Switches	7-65
Cisco Catalyst 6500 Series (IOS) Switches	7-70
Cisco ME 6500 Series Ethernet Switches (6524)	7-82
Cisco Nexus 7000 Series Switches	7-85
Cisco Service Control Engines	7-87
Supported Technologies on Cisco Switches	7-89

CHAPTER 8**Support Information for Generic Devices 8-1**

Understanding the Generic VNE	8-1
Supported Technologies on Generic Devices	8-5

PART 2**Technology Support and Information Model Objects****CHAPTER 9****Technology Support Introduction 9-1**

Supported Technologies	9-1
Networking-Related IMOs	9-4
Scheme Values	9-6
Polling Interval Values	9-6

CHAPTER 10**Internet Protocol 10-1**

Technology Description	10-1
Information Model Objects (IMOs)	10-4

Network Topology 10-13

Service Alarms 10-14

CHAPTER 11

Routing Protocols 11-1

Technology Description 11-1

Information Model Objects (IMOs) 11-3

Vendor-Specific Inventory and IMOs 11-7

Network Topology 11-7

Service Alarms 11-7

CHAPTER 12

VPN and VRF 12-1

Technology Description 12-1

Information Model Objects (IMOs) 12-2

Vendor-Specific Inventory and IMOs 12-4

Network Topology 12-4

Service Alarms 12-5

CHAPTER 13

Bidirectional Forwarding Detection 13-1

Technology Description 13-1

Information Model Objects (IMOs) 13-2

Vendor-Specific Inventory and IMOs 13-2

Network Topology 13-2

Service Alarms 13-3

CHAPTER 14

Session Border Controller 14-1

Technology Description 14-1

Information Model Objects (IMOs) 14-2

Vendor-Specific Inventory and IMOs 14-20

Network Topology 14-20

Service Alarms 14-20

CHAPTER 15

Multiprotocol Label Switching 15-1

Technology Description 15-1

Information Model Objects (IMOs) 15-2

Vendor-Specific Inventory and IMOs 15-6

Network Topology 15-6

Service Alarms 15-6

CHAPTER 16

Multiprotocol Label Switching Traffic Engineering 16-1

Technology Description 16-1

Information Model Objects (IMOs) 16-2

Vendor-Specific Inventory and IMOs 16-4

Network Topology 16-4

Service Alarms 16-5

CHAPTER 17

Pseudowire 17-1

Technology Description 17-1

Information Model Objects (IMOs) 17-2

Vendor-Specific Inventory and IMOs 17-3

Network Topology 17-3

Service Alarms 17-3

CHAPTER 18

Ethernet (IEEE 802.3) 18-1

Technology Description 18-1

Information Model Objects (IMOs) 18-5

Vendor-Specific Inventory and IMOs 18-19

Network Topology 18-21

Service Alarms 18-22

CHAPTER 19

Ethernet OAM 19-1

Technology Description 19-1

Information Model Objects (IMOs) 19-2

Vendor-Specific Inventory and IMOs 19-11

Network Topology 19-11

Service Alarms 19-11

CHAPTER 20

Asynchronous Transfer Mode 20-1

Technology Description 20-1

Information Model Objects (IMOs) 20-3

Vendor-Specific Inventory and IMOs 20-9

Network Topology 20-14

Service Alarms 20-14

CHAPTER 21

Frame Relay 21-1

- Technology Description 21-1
- Information Model Objects (IMOs) 21-1
- Vendor-Specific Inventory and IMOs 21-4
- Network Topology 21-4
- Service Alarms 21-4

CHAPTER 22

Integrated Services Digital Network 22-1

- Technology Description 22-1
- Information Model Objects (IMOs) 22-1
- Vendor-Specific Inventory and IMOs 22-3
- Network Topology 22-3
- Service Alarms 22-3

CHAPTER 23

Point-to-Point Protocol 23-1

- Technology Description 23-1
- Information Model Objects (IMOs) 23-3
- Vendor-Specific Inventory and IMOs 23-4
- Network Topology 23-4
- Service Alarms 23-5

CHAPTER 24

High-Level Data Link Control 24-1

- Technology Description 24-1
- Information Model Objects (IMOs) 24-2
- Vendor-Specific Inventory and IMOs 24-2
- Network Topology 24-2
- Service Alarms 24-2

CHAPTER 25

Layer 2 Tunnel Protocol 25-1

- Technology Description 25-1
- Information Model Objects (IMOs) 25-2
- Vendor-Specific Inventory and IMOs 25-3
- Network Topology 25-4
- Service Alarms 25-5

CHAPTER 26**Discovery Protocols 26-1**

- Technology Description 26-1
- Information Model Objects (IMOs) 26-2
- Vendor-Specific Inventory and IMOs 26-3
- Network Topology 26-4
- Service Alarms 26-4

CHAPTER 27**Local Switching 27-1**

- Technology Description 27-1
- Information Model Objects (IMOs) 27-2
- Vendor-Specific Inventory and IMOs 27-2
- Network Topology 27-3
- Service Alarms 27-3

CHAPTER 28**Digital Subscriber Line 28-1**

- Technology Description 28-1
- Information Model Objects (IMOs) 28-2
- Vendor-Specific Inventory and IMOs 28-5
- Network Topology 28-6
- Service Alarms 28-6

CHAPTER 29**SONET/SDH 29-1**

- Technology Description 29-1
- Information Model Objects (IMOs) 29-2
- Vendor-Specific Inventory and IMOs 29-5
- Network Topology 29-5
- Service Alarms 29-5

CHAPTER 30**Internet Protocol Over Dense Wave Division Multiplexing 30-1**

- Technology Description 30-1
- Information Model Objects (IMOs) 30-2
- Vendor-Specific Inventory and IMOs 30-4
- Network Topology 30-4
- Service Alarms 30-4

CHAPTER 31

TDM/DSx 31-1

- Technology Description 31-1
- Information Model Objects (IMOs) 31-2
- Vendor-Specific Inventory and IMOs 31-5
- Network Topology 31-5
- Service Alarms 31-5

CHAPTER 32

Clocking 32-1

- Technology Description 32-1
- Information Model Objects (IMOs) 32-2
- Vendor-Specific Inventory and IMOs 32-9
- Network Topology 32-9
- Service Alarms 32-9

CHAPTER 33

Serial 33-1

- Technology Description 33-1
- Information Model Objects (IMOs) 33-2
- Vendor-Specific Inventory and IMOs 33-2
- Network Topology 33-2
- Service Alarms 33-2

CHAPTER 34

Access Control Lists 34-1

- Technology Description 34-1
- Information Model Objects (IMOs) 34-2
- Vendor-Specific Inventory and IMOs 34-3
- Network Topology 34-3
- Service Alarms 34-3

CHAPTER 35

Physical Components 35-1

- Information Model Objects (IMOs) 35-1
- Service Alarms 35-4

CHAPTER 36

Logical Components 36-1

- Information Model Objects (IMOs) 36-1
- Service Alarms 36-4

CHAPTER 37**Common Components 37-1**

Information Model Objects (IMOs) 37-1

Network Topology 37-7

Service Alarms 37-7

CHAPTER 38**Cisco ANA VNE Topology 38-1**

Specifications 38-1

Topology Types 38-7

PART 3**Alarms and Events****CHAPTER 39****System Events 39-1****CHAPTER 40****Security Events 40-1****CHAPTER 41****Service Alarms 41-1**

Service Alarms 41-2

Registry Parameters 41-58

Alarm Source OIDs 41-187

CHAPTER 42**Traps 42-1**

Cisco ASR 9000 V1 Traps 42-3

Cisco ASR 9000 V2/V3 Traps 42-4

Cisco IOS V1 Traps 42-6

Cisco IOS V2/V3 Traps 42-62

Cisco IOX V1 Traps 42-90

Cisco IOX V2/V3 Traps 42-103

Cisco MIB2 V1 Traps 42-119

Cisco MIB2 V2/V3 Traps 42-129

Cisco ACE V1 Traps 42-139

Cisco ACE V2/V3 Traps 42-140

Cisco Nexus V1 Traps 42-141

Cisco Nexus V2/V3 Traps 42-154

Cisco ASR 9000 V1 Trap Registry Parameters 42-161

Cisco ASR 9000 V2/V3 Registry Parameters 42-162

Cisco IOS V1 Trap Registry Parameters 42-163

Cisco IOS V2/V3 Trap Registry Parameters	42-188
Cisco IOX V1 Trap Registry Parameters	42-209
Cisco IOX V2/V3 Trap Registry Parameters	42-218
Cisco MIB2 V1 Trap Registry Parameters	42-229
Cisco MIB2 V2/V3 Trap Registry Parameters	42-237
Cisco ACE V1 Trap Registry Parameters	42-245
Cisco ACE V2/V3 Trap Registry Parameters	42-246
Cisco Nexus V1 Trap Registry Parameters	42-247
Cisco Nexus V2/V3 Trap Registry Parameters	42-251

CHAPTER 43

Syslogs 43-1

Cisco ASR 9000 Syslogs	43-2
Cisco IOS Syslogs	43-3
Cisco IOX Syslogs	43-20
Cisco ACE Syslogs	43-32
Cisco Nexus Syslogs	43-36
Cisco ASR 9000 Syslog Registry Parameters	43-37
Cisco IOS Syslog Registry Parameters	43-39
Cisco IOX Syslog Registry Parameters	43-61
Cisco ACE Syslog Registry Parameters	43-71
Cisco Nexus Syslog Registry Parameters	43-76

PART 4

Commands

CHAPTER 44

Using Connectivity Fault Management Commands 44-1

Supported Network Elements	44-2
Configuring CFM Components	44-3
Diagnose CFM Components	44-10

CHAPTER 45

Using Resilient Ethernet Protocol Command 45-1

Supported Network Elements	45-2
Displaying REP Segment Data	45-3

CHAPTER 46

Using Cisco Carrier Grade NAT Commands 46-1

Supported Network Elements	46-2
Configuring Carrier Grade NAT Instance	46-2

Removing a Carrier Grade NAT instance 46-3

Displaying Pool Utilization 46-3

CHAPTER 47**Using Pseudowire Virtual Circuit Connectivity Verification Commands 47-1**

Supported Network Elements 47-2

Pinging the Peer Router from a Single Segment or Multisegment Pseudowire 47-2

Displaying Pseudowire Information 47-3

CHAPTER 48**Using Link Operations, Administration and Maintenance Operations Commands 48-1**

Supported Network Elements 48-1

Configuring L-OAM Components 48-2

CHAPTER 49**Using Ethernet Local Management Interface Commands 49-1**

Supported Network Elements 49-1

Configuring Ethernet LMI Components 49-2

INDEX



Preface

This Guide provides reference information on Cisco Active Network Abstraction (Cisco ANA) version 3.7.1. This information is presented in four parts:

- Part 1—Cisco VNEs: Supplies detailed information on all of the Virtual Network Elements (VNEs) supplied with Cisco ANA.
- Part 2—Technology Support and Information Model Objects: Details the level of functionality Cisco ANA provides for each of the networking technologies it supports, and explains how the product models these technologies using VNEs and Information Model Objects (IMOs).
- Part 3—Alarms and Events: Lists and describes all of the Cisco ANA alarms, events, SNMP traps, and syslogs, supported in this version of Cisco ANA.
- Part 4—Commands: Lists, describes, and explains how to use the commands supplied with Cisco ANA. Note that additional Cisco ANA command scripts are available for download from the Cisco ANA Tech Center at <http://developer.cisco.com/web/ana/home>.

New and Changed Information

The following table describes information that has been added or changed since the initial release of the *Cisco Active Network Abstraction 3.7.1 Reference Guide*.

Table 1 ***New and Changed Information in This Guide***

Date Released	Revision	Location
July 6, 2011	Removed ACE20-MOD-K9 module support for Cisco 7600 series routers.	Cisco 7600 Series—Supported Modules, page 96
	Updated SNMP informs support for traps.	Traps, page 1

Table 1 *New and Changed Information in This Guide (continued)*

Date Released	Revision	Location
June 8, 2011	Updated the NE Type and Sys OID for the Cisco Service Control Engines.	Cisco Service Control Engines, page 18
	Included additional information for Cisco XR 12000 series routers and Cisco Carrier Routing System (CRS-1).	• Cisco XR 12000 Series—Additional Information, page 141 • Cisco CRS-1—Additional Information, page 151
	Replaced the image capture for the expanded view of CRS-1 multichassis support.	Multichassis Support for CRS-1, page 152
	Updated the description of the supported modules for Cisco Catalyst 4500 series switches based on the prospectus.	Cisco Catalyst 4500 Series—Supported Modules, page 38
February 22, 2011	Verified and updated the short description of the subtype events for all the service alarms based on the Registry Editor.	Registry Parameters, page 58
February 3, 2011	Listed the following protocols that support Bidirectional Forwarding Detection (BFD): • OSPF • BGP • MPLS TE • IPv4 (static) • IPv6 (static) • IS-IS	Technology Description, page 1
	Changed the short description of the subtype events for the Lag Down and Lag Link Down alarms.	• Lag Admin Down • Lag Oper Down • Lag Up • Lag Link Admin Down • Lag Link Oper Down • Lag Link Up

Audience

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

Conventions

This document uses the following conventions:

Table 2 **Conventions**

Convention	Description
<i>string</i>	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.
<i>Italic text</i>	Indicates a variable or attribute value, including enumerated values.
<i>italic</i> 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

The following documentation is available for Cisco Active Network Abstraction 3.7.1:

- [Cisco Active Network Abstraction 3.7.1 Administrator Guide](#)
- [Cisco Active Network Abstraction 3.7.1 Customization User Guide](#)
- [Cisco Active Network Abstraction 3.7.1 Documentation Guide](#)
- [Cisco Active Network Abstraction 3.7.1 Installation Guide](#)
- [Cisco Active Network Abstraction 3.7.1 Release Notes](#)
- [Cisco Active Network Abstraction 3.7.1 User Guide](#)
- [Cisco Active Network Abstraction 3.7.1 Theory of Operations](#)
- [Cisco Active Network Abstraction Configuration and Image Management 1.0 User and Administrator Guide](#)
- [Cisco Active Network Abstraction Network Service Activation 1.1 User Guide](#)
- [Cisco Active Network Abstraction Network Service Activation 1.1 Customization Guide](#)
- [Open Source Used in Cisco Active Network Abstraction 3.7.1](#)

- *Cisco Active Network Abstraction 3.7.1 Integration Developer Guide* is available on the Cisco ANA Technology Center. This guide describes how to use Cisco ANA integration interfaces.

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

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 Cisco ANA 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](#)
- [ANA 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 Cisco ANA and that can be running on the NEs that Cisco ANA supports. For example: The “Cisco 7600 Series—Supported Software Versions” table lists Cisco IOS software version 12.2(18)SXD. This means that Cisco ANA will work with any supported Cisco 7600-series router (such as the Cisco 7603) that is running IOS release 12.2(18)SXD.

Cisco ANA may support subsequent maintenance releases of NE software versions, but only if these later NE software versions do not require changes in Cisco ANA to maintain compatibility. Changes in any of the following NE software components can affect compatibility with Cisco ANA, and may require Cisco ANA software changes: XML interfaces, SNMP commands, MIBs, and CLI commands. In cases where a new NE software version remains compatible without requiring changes in Cisco ANA, 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 Cisco ANA 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 Cisco ANA. For example, Cisco ANA supports IOS 12.2(33)SRC4 for 7600 devices. If IOS 12.2(33)SRC5 is released, Cisco ANA will recognize IOS 12.2.(33)SRC5 with the same level of support as IOS 12.2(33)SRC4 on 7600 devices. However, Cisco ANA will not support any additional software or hardware features introduced in IOS 12.2(33)SRC5.

Cisco ANA 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, Cisco ANA 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 Cisco ANA 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 Cisco ANA, and updates the online version of this Guide accordingly. If you are not sure whether the current version of Cisco ANA 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 Cisco ANA release. If the online version of this Guide does not list the new software version, contact Cisco Professional Services or your Cisco Sales Representative.

ANA Versions

The ANA Version column found in the tables in this Guide lists the version of ANA during which a VNE supporting the specified NE module, software, topology, or other feature was first introduced. It is therefore the earliest Cisco ANA version that supports that NE. All later versions of ANA also support the NE. 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, 3.6.2, and so on.

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 ANA Version 3.7.1

This chapter provides an overview of network elements (NEs) that are supported by Cisco ANA Version 3.7.1 and includes the following sections:

- [Supported Cisco Security Appliances in Cisco ANA Version 3.7.1, page 2-2](#)
- [Supported Cisco Access Servers in Cisco ANA Version 3.7.1, page 2-2](#)
- [Supported Cisco Gateways in Cisco ANA Version 3.7.1, page 2-3](#)
- [Supported Cisco Routers in Cisco ANA Version 3.7.1, page 2-3](#)
- [Supported Cisco Switches in Cisco ANA Version 3.7.1, page 2-12](#)
- [Supported Generic Devices in Cisco ANA Version 3.7.1, page 2-18](#)

Supported Cisco Security Appliances in Cisco ANA Version 3.7.1

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

- [Cisco Adaptive Security Appliance 5550 Series](#)
- [Cisco Adaptive Security Appliance 5580 Series](#)

Table 2-1 *Supported Cisco Security Appliances in Cisco ANA Version 3.7.1*

NE Type	Product Name	SysOID	ANA 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 ANA Version 3.7.1

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

- [Cisco Access Server 5800 Series](#)

Table 2-2 *Supported Cisco Access Servers in Cisco ANA Version 3.7.1*

NE Type	Product Name	SysOID	ANA 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 ANA Version 3.7.1

This document includes support information for the following Cisco gateways:

- [Cisco AS5300 Series Universal Gateways](#)

Table 2-3 **Supported Cisco Gateways in Cisco ANA Version 3.7.1**

NE Type	Product Name	SysOID	ANA 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 ANA Version 3.7.1

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 2900 Series Integrated Services Router](#)
- [Cisco 3600 Series Multiservice Platform Routers](#)
- [Cisco 3700 Series Multiservice Access Routers](#)
- [Cisco 3800 Series Integrated Services Routers](#)
- [Cisco 3900 Series Integrated Service Routers](#)
- [Cisco 4700 Series 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-1 Carrier Routing System](#)
- [Cisco ASR 1000 Series Routers](#)

- Cisco ASR 9000 Series Aggregation Services Routers
- Cisco MWR 2900 Series Mobile Wireless Routers
- Cisco Universal Broadband Router 7200 Series
- Cisco Universal Broadband Router 10000 Series

Table 2-4 Supported Cisco Routers in Cisco ANA Version 3.7.1

NE Type	Product Name	SysOID	ANA 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
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

Table 2-4 **Supported Cisco Routers in Cisco ANA Version 3.7.1 (continued)**

NE Type	Product Name	SysOID	ANA Version
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
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

Table 2-4 *Supported Cisco Routers in Cisco ANA Version 3.7.1 (continued)*

NE Type	Product Name	SysOID	ANA Version
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
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

Table 2-4 *Supported Cisco Routers in Cisco ANA Version 3.7.1 (continued)*

NE Type	Product Name	SysOID	ANA Version
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
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

Table 2-4 *Supported Cisco Routers in Cisco ANA Version 3.7.1 (continued)*

NE Type	Product Name	SysOID	ANA Version
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 2900 Series Integrated Services Router			
cisco2901	CISCO2901/K9	1.3.6.1.4.1.9.1.1046	3.7.1
cisco2911	CISCO2911/K9	1.3.6.1.4.1.9.1.1045	3.7.1
cisco2921	CISCO2921/K9	1.3.6.1.4.1.9.1.1044	3.7.1
cisco2951	CISCO2951/K9	1.3.6.1.4.1.9.1.1043	3.7.1
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
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			

Table 2-4 *Supported Cisco Routers in Cisco ANA Version 3.7.1 (continued)*

NE Type	Product Name	SysOID	ANA Version
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 3900 Series Integrated Service Routers			
ciscoISR3945	Cisco ISR 3945 Router	1.3.6.1.4.1.9.1.1041	3.7.1
ciscoISR3925	Cisco ISR 3925/K9 Router	1.3.6.1.4.1.9.1.1042	3.7.1
Cisco 4700 Series Routers			
cisco4700	Cisco 4700 Router	1.3.6.1.4.1.9.1.50	3.7.1
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			
cisco7604sysID	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

Table 2-4 *Supported Cisco Routers in Cisco ANA Version 3.7.1 (continued)*

NE Type	Product Name	SysOID	ANA Version
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	Cisco 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
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

Table 2-4 **Supported Cisco Routers in Cisco ANA Version 3.7.1 (continued)**

NE Type	Product Name	SysOID	ANA Version
cisco12404	Cisco 12404 Router	1.3.6.1.4.1.9.1.423	3.6.5
Cisco CRS-1 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
ciscoCrs4S	Cisco CRS-1 4-Slot Single-Shelf System	1.3.6.1.4.1.9.1.822	3.6.0
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	3.6.5
ciscoASR1006	Cisco ASR1006 Chassis, Dual P/S	1.3.6.1.4.1.9.1.925	3.6.5
ciscoASR1004	Cisco ASR1004 Chassis, Dual P/S	1.3.6.1.4.1.9.1.924	3.6.6
ciscoASR1002F	Cisco ASR 1002-F	1.3.6.1.4.1.9.1.1116	3.6.7
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 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 Universal Broadband Router 7200 Series			
ciscoUBR7246VXR	Cisco UBR7246VXR	1.3.6.1.4.1.9.1.271	3.7.1
Cisco Universal Broadband Router 10000 Series			
ciscoUBR10012	Cisco UBR 10012	1.3.6.1.4.1.9.1.317	3.7.1

Supported Cisco Switches in Cisco ANA Version 3.7.1

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 ME 3600X Ethernet Access Switch](#)
- [Cisco Catalyst 3750 Series Switches](#)
- [Cisco Catalyst 3750 Metro Series Switches](#)
- [Cisco ME 3800X Carrier Ethernet Switches](#)
- [Cisco Catalyst 4000 Series Switches](#)
- [Cisco Catalyst 4500 Series Switches](#)
- [Cisco ACE 4700 Series Access Control Engine](#)
- [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 Nexus 7000 Series Switches](#)
- [Cisco Service Control Engines](#)

Table 2-5 *Supported Cisco Switches in Cisco ANA Version 3.7.1*

NE Type	Product Name	SysOID	ANA 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

Table 2-5 *Supported Cisco Switches in Cisco ANA Version 3.7.1 (continued)*

NE Type	Product Name	SysOID	ANA Version
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
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
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

Table 2-5 *Supported Cisco Switches in Cisco ANA Version 3.7.1 (continued)*

NE Type	Product Name	SysOID	ANA Version
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
ciscoMe3400eg12Cs m	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
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

Table 2-5 *Supported Cisco Switches in Cisco ANA Version 3.7.1 (continued)*

NE Type	Product Name	SysOID	ANA Version
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
Cisco ME 3600X Ethernet Access Switch			
ciscoME3600x24FS M	Cisco ME-3600X-24FSM	1.3.6.1.4.1.9.1.1250	3.7.1
ciscoME3600x24TS M	Cisco ME-3600X-24TSM	1.3.6.1.4.1.9.1.1251	3.7.1
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
catalyst3750G24TS1 U	Cisco Catalyst 3750G-24TS-1U	1.3.6.1.4.1.9.1.624	3.6.4

Table 2-5 *Supported Cisco Switches in Cisco ANA Version 3.7.1 (continued)*

NE Type	Product Name	SysOID	ANA Version
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
catalyst3750Ge12Sfp Dc	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
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 ME 3800X Carrier Ethernet Switches			
ciscoME3800X24FSM	Cisco ME-3800X-24FSM	1.3.6.1.4.1.9.1.1252	3.7.1
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
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
catalyst4503E	Cisco Catalyst 4503E Switch	1.3.6.1.4.1.9.1.874	3.6.6
catalyst4507R-E	Cisco Catalyst 4507R-E Switch	1.3.6.1.4.1.9.1.876	3.6.6
catalyst4506E	Cisco Catalyst 4506-E Switch	1.3.6.1.4.1.9.1.875	3.6.7

Table 2-5 *Supported Cisco Switches in Cisco ANA Version 3.7.1 (continued)*

NE Type	Product Name	SysOID	ANA Version
catalyst4510	Cisco Catalyst 4510R Switch	1.3.6.1.4.1.9.1.537	3.6.7
catalyst4510RE	Cisco Catalyst 4510R-E Switch	1.3.6.1.4.1.9.1.877	3.6.7
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 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
Cisco ME 4900 Series Ethernet Switch			
ciscoMe492410GE	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
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			
ciscoWSC6509neba	Cisco Catalyst 6509-NEB-A Switch	1.3.6.1.4.1.9.1.534	3.6.0

Table 2-5 Supported Cisco Switches in Cisco ANA Version 3.7.1 (continued)

NE Type	Product Name	SysOID	ANA Version
cat6509Sp	Cisco Catalyst 6509-NEB Switch	1.3.6.1.4.1.9.1.310	3.6.0
ciscoWSC6503	Cisco Catalyst 6503 Switch	1.3.6.1.4.1.9.1.449	3.6.0
cat6506	Cisco Catalyst 6506 Switch	1.3.6.1.4.1.9.1.282	3.6.0
cat6509	Cisco Catalyst 6509 Switch	1.3.6.1.4.1.9.1.283	3.6.0
ciscoWSC6504E	Cisco Catalyst 6504-E Switch Chassis	1.3.6.1.4.1.9.1.657	3.6.0
ciscoWSC6513	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
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 Nexus 7000 Series Switches			
cevChassisN7Kc7010	Cisco Nexus 7010 Switch	1.3.6.1.4.1.9.12.3.1.3.612	3.7.1
cevChassisN7Kc7018	Cisco Nexus 7018 Switch	1.3.6.1.4.1.9.12.3.1.3.777	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.

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

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

Supported Generic Devices in Cisco ANA Version 3.7.1

This document includes support information for the following Generic devices:

- Generic VNE

Table 2-6 Supported Generic Devices in Cisco ANA Version 3.7.1

NE Type	Product Name	SysOID	ANA Version
Generic VNE			
Generic device		1.3.999.3	3.6.0



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 ANA Version 3.7.1. For more information about the objects and attributes described in this chapter, see Part 2: Technology Support and Information Model Objects.

This chapter contains the following topics:

- [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](#)

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 ANA Version 3.7.1, 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 ANA Version 3.7.1*

Software Version	ANA 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 ANA Version 3.7.1

Topology Type	Link Type	ANA Version
Ethernet	Ethernet	3.6.3

Cisco ASA 5550 Series—Supported Modules

Table 3-3 Supported Modules for Cisco ASA 5550 Series—Cisco ANA Version 3.7.1

Module Name	ANA 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 ANA Version 3.7.1:

- [IP, page 3-6](#)
- [Ethernet, page 3-9](#)
- [Hardware, page 3-14](#)
- [Serial, page 3-17](#)

Cisco ASA 5550 Series—Supported Service Events

Table 3-4 Supported Service Events for Cisco ASA 5550 Series—Cisco ANA Version 3.7.1

Event Name	ANA 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 ANA Version 3.7.1

Event Name	ANA 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

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 ANA Version 3.7.1, see [Cisco Adaptive Security Appliance 5580 Series](#)):

- [Cisco ASA 5580 Series—Supported Software Versions](#), page 3-3
- [Cisco ASA 5580 Series—Supported Topologies](#), page 3-3
- [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 3-5

Cisco ASA 5580 Series—Supported Software Versions

Table 3-5 Supported Software Versions for Cisco ASA 5580 Series—Cisco ANA Version 3.7.1

Software Version	ANA Version
8.1(2)	3.7
8.1(2)12	3.7

Cisco ASA 5580 Series—Supported Topologies

Table 3-6 Supported Topologies for Cisco ASA 5580 Series—Cisco ANA Version 3.7.1

Topology Type	Link Type	ANA Version
Ethernet	Ethernet	3.7

Cisco ASA 5580 Series—Supported Modules

Table 3-7 Supported Modules for Cisco ASA 5580 Series—Cisco ANA Version 3.7.1

Module Name	ANA 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 ANA Version 3.7.1:

- [IP, page 3-6](#)
- [Ethernet, page 3-9](#)
- [Hardware, page 3-14](#)
- [Serial, page 3-17](#)

Cisco ASA 5580 Series—Supported Service Events

Table 3-8 *Supported Service Events for Cisco ASA 5580 Series—Cisco ANA Version 3.7.1*

Event Name	ANA 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
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

Supported Technologies on Cisco Security Appliances

The following sections list the objects and attributes that are supported on Cisco security appliances in Cisco ANA Version 3.7.1 per technology:

- [IP, page 3-6](#)
- [Ethernet, page 3-9](#)
- [Hardware, page 3-14](#)
- [Serial, page 3-17](#)

For information about IMO changes in Cisco ANA 3.7.1, please see <http://developer.cisco.com/web/ana/integration>.

IP

Table 3-9 IP Attribute Support on Cisco Security Appliances—Cisco ANA Version 3.7.1

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

Table 3-9 IP Attribute Support on Cisco Security Appliances—Cisco ANA Version 3.7.1

Attribute	ASA5550	ASA5580
Next Hop IP Address	Y	Y
Type	Y	Y
Routing Protocol Type	Y	Y
Outgoing Interface Name	Y	Y
IMO Name—IARPEntity		
ARP Table	Y	Y
IMO Name—IARPEntity		
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—IIPRangeBasedIIPPoolEntry		
Start IP Address		
End IP Address		
Unused Addresses		
Used Addresses		
Reserved Addresses		
IMO Name—IIPSubnetBasedIIPPoolEntry		
IP Subnet		
Unused Addresses		
Used Addresses		
Reserved Addresses		
IMO Name—HSRPGGroupEntry		
Group Number		
Port Description		
Priority		
Coupled Router		
State		
Tracking Interfaces		
Virtual IP Address		
Virtual MAC Address		

Table 3-9 *IP Attribute Support on Cisco Security Appliances—Cisco ANA Version 3.7.1*

Attribute	ASA5550	ASA5580
IMO Name—I Tunnel GRE		
Name		
Tunnel Destination and Source		
IP Address		
IP Interface State		
IANA Type		
Containing CTPs		
Contained CTPs		
Keep Alive Time		
Keep Alive Retry		
IMO Name—I IPSLA Responder Service		
responderStatus		
TWAMP Responder Status		
tcpConnect		
udpEcho		
IMO Name—I IP Address Port Pair		
type		
ipAddress		
port		

Ethernet

Table 3-10 Ethernet Attribute Support on Cisco Security Appliances—Cisco ANA Version 3.7.1

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		

Table 3-10 Ethernet Attribute Support on Cisco Security Appliances—Cisco ANA Version 3.7.1

Attribute	ASA5550	ASA5580
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		
StpForwardDelay		

Table 3-10 Ethernet Attribute Support on Cisco Security Appliances—Cisco ANA Version 3.7.1

Attribute	ASA5550	ASA5580
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		
StpBridgeMaxAge		

Table 3-10 Ethernet Attribute Support on Cisco Security Appliances—Cisco ANA Version 3.7.1

Attribute	ASA5550	ASA5580
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		
Mac Address		

Table 3-10 Ethernet Attribute Support on Cisco Security Appliances—Cisco ANA Version 3.7.1

Attribute	ASA5550	ASA5580
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		
IslAgeoutTimer		
remoteDeviceName		
remoteDeviceMac		

Table 3-10 Ethernet Attribute Support on Cisco Security Appliances—Cisco ANA Version 3.7.1

Attribute	ASA5550	ASA5580
remotePortName		
IMO Name—IBridgeLan		
Id		
IMO Name—IIBridgeEntry		
IS Id		
IBridge		
BBridge		

Hardware

Table 3-11 Hardware Attribute Support on Cisco Security Appliances—Cisco ANA Version 3.7.1

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		

Table 3-11 Hardware Attribute Support on Cisco Security Appliances—Cisco ANA Version 3.7.1

Attribute	ASA5550	ASA5580
Redundant Equipment		
Configured Redundancy		
Redundancy Status		
Operational Status Last Changed		
Supported Physical Termination Points		
Serial Number (soft property)	Y	Y
Slots Number		
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		
IP Address Pools		
Forwarding Components List		

Table 3-11 Hardware Attribute Support on Cisco Security Appliances—Cisco ANA Version 3.7.1

Attribute	ASA5550	ASA5580
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 ANA Version 3.7.1

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		
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 ANA Version 3.7.1. For more information about the objects and attributes described in this chapter, see Part 2: Technology Support and Information Model Objects.

This chapter contains the following topics:

- [Cisco Access Server 5800 Series, page 4-1](#)
- [Supported Technologies on Cisco Access Servers, page 4-4](#)

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 ANA Version 3.7.1, see [Cisco Access Server 5800 Series](#)):

This section contains the following topics:

- [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 ANA Version 3.7.1*

Software Version	ANA 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 ANA Version 3.7.1*

Topology Type	Link Type	ANA 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 ANA Version 3.7.1*

Module Name	ANA 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 ANA Version 3.7.1:

- [IP, page 4-5](#)
- [Routing Protocols, page 4-8](#)
- [Ethernet, page 4-10](#)
- [TDM/DSx, page 4-15](#)
- [Security, page 4-18](#)
- [Hardware, page 4-19](#)
- [Serial, page 4-21](#)

Cisco AS 5800 Series—Supported Service Events

Table 4-4 Supported Service Events for Cisco AS 5800 Series—Cisco ANA Version 3.7.1

Event Name	ANA 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
Interface status down flapping	3.7.1	Y
Interface status down flapping update	3.7.1	Y
Layer 2 Tunnel Down	3.7.1	N
Link 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
Port Down	3.7.1	N
Port Flapping	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 down	3.7.1	N

Table 4-4 *Supported Service Events for Cisco AS 5800 Series—Cisco ANA Version 3.7.1*

Event Name	ANA Version	Expedited
EFP up	3.7.1	N
Interface status up	3.7.1	N
LAG down	3.7.1	N
LAG down	3.7.1	N
LAG Link 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
MPLS-TE tunnel down	3.7.1	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 down	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

Supported Technologies on Cisco Access Servers

The following sections list the objects and attributes that are supported on Cisco access servers in Cisco ANA Version 3.7.1 per technology:

This section contains the following topics:

- [IP, page 4-5](#)
- [Routing Protocols, page 4-8](#)
- [Ethernet, page 4-10](#)
- [TDM/DSx, page 4-15](#)
- [Security, page 4-18](#)
- [Hardware, page 4-19](#)
- [Serial, page 4-21](#)

IP

Table 4-5 *IP Attribute Support on Cisco Access Servers—Cisco ANA Version 3.7.1*

Attribute	AS5800
IMO Name—IPIInterface	
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 ANA Version 3.7.1 (continued)

Attribute	AS5800
Type	Y
Routing Protocol Type	Y
Outgoing Interface Name	Y
IMO Name—IARPEntity	
ARP Table	Y
IMO Name—IARPEntity	
IP Address	Y
MAC Address	Y
Port	Y
Entry Type	Y
IMO Name—IIPPool	
IP Address Pool Entries	
Name	
Index	
IMO Name—IIPRangeBasedIIPPoolEntry	
Start IP Address	
End IP Address	
Unused Addresses	
Used Addresses	
Reserved Addresses	
IMO Name—IIPSubnetBasedIIPPoolEntry	
IP Subnet	
Unused Addresses	
Used Addresses	
Reserved Addresses	
IMO Name—HSRPGGroupEntry	
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 ANA Version 3.7.1 (continued)*

Attribute	AS5800
IMO Name—I Tunnel GRE	
Name	
Tunnel Destination and Source	
IP Address	
IP Interface State	
IANA Type	
Containing CTPs	
Contained CTPs	
Keep Alive Time	
Keep Alive Retry	
IMO Name—I IPSLA Responder Service	
responderStatus	
TWAMP Responder Status	
tcpConnect	
udpEcho	
IMO Name—I IP Address Port Pair	
type	
ipAddress	
port	

Routing Protocols

Table 4-6 Routing Protocols Attribute Support on Cisco Access Servers—Cisco ANA Version 3.7.1

Attribute	AS5800
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 ANA Version 3.7.1 (continued)

Attribute	AS5800
State	
Interface Address	
Type	
IF Priority	
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 ANA Version 3.7.1

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	

Table 4-7 Ethernet Attribute Support on Cisco Access Servers—Cisco ANA Version 3.7.1

Attribute	AS5800
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 4-7 Ethernet Attribute Support on Cisco Access Servers—Cisco ANA Version 3.7.1

Attribute	AS5800
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 4-7 Ethernet Attribute Support on Cisco Access Servers—Cisco ANA Version 3.7.1

Attribute	AS5800
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 4-7 Ethernet Attribute Support on Cisco Access Servers—Cisco ANA Version 3.7.1

Attribute	AS5800
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—IRESservice	
version	
administrativeVlan	
notificationEnabled	
IMO Name—IRESsegmentInfo	
segmentId	
segmentComplete	
IMO Name—IRESportInfo	
portName	
portKey	
segmentId	
portType	
portRole	
operStatus	
blockedVlans	
preemptTimer	
lslAgeoutTimer	
remoteDeviceName	

Table 4-7 Ethernet Attribute Support on Cisco Access Servers—Cisco ANA Version 3.7.1

Attribute	AS5800
remoteDeviceMac	
remotePortName	
IMO Name—IBridgeLan	
Id	
IMO Name—IIBridgeEntry	
IS Id	
IBridge	
BBridge	

TDM/DSx

Table 4-8 TDM/DSx Attribute Support on Cisco Access Servers—Cisco ANA Version 3.7.1

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	

Table 4-8 TDM/DSx Attribute Support on Cisco Access Servers—Cisco ANA Version 3.7.1

Attribute	AS5800
recoveredClockingId	
clocking	
loopback	
alarmState	Y
IMO Name—IClockService	
ActiveClockSource	
NcsMode	
HoldTimeout	
UseStratum4	
Mode	
NcsPriorityList	
PtpService	
IMO Name—IClockSource	
Priority	
Source	
Status	
Type	
IMO Name—IPtpService	
Mode	
ClockId	
Domain	
Priority1	
Priority2	
PtpEnabled	
PtpInterfaceList	
IMO Name—IPtpInterface	
Version	
AnnounceInterval	
AnnounceTimeout	
DestinationAddress	
SourceAddress	
DelayReq	
MasterMode	
SlaveMode	
SyncInterval	

Table 4-8 TDM/DSx Attribute Support on Cisco Access Servers—Cisco ANA Version 3.7.1

Attribute	AS5800
SyncLimit	
InterfaceXid	
IMO Name—IACRService	
RecoveredClockSource	
RecoveredClockMode	
CemInterface	
RecoveredClockList	
IMO Name—IRecoveredClock	
ClockId	
RecoveredClockMode	
Port	
Cem	
Status	
FrequencyOffset	
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 ANA Version 3.7.1

Attribute	AS5800
IMO Name—IISyncEInterface	
selectionInput	
ingressESMCMode	
egressESMCMode	
ingressQLMode	
ingressQuality	
egressQLMode	
egressQuality	
waitToRestore	
holdOffTimer	

Security

Table 4-9 Security Attribute Support on Cisco Access Servers—Cisco ANA Version 3.7.1

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	
Source and Destination Port Action	
Protocol Specific Info	
Differential Services Code Points	
Type of Service	

Table 4-9 Security Attribute Support on Cisco Access Servers—Cisco ANA Version 3.7.1

Attribute	AS5800
Precedence	
Matches	

Hardware

Table 4-10 Hardware Attribute Support on Cisco Access Servers—Cisco ANA Version 3.7.1

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	
Operational Status Last Changed	
Supported Physical Termination Points	

Table 4-10 Hardware Attribute Support on Cisco Access Servers—Cisco ANA Version 3.7.1

Attribute	AS5800
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	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	

Table 4-10 Hardware Attribute Support on Cisco Access Servers—Cisco ANA Version 3.7.1

Attribute	AS5800
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 ANA Version 3.7.1

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

Table 4-11 *Serial Attribute Support on Cisco Access Servers—Cisco ANA Version 3.7.1*

Attribute	AS5800
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 ANA Version 3.7.1. For more information about the objects and attributes described in this chapter, see Part 2: Technology Support and Information Model Objects.

This chapter contains the following topics:

- [Cisco AS5300 Series Universal Gateways, page 5-1](#)
- [Supported Technologies on Cisco Gateways, page 5-4](#)

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 ANA Version 3.7.1, see [Cisco AS5300 Series Universal Gateways](#)):

- [Cisco AS5300 Series—Supported Software Versions, page 5-2](#)
- [Cisco AS5300 Series—Supported Topologies, page 5-2](#)
- [Cisco AS5300 Series—Supported Modules, page 5-2](#)
- [Cisco AS5300 Series—Supported Technologies, page 5-3](#)
- [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 ANA Version 3.7.1

Software Version	ANA 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
12.3(3)	3.6.0

Cisco AS5300 Series—Supported Topologies

Table 5-2 Supported Topologies for Cisco AS5300 Series—Cisco ANA Version 3.7.1

Topology Type	Link Type	ANA 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 ANA Version 3.7.1

Module Name	ANA 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 ANA Version 3.7.1:

- [IP, page 5-4](#)
- [Ethernet, page 5-7](#)
- [Security, page 5-12](#)
- [Hardware, page 5-13](#)
- [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 ANA Version 3.7.1

Event Name	ANA 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 ANA Version 3.7.1 per technology:

- [IP, page 5-4](#)
- [Ethernet, page 5-7](#)
- [Security, page 5-12](#)
- [Hardware, page 5-13](#)
- [Serial, page 5-15](#)
- [CDP, page 5-16](#)
- [Discovery Protocol, page 5-16](#)

For information about IMO changes in Cisco ANA 3.7.1, please see <http://developer.cisco.com/web/ana/integration>.

IP

Table 5-5 *IP Attribute Support on Cisco Gateways—Cisco ANA Version 3.7.1*

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	

Table 5-5 IP Attribute Support on Cisco Gateways—Cisco ANA Version 3.7.1 (continued)

Attribute	AS5300
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
Type	Y
Routing Protocol Type	Y
Outgoing Interface Name	Y
IMO Name—IARPEntity	
ARP Table	Y
IMO Name—IARPEntity	
IP Address	Y
MAC Address	Y
Port	Y
Entry Type	Y
IMO Name—IIPPool	
IP Address Pool Entries	
Name	
Index	
IMO Name—IIPRangeBasedIIPPoolEntry	
Start IP Address	
End IP Address	
Unused Addresses	
Used Addresses	
Reserved Addresses	

Table 5-5 *IP Attribute Support on Cisco Gateways—Cisco ANA Version 3.7.1 (continued)*

Attribute	AS5300
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—ITunnelIGRE	
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 5-6 Ethernet Attribute Support on Cisco Gateways—Cisco ANA Version 3.7.1

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	

Table 5-6 Ethernet Attribute Support on Cisco Gateways—Cisco ANA Version 3.7.1 (continued)

Attribute	AS5300
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 5-6 Ethernet Attribute Support on Cisco Gateways—Cisco ANA Version 3.7.1 (continued)

Attribute	AS5300
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 5-6 Ethernet Attribute Support on Cisco Gateways—Cisco ANA Version 3.7.1 (continued)

Attribute	AS5300
StpBridgeMaxAge	
StpBridgeHelloTime	
StpBridgeForwardDelay	
StpProtocolSpecification	
StpVlanId	
StpForwardDelay	
StpMaxAge	
IMO Name—IStpInstanceInfo	
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 5-6 Ethernet Attribute Support on Cisco Gateways—Cisco ANA Version 3.7.1 (continued)

Attribute	AS5300
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	
IslAgeoutTimer	
remoteDeviceName	

Table 5-6 Ethernet Attribute Support on Cisco Gateways—Cisco ANA Version 3.7.1 (continued)

Attribute	AS5300
remoteDeviceMac	
remotePortName	
IMO Name—IBridgeLan	
Id	
IMO Name—IIBridgeEntry	
IS Id	
IBridge	
BBridge	

Security

Table 5-7 Security Attribute Support on Cisco Gateways—Cisco ANA Version 3.7.1

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 ANA Version 3.7.1*

Attribute	AS5300
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	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—IManagedElement	
IP Address	Y
Communication State	Y
Investigation State	Y
Element Category	Y

Table 5-8 Hardware Attribute Support on Cisco Gateways—Cisco ANA Version 3.7.1 (continued)

Attribute	AS5300
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	
Type	
MAC Address	
IP Interface	

Table 5-8 *Hardware Attribute Support on Cisco Gateways—Cisco ANA Version 3.7.1 (continued)*

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

Serial

Table 5-9 *Serial Attribute Support on Cisco Gateways—Cisco ANA Version 3.7.1*

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 ANA Version 3.7.1 (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 ANA Version 3.7.1

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 ANA Version 3.7.1

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 ANA Version 3.7.1. For more information about the objects and attributes described in this chapter, see Part 2: Technology Support and Information Model Objects.

This chapter contains the following topics:

- [Cisco 800 Series Routers, page 6-2](#)
- [Cisco 1000 Series Routers, page 6-5](#)
- [Cisco 1600 Series Routers, page 6-8](#)
- [Cisco 1700 Series Modular Access Routers, page 6-12](#)
- [Cisco 1800 Series Integrated Services Routers, page 6-17](#)
- [Cisco 2500 Series Routers, page 6-26](#)
- [Cisco 2600 Series Multiservice Platform Routers, page 6-30](#)
- [Cisco 2800 Series Integrated Services Routers, page 6-35](#)
- [Cisco 2900 Series Integrated Services Router, page 6-41](#)
- [Cisco 3600 Series Multiservice Platform Routers, page 6-45](#)
- [Cisco 3700 Series Multiservice Access Routers, page 6-54](#)
- [Cisco 3800 Series Integrated Services Routers, page 6-58](#)
- [Cisco 3900 Series Integrated Service Routers, page 6-63](#)
- [Cisco 4700 Series Routers, page 6-67](#)
- [Cisco 7200 Series Routers, page 6-70](#)
- [Cisco 7300 Series Routers, page 6-79](#)
- [Cisco 7400 Series Routers, page 6-84](#)
- [Cisco 7500 Series Routers, page 6-90](#)
- [Cisco 7600 Series Routers, page 6-94](#)
- [Cisco 10000 Series Routers, page 6-114](#)
- [Cisco 12000 Series Routers, page 6-119](#)
- [Cisco XR 12000 Series Routers, page 6-130](#)
- [Cisco CRS-1 Carrier Routing System, page 6-142](#)
- [Cisco ASR 1000 Series Routers, page 6-154](#)

- [Cisco ASR 9000 Series Aggregation Services Routers](#), page 6-160
- [Cisco MWR 2900 Series Mobile Wireless Routers](#), page 6-166
- [Cisco Universal Broadband Router 7200 Series](#), page 6-172
- [Cisco Universal Broadband Router 10000 Series](#), page 6-176
- [Supported Technologies on Cisco Routers](#), page 6-181

Cisco 800 Series Routers

This section includes the following information about Cisco 800 Series routers (for information on the NE types supported in Cisco ANA Version 3.7.1, see [Cisco 800 Series Routers](#)):

This section contains the following topics:

- [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 ANA Version 3.7.1*

Software Version	ANA 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 ANA Version 3.7.1*

Topology Type	Link Type	ANA Version
ATM	ATM	3.6.0
Ethernet	Ethernet	3.6.0
GRE Tunnel	GRE Tunnel	3.6.0
Physical Layer	Physical Layer	3.6.0

Cisco 800 Series—Supported Technologies

The following technologies are supported by the Cisco 800 Series in Cisco ANA Version 3.7.1:

- [IP, page 6-182](#)
- [Routing Protocols, page 6-185](#)
- [Ethernet, page 6-188](#)
- [ATM, page 6-197](#)
- [TDM/DSx, page 6-206](#)
- [VPN \(VRF\), page 6-215](#)
- [Security, page 6-218](#)
- [Hardware, page 6-220](#)
- [Serial, page 6-223](#)
- [Additional Technologies, page 6-224](#)
- [LocalSwitching, page 6-226](#)
- [CDP, page 6-230](#)
- [Discovery Protocol, page 6-230](#)

Cisco 800 Series—Supported Service Events

Table 6-3 *Supported Service Events for Cisco 800 Series—Cisco ANA Version 3.7.1*

Event Name	ANA 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
Device Unreachable	3.6.1	N
Device Unsupported	3.6.1	N
Interface status down flapping	3.6.1	Y
Interface status down flapping update	3.6.1	Y
Link Down	3.6.1	N
Link up	3.6.1	N
Module Unsupported	3.6.1	N
Port Down	3.6.1	N
Port Flapping	3.6.1	N

Table 6-3 **Supported Service Events for Cisco 800 Series—Cisco ANA Version 3.7.1 (continued)**

Event Name	ANA Version	Expedited
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
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 down	3.7.1	N
EFP up	3.7.1	N
Primary HSRP interface is active	3.7.1	N
Primary HSRP interface is not active	3.7.1	N
Secondary HSRP interface is active	3.7.1	N
Secondary HSRP interface is 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 down	3.7.1	N
LAG Link 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

Table 6-3 Supported Service Events for Cisco 800 Series—Cisco ANA Version 3.7.1 (continued)

Event Name	ANA Version	Expedited
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
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 1000 Series Routers

This section includes the following information about Cisco 1000 Series routers (for information on the NE types supported in Cisco ANA Version 3.7.1, see [Cisco 1000 Series Routers](#)):

This section contains the following topics:

- [Cisco 1000 Series—Supported Software Versions](#), page 6-5
- [Cisco 1000 Series—Supported Topologies](#), page 6-6
- [Cisco 1000 Series—Supported Technologies](#), page 6-6
- [Cisco 1000 Series—Supported Service Events](#), page 6-6

Cisco 1000 Series—Supported Software Versions

Table 6-4 Supported Software Versions for Cisco 1000 Series—Cisco ANA Version 3.7.1

Software Version	ANA 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 ANA Version 3.7.1*

Topology Type	Link Type	ANA 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 ANA Version 3.7.1:

- [IP, page 6-182](#)
- [Routing Protocols, page 6-185](#)
- [Ethernet, page 6-188](#)
- [ATM, page 6-197](#)
- [Frame Relay, page 6-200](#)
- [PPP, page 6-202](#)
- [HDLC, page 6-204](#)
- [SONET/SDH, page 6-204](#)
- [TDM/DSx, page 6-206](#)
- [Security, page 6-218](#)
- [Hardware, page 6-220](#)
- [Serial, page 6-223](#)
- [Additional Technologies, page 6-224](#)
- [LocalSwitching, page 6-226](#)
- [CDP, page 6-230](#)
- [Discovery Protocol, page 6-230](#)

Cisco 1000 Series—Supported Service Events

Table 6-6 *Supported Service Events for Cisco 1000 Series—Cisco ANA Version 3.7.1*

Event Name	ANA Version	Expedited
Active IP Interfaces Found	3.6.1	Y

Table 6-6 *Supported Service Events for Cisco 1000 Series—Cisco ANA Version 3.7.1 (continued)*

Event Name	ANA Version	Expedited
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
Cloud Problem	3.6.1	N
CPU utilization exceeded upper threshold	3.6.1	N
Device Unreachable	3.6.1	N
Device Unsupported	3.6.1	N
Interface status down flapping	3.6.1	Y
Interface status down flapping update	3.6.1	Y
Keepalive configured	3.6.1	N
Keepalive not configured	3.6.1	N
Layer 2 Tunnel Down	3.6.1	N
Link 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
Port Down	3.6.1	N
Port Flapping	3.6.1	N
Rx utilization exceeded upper threshold	3.6.1	N
Tx utilization exceeded upper threshold	3.6.1	N
VPN Leak	3.6.1	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

Table 6-6 *Supported Service Events for Cisco 1000 Series—Cisco ANA Version 3.7.1 (continued)*

Event Name	ANA Version	Expedited
DS3 Path up	3.7.1	N
EFP down	3.7.1	N
EFP down	3.7.1	N
EFP up	3.7.1	N
Interface status up	3.7.1	N
LAG down	3.7.1	N
LAG down	3.7.1	N
LAG Link 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
MPLS-TE tunnel down	3.7.1	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 down	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 1600 Series Routers

This section includes the following information about Cisco 1600 Series routers (for information on the NE types supported in Cisco ANA Version 3.7.1, see [Cisco 1600 Series Routers](#)):

This section contains the following topics:

- [Cisco 1600 Series—Supported Software Versions, page 6-9](#)
- [Cisco 1600 Series—Supported Topologies, page 6-9](#)
- [Cisco 1600 Series—Supported Technologies, page 6-9](#)
- [Cisco 1600 Series—Supported Service Events, page 6-10](#)

Cisco 1600 Series—Supported Software Versions

Table 6-7 Supported Software Versions for Cisco 1600 Series—Cisco ANA Version 3.7.1

Software Version	ANA Version
12.0(12)	3.6.1

Cisco 1600 Series—Supported Topologies

Table 6-8 Supported Topologies for Cisco 1600 Series—Cisco ANA Version 3.7.1

Topology Type	Link Type	ANA 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 ANA Version 3.7.1:

- [IP, page 6-182](#)
- [Routing Protocols, page 6-185](#)
- [Ethernet, page 6-188](#)
- [ATM, page 6-197](#)
- [Frame Relay, page 6-200](#)
- [PPP, page 6-202](#)
- [HDLC, page 6-204](#)
- [SONET/SDH, page 6-204](#)
- [TDM/DSx, page 6-206](#)
- [Security, page 6-218](#)
- [Hardware, page 6-220](#)
- [Serial, page 6-223](#)
- [LocalSwitching, page 6-226](#)
- [CDP, page 6-230](#)
- [Discovery Protocol, page 6-230](#)

Cisco 1600 Series—Supported Service Events

Table 6-9 *Supported Service Events for Cisco 1600 Series—Cisco ANA Version 3.7.1*

Event Name	ANA 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
Cloud Problem	3.6.1	N
CPU utilization exceeded upper threshold	3.6.1	N
Device Unreachable	3.6.1	N
Device Unsupported	3.6.1	N
Interface status down flapping	3.6.1	Y
Interface status down flapping update	3.6.1	Y
Keepalive configured	3.6.1	N
Keepalive not configured	3.6.1	N
Layer 2 Tunnel Down	3.6.1	N
Link 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
Port Down	3.6.1	N
Port Flapping	3.6.1	N
Rx utilization exceeded upper threshold	3.6.1	N
Tx utilization exceeded upper threshold	3.6.1	N
VPN Leak	3.6.1	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

Table 6-9 **Supported Service Events for Cisco 1600 Series—Cisco ANA Version 3.7.1 (continued)**

Event Name	ANA 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 down	3.7.1	N
EFP up	3.7.1	N
Primary HSRP interface is active	3.7.1	N
Primary HSRP interface is not active	3.7.1	N
Secondary HSRP interface is active	3.7.1	N
Secondary HSRP interface is 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 down	3.7.1	N
LAG Link 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

Table 6-9 Supported Service Events for Cisco 1600 Series—Cisco ANA Version 3.7.1 (continued)

Event Name	ANA Version	Expedited
OSPF Neighbor Up	3.7.1	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 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 ANA Version 3.7.1, see [Cisco 1700 Series Modular Access Routers](#)):

This section contains the following topics:

- [Cisco 1700 Series—Supported Software Versions, page 6-12](#)
- [Cisco 1700 Series—Supported Topologies, page 6-13](#)
- [Cisco 1700 Series—Supported Modules, page 6-13](#)
- [Cisco 1700 Series—Supported Technologies, page 6-14](#)
- [Cisco 1700 Series—Supported Service Events, page 6-14](#)

Cisco 1700 Series—Supported Software Versions

Table 6-10 Supported Software Versions for Cisco 1700 Series—Cisco ANA Version 3.7.1

Software Version	ANA 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 ANA Version 3.7.1

Topology Type	Link Type	ANA 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 ANA Version 3.7.1

Module Name	ANA 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 Multiflex 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
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

Table 6-12 *Supported Modules for Cisco 1700 Series—Cisco ANA Version 3.7.1 (continued)*

Module Name	ANA Version	Module Description
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 ANA Version 3.7.1:

- [IP, page 6-182](#)
- [Routing Protocols, page 6-185](#)
- [Ethernet, page 6-188](#)
- [ATM, page 6-197](#)
- [Frame Relay, page 6-200](#)
- [PPP, page 6-202](#)
- [HDLC, page 6-204](#)
- [SONET/SDH, page 6-204](#)
- [TDM/DSx, page 6-206](#)
- [Security, page 6-218](#)
- [Hardware, page 6-220](#)
- [Serial, page 6-223](#)
- [Additional Technologies, page 6-224](#)
- [LocalSwitching, page 6-226](#)
- [BFD, page 6-227](#)
- [CDP, page 6-230](#)
- [Discovery Protocol, page 6-230](#)

Cisco 1700 Series—Supported Service Events

Table 6-13 *Supported Service Events for Cisco 1700 Series—Cisco ANA Version 3.7.1*

Event Name	ANA 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

Table 6-13 **Supported Service Events for Cisco 1700 Series—Cisco ANA Version 3.7.1 (continued)**

Event Name	ANA Version	Expedited
Card In	3.6.1	Y
Card Out	3.6.1	Y
Card Up	3.6.1	Y
Cloud Problem	3.6.1	N
CPU utilization exceeded upper threshold	3.6.1	N
Device Unreachable	3.6.1	N
Device Unsupported	3.6.1	N
Interface status down flapping	3.6.1	Y
Interface status down flapping update	3.6.1	Y
Keepalive configured	3.6.1	N
Keepalive not configured	3.6.1	N
Layer 2 Tunnel Down	3.6.1	N
Link 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
Port Down	3.6.1	N
Port Flapping	3.6.1	N
Rx utilization exceeded upper threshold	3.6.1	N
Tx utilization exceeded upper threshold	3.6.1	N
VPN Leak	3.6.1	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
Device Managed	3.7.1	N

Table 6-13 **Supported Service Events for Cisco 1700 Series—Cisco ANA Version 3.7.1 (continued)**

Event Name	ANA Version	Expedited
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 down	3.7.1	N
EFP up	3.7.1	N
Primary HSRP interface is active	3.7.1	N
Primary HSRP interface is not active	3.7.1	N
Secondary HSRP interface is active	3.7.1	N
Secondary HSRP interface is 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 down	3.7.1	N
LAG Link 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
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

Table 6-13 Supported Service Events for Cisco 1700 Series—Cisco ANA Version 3.7.1 (continued)

Event Name	ANA Version	Expedited
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 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 ANA Version 3.7.1, see [Cisco 1800 Series Integrated Services Routers](#)):

This section contains the following topics:

- [Cisco 1800 Series—Supported Software Versions, page 6-17](#)
- [Cisco 1800 Series—Supported Topologies, page 6-18](#)
- [Cisco 1800 Series—Supported Modules, page 6-18](#)
- [Cisco 1800 Series—Supported Technologies, page 6-19](#)
- [Cisco 1800 Series—Supported Service Events, page 6-19](#)

Cisco 1800 Series—Supported Software Versions

Table 6-14 Supported Software Versions for Cisco 1800 Series—Cisco ANA Version 3.7.1

Software Version	ANA 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 ANA Version 3.7.1

Topology Type	Link Type	ANA Version
ATM	ATM	3.6.0
BGP	BGP	3.6.0
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 ANA Version 3.7.1

Module Name	ANA 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 ANA Version 3.7.1:

- [IP, page 6-182](#)
- [Routing Protocols, page 6-185](#)
- [Ethernet, page 6-188](#)
- [ATM, page 6-197](#)
- [Frame Relay, page 6-200](#)
- [PPP, page 6-202](#)
- [HDLC, page 6-204](#)
- [SONET/SDH, page 6-204](#)
- [TDM/DSx, page 6-206](#)
- [VPN \(VRF\), page 6-215](#)
- [Security, page 6-218](#)
- [Hardware, page 6-220](#)
- [Serial, page 6-223](#)
- [Additional Technologies, page 6-224](#)
- [LocalSwitching, page 6-226](#)
- [CDP, page 6-230](#)
- [Discovery Protocol, page 6-230](#)

Cisco 1800 Series—Supported Service Events

Table 6-17 *Supported Service Events for Cisco 1800 Series—Cisco ANA Version 3.7.1*

Event Name	ANA Version	Expedited
All IP Interfaces Down / Active IP Interfaces Found	3.6.0	Y
BGP Neighbor Down	3.6.0	Y
Card In/Out	3.6.0	Y
Card Up/Down	3.6.0	Y
Cloud Problem	3.6.0	N
CPU Over Utilized	3.6.0	Y
Device Unreachable	3.6.0	Y
Device Unsupported	3.6.0	Y
Discard Packets	3.6.0	N
Dropped Packets	3.6.0	N
Interface Status Down/Up	3.6.0	Y

Table 6-17 **Supported Service Events for Cisco 1800 Series—Cisco ANA Version 3.7.1 (continued)**

Event Name	ANA Version	Expedited
Link Down/Up	3.6.0	Y
Memory Over Utilized	3.6.0	Y
Module Unsupported	3.6.0	N
Port Down	3.6.0	Y
Port Flapping	3.6.0	N
Primary HSRP Interface Active/Inactive	3.6.0	Y
Rx Over Utilized	3.6.0	N
Secondary HSRP Interface Active/Inactive	3.6.0	Y
Tx Over Utilized	3.6.0	N
VPN Leak	3.6.0	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
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
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
LDP neighbor down	3.7.1	N
LDP neighbor up	3.7.1	N
MPLS Black hole cleared	3.7.1	N
MPLS Black hole found	3.7.1	N
MPLS TE FRR State Changed to Active	3.7.1	N

Table 6-17 **Supported Service Events for Cisco 1800 Series—Cisco ANA Version 3.7.1 (continued)**

Event Name	ANA Version	Expedited
MPLS TE FRR State Changed to Ready	3.7.1	N
MPLS interface added	3.7.1	N
MPLS interface removed	3.7.1	N
Active ip interfaces found	3.7.1	N
All ip interfaces down	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 up	3.7.1	N
Card in	3.7.1	N
Card out	3.7.1	N
cgn statistics dropsPortLimitIn2Out higher threshold exceeded	3.7.1	N
cgn statistics dropsPortLimitIn2Out lower threshold exceeded	3.7.1	N
cgn statistics dropsPortLimitIn2Out threshold normal	3.7.1	N
cgn statistics dropsResourceDepletionIn2Out higher threshold exceeded	3.7.1	N
cgn statistics dropsResourceDepletionIn2Out lower threshold exceeded	3.7.1	N
cgn statistics dropsResourceDepletionIn2Out threshold normal	3.7.1	N
cgn statistics dropsSystemLimitIn2Out higher threshold exceeded	3.7.1	N
cgn statistics dropsSystemLimitIn2Out lower threshold exceeded	3.7.1	N
cgn statistics dropsSystemLimitIn2Out threshold normal	3.7.1	N
cgn statistics fwdIn2Out higher threshold exceeded	3.7.1	N
cgn statistics fwdIn2Out lower threshold exceeded	3.7.1	N

Table 6-17 **Supported Service Events for Cisco 1800 Series—Cisco ANA Version 3.7.1 (continued)**

Event Name	ANA Version	Expedited
cgn statistics fwdIn2Out threshold normal	3.7.1	N
cgn statistics fwdOut2In higher threshold exceeded	3.7.1	N
cgn statistics fwdOut2In lower threshold exceeded	3.7.1	N
cgn statistics fwdOut2In threshold normal	3.7.1	N
cgn statistics translationsCreate higher threshold exceeded	3.7.1	N
cgn statistics translationsCreate lower threshold exceeded	3.7.1	N
cgn statistics translationsCreate threshold normal	3.7.1	N
cgn statistics translationsDelete higher threshold exceeded	3.7.1	N
cgn statistics translationsDelete lower threshold exceeded	3.7.1	N
cgn statistics translationsDelete threshold normal	3.7.1	N
Device Managed	3.7.1	N
Management Unreachable	3.7.1	N
Device Partially Managed	3.7.1	N
CPU utilization less than lower threshold	3.7.1	N
CPU utilization exceeded upper threshold	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 Link down due to Card event	3.7.1	N
DS1 Path Link down on unreachable	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 6-17 **Supported Service Events for Cisco 1800 Series—Cisco ANA Version 3.7.1 (continued)**

Event Name	ANA Version	Expedited
DS1 Path down due to Oper	3.7.1	N
DS1 Path up	3.7.1	N
DS3 Path Link down due to admin down	3.7.1	N
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 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
dwdm controller down	3.7.1	N
dwdm controller up	3.7.1	N
dwdm g709 status down	3.7.1	N
dwdm g709 status up	3.7.1	N
EFP down	3.7.1	N
EFP down	3.7.1	N
EFP up	3.7.1	N
Primary HSRP interface is active	3.7.1	N
Primary HSRP interface is not active	3.7.1	N
Secondary HSRP interface is active	3.7.1	N
Secondary HSRP interface is not active	3.7.1	N
ima administratively down	3.7.1	N
ima administratively up	3.7.1	N
ima operationally down	3.7.1	N
ima operationally up	3.7.1	N
Interface status down	3.7.1	N
Interface status up	3.7.1	N
keepalive not configured	3.7.1	N
keepalive 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

Table 6-17 **Supported Service Events for Cisco 1800 Series—Cisco ANA Version 3.7.1 (continued)**

Event Name	ANA Version	Expedited
LAG down	3.7.1	N
LAG down	3.7.1	N
LAG up	3.7.1	N
LAG Link down	3.7.1	N
LAG Link down	3.7.1	N
LAG Link up	3.7.1	N
Layer 2 tunnel 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 up	3.7.1	N
Link over utilized	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
Memory utilization less than lower threshold	3.7.1	N
Memory utilization exceeded upper threshold	3.7.1	N
mlppp administratively down	3.7.1	N
mlppp operationally down	3.7.1	N
High Priority MPLS-TE tunnel down	3.7.1	N
Low Priority MPLS-TE tunnel down	3.7.1	N
Medium Priority MPLS-TE tunnel down	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 out	3.7.1	N
Port down due to Card down	3.7.1	N
Port down due to oper	3.7.1	N

Table 6-17 **Supported Service Events for Cisco 1800 Series—Cisco ANA Version 3.7.1 (continued)**

Event Name	ANA Version	Expedited
Port up	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
Shelf in	3.7.1	N
Shelf out	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 down due to Admin	3.7.1	N
SONET Path down due to Card	3.7.1	N
SONET Path down due to Oper	3.7.1	N
SONET Path up	3.7.1	N
VLAN Sub Interface down	3.7.1	N
VLAN Sub Interface down	3.7.1	N
VLAN Sub Interface up	3.7.1	N
Service down	3.7.1	N
Service 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
VSI down	3.7.1	N
VSI down	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 2500 Series Routers

This section includes the following information about Cisco 2500 Series routers (for information on the NE types supported in Cisco ANA Version 3.7.1, see [Cisco 2500 Series Routers](#)):

This section contains the following topics:

- [Cisco 2500 Series—Supported Software Versions, page 6-26](#)
- [Cisco 2500 Series—Supported Topologies, page 6-26](#)
- [Cisco 2500 Series—Supported Modules, page 6-26](#)
- [Cisco 2500 Series—Supported Technologies, page 6-27](#)
- [Cisco 2500 Series—Supported Service Events, page 6-27](#)

Cisco 2500 Series—Supported Software Versions

Table 6-18 Supported Software Versions for Cisco 2500 Series—Cisco ANA Version 3.7.1

Software Version	ANA 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 ANA Version 3.7.1

Topology Type	Link Type	ANA 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 ANA Version 3.7.1

Module Name	ANA 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 ANA Version 3.7.1:

- [IP, page 6-182](#)
- [Routing Protocols, page 6-185](#)
- [Ethernet, page 6-188](#)
- [ATM, page 6-197](#)
- [Frame Relay, page 6-200](#)
- [SONET/SDH, page 6-204](#)
- [TDM/DSx, page 6-206](#)
- [MPLS, page 6-210](#)
- [VPN \(VRF\), page 6-215](#)
- [Security, page 6-218](#)
- [Hardware, page 6-220](#)
- [Serial, page 6-223](#)
- [Additional Technologies, page 6-224](#)
- [LocalSwitching, page 6-226](#)
- [CDP, page 6-230](#)
- [Discovery Protocol, page 6-230](#)

Cisco 2500 Series—Supported Service Events

Table 6-21 *Supported Service Events for Cisco 2500 Series—Cisco ANA Version 3.7.1*

Event Name	ANA 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
Device Unreachable	3.6.0	N
Device Unsupported	3.6.0	N
Interface status down flapping	3.6.0	Y

Table 6-21 *Supported Service Events for Cisco 2500 Series—Cisco ANA Version 3.7.1 (continued)*

Event Name	ANA Version	Expedited
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
Module Unsupported	3.6.0	N
MPLS Black Hole found	3.6.0	N
Port Down	3.6.0	N
Port Flapping	3.6.0	N
Rx utilization exceeded upper threshold	3.6.0	N
Tx utilization exceeded upper threshold	3.6.0	N
VPN Leak	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
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

Table 6-21 **Supported Service Events for Cisco 2500 Series—Cisco ANA Version 3.7.1 (continued)**

Event Name	ANA Version	Expedited
EFP down	3.7.1	N
EFP up	3.7.1	N
Primary HSRP interface is active	3.7.1	N
Primary HSRP interface is not active	3.7.1	N
Secondary HSRP interface is active	3.7.1	N
Secondary HSRP interface is not active	3.7.1	N
ima operationaly 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 down	3.7.1	N
LAG Link 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 administatively 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
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 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 ANA Version 3.7.1, see [Cisco 2600 Series Multiservice Platform Routers](#)):

This section contains the following topics:

- [Cisco 2600 Series—Supported Software Versions, page 6-30](#)
- [Cisco 2600 Series—Supported Topologies, page 6-30](#)
- [Cisco 2600 Series—Supported Modules, page 6-31](#)
- [Cisco 2600 Series—Supported Technologies, page 6-32](#)
- [Cisco 2600 Series—Supported Service Events, page 6-32](#)

Cisco 2600 Series—Supported Software Versions

Table 6-22 *Supported Software Versions for Cisco 2600 Series—Cisco ANA Version 3.7.1*

Software Version	ANA 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 ANA Version 3.7.1*

Topology Type	Link Type	ANA 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 ANA Version 3.7.1*

Module Name	ANA 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
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

Table 6-24 Supported Modules for Cisco 2600 Series—Cisco ANA Version 3.7.1 (continued)

Module Name	ANA Version	Module Description
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 ANA Version 3.7.1:

- [IP, page 6-182](#)
- [Routing Protocols, page 6-185](#)
- [Ethernet, page 6-188](#)
- [ATM, page 6-197](#)
- [Frame Relay, page 6-200](#)
- [PPP, page 6-202](#)
- [HDLC, page 6-204](#)
- [SONET/SDH, page 6-204](#)
- [TDM/DSx, page 6-206](#)
- [VPN \(VRF\), page 6-215](#)
- [Security, page 6-218](#)
- [Hardware, page 6-220](#)
- [Serial, page 6-223](#)
- [Additional Technologies, page 6-224](#)
- [LocalSwitching, page 6-226](#)
- [CDP, page 6-230](#)
- [Discovery Protocol, page 6-230](#)

Cisco 2600 Series—Supported Service Events

Table 6-25 Supported Service Events for Cisco 2600 Series—Cisco ANA Version 3.7.1

Event Name	ANA 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

Table 6-25 *Supported Service Events for Cisco 2600 Series—Cisco ANA Version 3.7.1 (continued)*

Event Name	ANA Version	Expedited
Card Out	3.6.1	Y
Card Up	3.6.1	Y
Cloud Problem	3.6.1	N
CPU utilization exceeded upper threshold	3.6.1	N
Device Unreachable	3.6.1	N
Device Unsupported	3.6.1	N
Interface status down flapping	3.6.1	Y
Interface status down flapping update	3.6.1	Y
Keepalive configured	3.6.1	N
Keepalive not configured	3.6.1	N
Layer 2 Tunnel Down	3.6.1	N
Link 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
Port Down	3.6.1	N
Port Flapping	3.6.1	N
Rx utilization exceeded upper threshold	3.6.1	N
Tx utilization exceeded upper threshold	3.6.1	N
VPN Leak	3.6.1	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
Device Managed	3.7.1	N
Management Unreachable	3.7.1	N

Table 6-25 *Supported Service Events for Cisco 2600 Series—Cisco ANA Version 3.7.1 (continued)*

Event Name	ANA Version	Expedited
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 down	3.7.1	N
EFP up	3.7.1	N
Primary HSRP interface is active	3.7.1	N
Primary HSRP interface is not active	3.7.1	N
Secondary HSRP interface is active	3.7.1	N
Secondary HSRP interface is 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 down	3.7.1	N
LAG Link 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
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

Table 6-25 Supported Service Events for Cisco 2600 Series—Cisco ANA Version 3.7.1 (continued)

Event Name	ANA Version	Expedited
Low priority member down	3.7.1	N
Medium priority member down	3.7.1	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 ANA Version 3.7.1, see [Cisco 2800 Series Integrated Services Routers](#)):

This section contains the following topics:

- [Cisco 2800 Series—Supported Software Versions](#), page 6-35
- [Cisco 2800 Series—Supported Topologies](#), page 6-36
- [Cisco 2800 Series—Supported Modules](#), page 6-36
- [Cisco 2800 Series—Supported Technologies](#), page 6-38
- [Cisco 2800 Series—Supported Service Events](#), page 6-39

Cisco 2800 Series—Supported Software Versions

Table 6-26 Supported Software Versions for Cisco 2800 Series—Cisco ANA Version 3.7.1

Software Version	ANA 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

Table 6-26 Supported Software Versions for Cisco 2800 Series—Cisco ANA Version 3.7.1

Software Version	ANA Version
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
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.

³Support 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 ANA Version 3.7.1

Topology Type	Link Type	ANA 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 ANA Version 3.7.1

Module Name	ANA 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

Table 6-28 Supported Modules for Cisco 2800 Series—Cisco ANA Version 3.7.1 (continued)

Module Name	ANA Version	Module Description
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
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

Table 6-28 **Supported Modules for Cisco 2800 Series—Cisco ANA Version 3.7.1 (continued)**

Module Name	ANA Version	Module Description
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
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 ANA Version 3.7.1:

- [IP, page 6-182](#)
- [Routing Protocols, page 6-185](#)
- [Ethernet, page 6-188](#)
- [ATM, page 6-197](#)
- [Frame Relay, page 6-200](#)
- [PPP, page 6-202](#)

- [HDLC, page 6-204](#)
- [SONET/SDH, page 6-204](#)
- [TDM/DSx, page 6-206](#)
- [VPN \(VRF\), page 6-215](#)
- [Security, page 6-218](#)
- [Hardware, page 6-220](#)
- [Serial, page 6-223](#)
- [Additional Technologies, page 6-224](#)
- [LocalSwitching, page 6-226](#)

Cisco 2800 Series—Supported Service Events

Table 6-29 *Supported Service Events for Cisco 2800 Series—Cisco ANA Version 3.7.1*

Event Name	ANA 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
Cloud Problem	3.6.1	N
CPU utilization exceeded upper threshold	3.6.1	N
Device Unreachable	3.6.1	N
Device Unsupported	3.6.1	N
Interface status down flapping	3.6.1	Y
Interface status down flapping update	3.6.1	Y
Keepalive configured	3.6.1	N
Keepalive not configured	3.6.1	N
Layer 2 Tunnel Down	3.6.1	N
Link 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

Table 6-29 **Supported Service Events for Cisco 2800 Series—Cisco ANA Version 3.7.1 (continued)**

Event Name	ANA Version	Expedited
Port Down	3.6.1	N
Port Flapping	3.6.1	N
Rx utilization exceeded upper threshold	3.6.1	N
Tx utilization exceeded upper threshold	3.6.1	N
VPN Leak	3.6.1	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
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 down	3.7.1	N
EFP up	3.7.1	N
Primary HSRP interface is active	3.7.1	N
Primary HSRP interface is not active	3.7.1	N
Secondary HSRP interface is active	3.7.1	N
Secondary HSRP interface is 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

Table 6-29 **Supported Service Events for Cisco 2800 Series—Cisco ANA Version 3.7.1 (continued)**

Event Name	ANA Version	Expedited
LAG down	3.7.1	N
LAG down	3.7.1	N
LAG Link 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
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 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 ANA Version 3.7.1, see [Cisco 2900 Series Integrated Services Router](#)):

This section contains the following topics:

- [Cisco ISR 2900 Series—Supported Software Versions, page 6-42](#)
- [Cisco ISR 2900 Series—Supported Topologies, page 6-42](#)
- [Cisco ISR 2900 Series—Supported Modules, page 6-42](#)
- [Cisco ISR 2900 Series—Supported Technologies, page 6-42](#)
- [Cisco ISR 2900 Series—Supported Service Events, page 6-43](#)

Cisco ISR 2900 Series—Supported Software Versions

Table 6-30 Supported Software Versions for Cisco ISR 2900 Series—Cisco ANA Version 3.7.1

Software Version	ANA Version
IOS 15.1(1)T	3.7.1

Cisco ISR 2900 Series—Supported Topologies

Table 6-31 Supported Topologies for Cisco ISR 2900 Series—Cisco ANA Version 3.7.1

Topology Type	Link Type	ANA 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 6-32 Supported Modules for Cisco ISR 2900 Series—Cisco ANA Version 3.7.1

Module Name	ANA 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
NM-16ESW-1GIG	3.7.1	16-port 10/100 EtherSwitch Network Module with 1 GbE (1000BASE-T) Port

Cisco ISR 2900 Series—Supported Technologies

The following technologies are supported by the Cisco ISR 2900 Series in Cisco ANA Version 3.7.1:

- [IP, page 6-182](#)
- [Routing Protocols, page 6-185](#)
- [Ethernet, page 6-188](#)

- [Security, page 6-218](#)
- [Hardware, page 6-220](#)
- [BFD, page 6-227](#)
- [Carrier Ethernet, page 6-228](#)
- [CDP, page 6-230](#)
- [Discovery Protocol, page 6-230](#)
- [Ethernet OAM, page 6-231](#)

Cisco ISR 2900 Series—Supported Service Events

Table 6-33 *Supported Service Events for Cisco ISR 2900 Series—Cisco ANA Version 3.7.1*

Event Name	ANA 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
Interface status down flapping	3.7.1	Y
Interface status down flapping update	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 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
Port Down	3.7.1	N
Port Flapping	3.7.1	N
Rx utilization exceeded upper threshold	3.7.1	N

Table 6-33 **Supported Service Events for Cisco ISR 2900 Series—Cisco ANA Version 3.7.1**

Event Name	ANA Version	Expedited
SONET Path up	3.7	N
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
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
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 down	3.7.1	N
EFP up	3.7.1	N
Primary HSRP interface is active	3.7.1	N
Primary HSRP interface is not active	3.7.1	N
Secondary HSRP interface is active	3.7.1	N
Secondary HSRP interface is not active	3.7.1	N
ima operationaly 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

Table 6-33 **Supported Service Events for Cisco ISR 2900 Series—Cisco ANA Version 3.7.1**

Event Name	ANA Version	Expedited
LAG down	3.7.1	N
LAG Link 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
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 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 ANA Version 3.7.1, see [Cisco 3600 Series Multiservice Platform Routers](#)):

This section contains the following topics:

- [Cisco 3600 Series—Supported Software Versions, page 6-46](#)
- [Cisco 3600 Series—Supported Topologies, page 6-46](#)
- [Cisco 3600 Series—Supported Modules, page 6-46](#)
- [Cisco 3600 Series—Supported Technologies, page 6-47](#)
- [Cisco 3600 Series—Supported Service Events, page 6-47](#)

Cisco 3600 Series—Supported Software Versions

Table 6-34 Supported Software Versions for Cisco 3600 Series—Cisco ANA Version 3.7.1

Software Version	ANA 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 6-35 Supported Topologies for Cisco 3600 Series—Cisco ANA Version 3.7.1

Topology Type	Link Type	ANA Version
Ethernet	Ethernet	3.6.0
Physical Layer	Physical Layer	3.6.0

Cisco 3600 Series—Supported Modules

Table 6-36 Supported Modules for Cisco 3600 Series—Cisco ANA Version 3.7.1

Module Name	ANA 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 ANA Version 3.7.1:

- [IP, page 6-182](#)
- [Routing Protocols, page 6-185](#)
- [Ethernet, page 6-188](#)
- [ATM, page 6-197](#)
- [Frame Relay, page 6-200](#)
- [PPP, page 6-202](#)
- [SONET/SDH, page 6-204](#)
- [TDM/DSx, page 6-206](#)
- [MPLS, page 6-210](#)
- [MPLS-TE, page 6-212](#)
- [VPN \(VRF\), page 6-215](#)
- [PWE3, page 6-217](#)
- [Security, page 6-218](#)
- [Hardware, page 6-220](#)
- [Serial, page 6-223](#)
- [Additional Technologies, page 6-224](#)
- [LocalSwitching, page 6-226](#)
- [CDP, page 6-230](#)
- [Discovery Protocol, page 6-230](#)

Cisco 3600 Series—Supported Service Events

Table 6-37 *Supported Service Events for Cisco 3600 Series—Cisco ANA Version 3.7.1*

Event Name	ANA Version	Expedited
All IP Interfaces Down / Active IP Interfaces Found	3.6.0	Y
BGP Neighbor Down	3.6.0	N
Broken LSP Discovered	3.6.0	N
Card In/Out	3.6.0	Y
Card Up/Down	3.6.0	Y
Cloud Problem	3.6.0	N
CPU Over Utilized	3.6.0	N
Device Unreachable	3.6.0	N
Device Unsupported	3.6.0	N

Table 6-37 **Supported Service Events for Cisco 3600 Series—Cisco ANA Version 3.7.1 (continued)**

Event Name	ANA Version	Expedited
Discard Packets	3.6.0	N
Dropped Packets	3.6.0	N
Interface Status Down/Up	3.6.0	Y
Layer 2 Tunnel Down	3.6.0	N
Link Down/Up	3.6.0	Y
Memory Over Utilized	3.6.0	N
Module Unsupported	3.6.0	N
MPLS Black Hole	3.6.0	N
MPLS TE Tunnel Down/Flapping	3.6.0	N
Port Down	3.6.0	Y
Port Flapping	3.6.0	N
Primary HSRP Interface Active/Inactive	3.6.0	N
Rx Over Utilized	3.6.0	N
Secondary HSRP Interface Active/Inactive	3.6.0	N
Tx Over Utilized	3.6.0	N
VPN Leak	3.6.0	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
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
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

Table 6-37 **Supported Service Events for Cisco 3600 Series—Cisco ANA Version 3.7.1 (continued)**

Event Name	ANA Version	Expedited
LDP neighbor down	3.7.1	N
LDP neighbor up	3.7.1	N
MPLS Black hole cleared	3.7.1	N
MPLS Black hole found	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 interface added	3.7.1	N
MPLS interface removed	3.7.1	N
Active ip interfaces found	3.7.1	N
All ip interfaces down	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 up	3.7.1	N
Card in	3.7.1	N
Card out	3.7.1	N
cgn statistics dropsPortLimitIn2Out higher threshold exceeded	3.7.1	N
cgn statistics dropsPortLimitIn2Out lower threshold exceeded	3.7.1	N
cgn statistics dropsPortLimitIn2Out threshold normal	3.7.1	N
cgn statistics dropsResourceDepletionIn2Out lower threshold exceeded	3.7.1	N
cgn statistics dropsResourceDepletionIn2Out threshold normal	3.7.1	N
cgn statistics dropsSystemLimitIn2Out higher threshold exceeded	3.7.1	N
cgn statistics dropsSystemLimitIn2Out lower threshold exceeded	3.7.1	N
cgn statistics dropsSystemLimitIn2Out threshold normal	3.7.1	N

Table 6-37 **Supported Service Events for Cisco 3600 Series—Cisco ANA Version 3.7.1 (continued)**

Event Name	ANA Version	Expedited
cgns statistics fwdIn2Out higher threshold exceeded	3.7.1	N
cgns statistics fwdIn2Out lower threshold exceeded	3.7.1	N
cgns statistics fwdIn2Out threshold normal	3.7.1	N
cgns statistics fwdOut2In higher threshold exceeded	3.7.1	N
cgns statistics fwdOut2In lower threshold exceeded	3.7.1	N
cgns statistics fwdOut2In threshold normal	3.7.1	N
cgns statistics translationsCreate higher threshold exceeded	3.7.1	N
cgns statistics translationsCreate lower threshold exceeded	3.7.1	N
cgns statistics translationsCreate threshold normal	3.7.1	N
cgns statistics translationsDelete higher threshold exceeded	3.7.1	N
cgns statistics translationsDelete lower threshold exceeded	3.7.1	N
cgns statistics translationsDelete threshold normal	3.7.1	N
Device Managed	3.7.1	N
Management Unreachable	3.7.1	N
Device Partially Managed	3.7.1	N
CPU utilization less than lower threshold	3.7.1	N
CPU utilization exceeded upper threshold	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 Link down due to Card event	3.7.1	N

Table 6-37 **Supported Service Events for Cisco 3600 Series—Cisco ANA Version 3.7.1 (continued)**

Event Name	ANA Version	Expedited
DS1 Path Link down on unreachable	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 up	3.7.1	N
DS3 Path Link down due to admin down	3.7.1	N
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 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
dwdm controller down	3.7.1	N
dwdm controller up	3.7.1	N
dwdm g709 status down	3.7.1	N
dwdm g709 status up	3.7.1	N
EFP down	3.7.1	N
EFP down	3.7.1	N
EFP up	3.7.1	N
Primary HSRP interface is active	3.7.1	N
Primary HSRP interface is not active	3.7.1	N
Secondary HSRP interface is active	3.7.1	N
Secondary HSRP interface is not active	3.7.1	N
ima administratively down	3.7.1	N
ima administratively up	3.7.1	N
ima operationally down	3.7.1	N
ima operationally up	3.7.1	N
Interface status down	3.7.1	N
Interface status up	3.7.1	N
keepalive not configured	3.7.1	N
keepalive configured	3.7.1	N

Table 6-37 Supported Service Events for Cisco 3600 Series—Cisco ANA Version 3.7.1 (continued)

Event Name	ANA Version	Expedited
l2tp peer established	3.7.1	N
l2tp peer is removed	3.7.1	N
l2tp peer not established	3.7.1	N
LAG down	3.7.1	N
LAG down	3.7.1	N
LAG up	3.7.1	N
LAG Link down	3.7.1	N
LAG Link down	3.7.1	N
LAG Link up	3.7.1	N
Layer 2 tunnel 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 up	3.7.1	N
Link over utilized	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
Memory utilization less than lower threshold	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
High Priority MPLS-TE tunnel down	3.7.1	N
Low Priority MPLS-TE tunnel down	3.7.1	N
Medium Priority MPLS-TE tunnel down	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

Table 6-37 **Supported Service Events for Cisco 3600 Series—Cisco ANA Version 3.7.1 (continued)**

Event Name	ANA Version	Expedited
Port down due to Card out	3.7.1	N
Port down due to Card down	3.7.1	N
Port down due to oper	3.7.1	N
Port up	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
Shelf in	3.7.1	N
Shelf out	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 down due to Admin	3.7.1	N
SONET Path down due to Card	3.7.1	N
SONET Path down due to Oper	3.7.1	N
SONET Path up	3.7.1	N
VLAN Sub Interface down	3.7.1	N
VLAN Sub Interface down	3.7.1	N
VLAN Sub Interface up	3.7.1	N
Service down	3.7.1	N
Service 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
VSI down	3.7.1	N
VSI down	3.7.1	N
VSI up	3.7.1	N

Table 6-37 Supported Service Events for Cisco 3600 Series—Cisco ANA Version 3.7.1 (continued)

Event Name	ANA Version	Expedited
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 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 ANA Version 3.7.1, see [Cisco 3700 Series Multiservice Access Routers](#)):

This section contains the following topics:

- [Cisco 3700 Series—Supported Software Versions, page 6-54](#)
- [Cisco 3700 Series—Supported Topologies, page 6-54](#)
- [Cisco 3700 Series—Supported Modules, page 6-55](#)
- [Cisco 3700 Series—Supported Technologies, page 6-55](#)
- [Cisco 3700 Series—Supported Service Events, page 6-56](#)

Cisco 3700 Series—Supported Software Versions

Table 6-38 Supported Software Versions for Cisco 3700 Series—Cisco ANA Version 3.7.1

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

Cisco 3700 Series—Supported Topologies

Table 6-39 Supported Topologies for Cisco 3700 Series—Cisco ANA Version 3.7.1

Topology Type	Link Type	ANA 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 6-40 *Supported Modules for Cisco 3700 Series—Cisco ANA Version 3.7.1*

Module Name	ANA 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 ANA Version 3.7.1:

- [IP, page 6-182](#)
- [Routing Protocols, page 6-185](#)
- [Ethernet, page 6-188](#)
- [ATM, page 6-197](#)
- [Frame Relay, page 6-200](#)
- [PPP, page 6-202](#)
- [SONET/SDH, page 6-204](#)
- [TDM/DSx, page 6-206](#)
- [MPLS, page 6-210](#)
- [MPLS-TE, page 6-212](#)

- [VPN \(VRF\), page 6-215](#)
- [PWE3, page 6-217](#)
- [Security, page 6-218](#)
- [Hardware, page 6-220](#)
- [Serial, page 6-223](#)
- [Additional Technologies, page 6-224](#)
- [LocalSwitching, page 6-226](#)
- [CDP, page 6-230](#)
- [Discovery Protocol, page 6-230](#)

Cisco 3700 Series—Supported Service Events

Table 6-41 Supported Service Events for Cisco 3700 Series—Cisco ANA Version 3.7.1

Event Name	ANA 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
Device Unreachable	3.6.0	N
Device Unsupported	3.6.0	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
Module Unsupported	3.6.0	N
MPLS Black Hole found	3.6.0	N

Table 6-41 **Supported Service Events for Cisco 3700 Series—Cisco ANA Version 3.7.1 (continued)**

Event Name	ANA Version	Expedited
MPLS TE Tunnel Down/Flapping	3.6.0	N
Port Down	3.6.0	N
Port Flapping	3.6.0	N
Rx utilization exceeded upper threshold	3.6.0	N
Tx utilization exceeded upper threshold	3.6.0	N
VPN Leak	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
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 down	3.7.1	N
EFP up	3.7.1	N
Primary HSRP interface is active	3.7.1	N
Primary HSRP interface is not active	3.7.1	N
Secondary HSRP interface is active	3.7.1	N
Secondary HSRP interface is not active	3.7.1	N
ima operationaly down	3.7.1	N
Interface status down	3.7.1	N

Table 6-41 *Supported Service Events for Cisco 3700 Series—Cisco ANA Version 3.7.1 (continued)*

Event Name	ANA Version	Expedited
Interface status up	3.7.1	N
LAG down	3.7.1	N
LAG down	3.7.1	N
LAG Link 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
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 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 ANA Version 3.7.1, see [Cisco 3800 Series Integrated Services Routers](#)):

This section contains the following topics:

- [Cisco 3800 Series—Supported Software Versions, page 6-59](#)
- [Cisco 3800 Series—Supported Topologies, page 6-59](#)
- [Cisco 3800 Series—Supported Modules, page 6-59](#)
- [Cisco 3800 Series—Supported Technologies, page 6-61](#)
- [Cisco 3800 Series—Supported Service Events, page 6-61](#)

Cisco 3800 Series—Supported Software Versions

Table 6-42 Supported Software Versions for Cisco 3800 Series—Cisco ANA Version 3.7.1

Software Version	ANA 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

¹ANA 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 6-43 Supported Topologies for Cisco 3800 Series—Cisco ANA Version 3.7.1

Topology Type	Link Type	ANA 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 6-44 Supported Modules for Cisco 3800 Series—Cisco ANA Version 3.7.1

Module Name	ANA 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

Table 6-44 **Supported Modules for Cisco 3800 Series—Cisco ANA Version 3.7.1 (continued)**

Module Name	ANA Version	Module Description
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
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 ANA Version 3.7.1:

- [IP, page 6-182](#)
- [Routing Protocols, page 6-185](#)
- [Ethernet, page 6-188](#)
- [ATM, page 6-197](#)
- [Frame Relay, page 6-200](#)
- [PPP, page 6-202](#)
- [HDLC, page 6-204](#)
- [TDM/DSx, page 6-206](#)
- [MPLS, page 6-210](#)
- [MPLS-TE, page 6-212](#)
- [VPN \(VRF\), page 6-215](#)
- [PWE3, page 6-217](#)
- [Security, page 6-218](#)
- [Hardware, page 6-220](#)
- [Serial, page 6-223](#)
- [CDP, page 6-230](#)
- [Discovery Protocol, page 6-230](#)

Cisco 3800 Series—Supported Service Events

Table 6-45 *Supported Service Events for Cisco 3800 Series—Cisco ANA Version 3.7.1*

Event Name	ANA 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
Device Unreachable	3.6.0	N
Device Unsupported	3.6.0	N

Table 6-45 *Supported Service Events for Cisco 3800 Series—Cisco ANA Version 3.7.1 (continued)*

Event Name	ANA Version	Expedited
Interface status down flapping	3.6.0	Y
Interface status down flapping update	3.6.0	Y
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
Module Unsupported	3.6.0	N
MPLS Black Hole found	3.6.0	N
Port Down	3.6.0	N
Port Flapping	3.6.0	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 down	3.7.1	N
EFP up	3.7.1	N
Interface status up	3.7.1	N
LAG down	3.7.1	N
LAG down	3.7.1	N
LAG Link 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
MPLS-TE tunnel down	3.7.1	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

Table 6-45 Supported Service Events for Cisco 3800 Series—Cisco ANA Version 3.7.1 (continued)

Event Name	ANA Version	Expedited
tx dormant	3.7.1	N
VSI down	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 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 ANA Version 3.7.1, see [Cisco 3900 Series Integrated Service Routers](#)):

This section contains the following topics:

- [Cisco ISR 3900 Series—Supported Software Versions](#), page 6-63
- [Cisco ISR 3900 Series—Supported Topologies](#), page 6-63
- [Cisco ISR 3900 Series—Supported Modules](#), page 6-64
- [Cisco ISR 3900 Series—Supported Technologies](#), page 6-64
- [Cisco ISR 3900 Series—Supported Service Events](#), page 6-65

Cisco ISR 3900 Series—Supported Software Versions

Table 6-46 Supported Software Versions for Cisco ISR 3900 Series—Cisco ANA Version 3.7.1

Software Version	ANA Version
IOS 15.1(T)	3.7.1

Cisco ISR 3900 Series—Supported Topologies

Table 6-47 Supported Topologies for Cisco ISR 3900 Series—Cisco ANA Version 3.7.1

Topology Type	Link Type	ANA 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 6-48 Supported Modules for Cisco ISR 3900 Series—Cisco ANA Version 3.7.1

Module Name	ANA 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

Cisco ISR 3900 Series—Supported Technologies

The following technologies are supported by the Cisco ISR 3900 Series in Cisco ANA Version 3.7.1:

- [IP, page 6-182](#)
- [Routing Protocols, page 6-185](#)
- [Ethernet, page 6-188](#)
- [ATM, page 6-197](#)
- [PPP, page 6-202](#)
- [TDM/DSx, page 6-206](#)
- [Security, page 6-218](#)
- [Hardware, page 6-220](#)
- [Serial, page 6-223](#)
- [LocalSwitching, page 6-226](#)
- [BFD, page 6-227](#)
- [Carrier Ethernet, page 6-228](#)
- [CDP, page 6-230](#)
- [Discovery Protocol, page 6-230](#)
- [Ethernet OAM, page 6-231](#)

Cisco ISR 3900 Series—Supported Service Events

Table 6-49 Supported Service Events for Cisco ISR 3900 Series—Cisco ANA Version 3.7.1

Event Name	ANA 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
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
Interface status down flapping update	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 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
Port Down	3.7.1	N
Port Flapping	3.7.1	N
Rx utilization exceeded upper threshold	3.7.1	N
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

Table 6-49 **Supported Service Events for Cisco ISR 3900 Series—Cisco ANA Version 3.7.1**

Event Name	ANA Version	Expedited
VSI Admin Down	3.7.1	N
VSI Down	3.7.1	N
VSI Up/Down	3.7.1	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
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 down	3.7.1	N
EFP up	3.7.1	N
Primary HSRP interface is active	3.7.1	N
Primary HSRP interface is not active	3.7.1	N
Secondary HSRP interface is active	3.7.1	N
Secondary HSRP interface is 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 down	3.7.1	N
LAG Link down	3.7.1	N

Table 6-49 Supported Service Events for Cisco ISR 3900 Series—Cisco ANA Version 3.7.1

Event Name	ANA Version	Expedited
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
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 4700 Series Routers

This section includes the following information about Cisco 4700 Series routers (for information on the NE types supported in Cisco ANA Version 3.7.1, see [Cisco 4700 Series Routers](#)):

This section contains the following topics:

- [Cisco 4700 Series—Supported Topologies, page 6-67](#)
- [Cisco 4700 Series—Supported Technologies, page 6-68](#)
- [Cisco 4700 Series—Supported Service Events, page 6-68](#)

Cisco 4700 Series—Supported Topologies

Table 6-50 Supported Topologies for Cisco 4700 Series—Cisco ANA Version 3.7.1

Topology Type	Link Type	ANA 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 ANA Version 3.7.1:

- [IP](#), page 6-182
- [Routing Protocols](#), page 6-185
- [Ethernet](#), page 6-188
- [ATM](#), page 6-197
- [Frame Relay](#), page 6-200
- [PPP](#), page 6-202
- [HDLC](#), page 6-204
- [SONET/SDH](#), page 6-204
- [TDM/DSx](#), page 6-206
- [MPLS](#), page 6-210
- [MPLS-TE](#), page 6-212
- [VPN \(VRF\)](#), page 6-215
- [PWE3](#), page 6-217
- [Security](#), page 6-218
- [Hardware](#), page 6-220
- [Serial](#), page 6-223
- [IPoDWDM](#), page 6-224
- [LocalSwitching](#), page 6-226
- [BFD](#), page 6-227
- [Carrier Ethernet](#), page 6-228
- [CDP](#), page 6-230
- [Discovery Protocol](#), page 6-230

Cisco 4700 Series—Supported Service Events

Table 6-51 *Supported Service Events for Cisco 4700 Series—Cisco ANA Version 3.7.1*

Event Name	ANA 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 6-51 **Supported Service Events for Cisco 4700 Series—Cisco ANA Version 3.7.1 (continued)**

Event Name	ANA Version	Expedited
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
Interface status down flapping	3.7.1	Y
Interface status down flapping update	3.7.1	Y
Layer 2 Tunnel Down	3.7.1	N
Link 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
Port Down	3.7.1	N
Port Flapping	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 down	3.7.1	N
EFP up	3.7.1	N
Interface status up	3.7.1	N
LAG down	3.7.1	N
LAG down	3.7.1	N
LAG Link 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

Table 6-51 Supported Service Events for Cisco 4700 Series—Cisco ANA Version 3.7.1 (continued)

Event Name	ANA Version	Expedited
MPLS-TE tunnel down	3.7.1	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 down	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 7200 Series Routers

This section includes the following information about Cisco 7200 Series routers (for information on the NE types supported in Cisco ANA Version 3.7.1, see [Cisco 7200 Series Routers](#)):

This section contains the following topics:

- [Cisco 7200 Series—Supported Software Versions, page 6-70](#)
- [Cisco 7200 Series—Supported Topologies, page 6-73](#)
- [Cisco 7200 Series—Supported Modules, page 6-73](#)
- [Cisco 7200 Series—Supported Technologies, page 6-76](#)
- [Cisco 7200 Series—Supported Service Events, page 6-76](#)

Cisco 7200 Series—Supported Software Versions

Table 6-52 Supported Software Versions for Cisco 7200 Series—Cisco ANA Version 3.7.1

Software Version	ANA 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

Table 6-52 *Supported Software Versions for Cisco 7200 Series—Cisco ANA Version 3.7.1*

Software Version	ANA Version
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
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
IOS 12.2(33)SRC2	3.7.1
IOS 12.2(33)SRC3	3.6.7 ⁴
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
IOS 12.2(33)SRD1	3.6.6 ⁵

Table 6-52 Supported Software Versions for Cisco 7200 Series—Cisco ANA Version 3.7.1

Software Version	ANA Version
IOS 12.2(33)SRD2	3.7.1
IOS 12.2(33)SRD3	3.7.1
IOS 12.2(34)	3.6.0 ⁶
IOS 12.2(37)	3.6.0 ⁷
IOS 12.2(40)	3.6.0 ⁸
IOS 12.2(31)SB11	3.7 ⁹
IOS 12.3(10)	3.6.0 ¹⁰
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 ¹¹
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 ¹²
IOS 12.4(24)T	3.7.1

^{1, 2, 9, 10, 11}ANA models pluggable ports for this IOS version.

³ANA 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.

⁴Physical Inventory for this IOS 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.

⁵ANA recognizes all maintenance builds in this IOS release train. Physical Inventory for this IOS version will not be modeled since inventory data is not available using CLI and SNMP. ANA models pluggable ports for this IOS version.

^{6, 12}ANA recognizes all maintenance builds in this IOS release train. ANA models pluggable ports for this IOS version.

^{7, 8}ANA recognizes all maintenance builds in this IOS release train.

Cisco 7200 Series—Supported Topologies

Table 6-53 Supported Topologies for Cisco 7200 Series—Cisco ANA Version 3.7.1

Topology Type	Link Type	ANA 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
Physical Layer	Physical Layer	3.6.0
MLPPP	MLPPP	3.7.1
BFD	BFD	3.7.1
VPN (IPv6)	VPN	3.7.1

Cisco 7200 Series—Supported Modules

Table 6-54 Supported Modules for Cisco 7200 Series—Cisco ANA Version 3.7.1

Module Name	ANA 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 6-54 **Supported Modules for Cisco 7200 Series—Cisco ANA Version 3.7.1 (continued)**

Module Name	ANA 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-2FE-TX	3.6.0	2-Port Fast Ethernet 100Base TX 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-8E	3.6.0	8-Port 10BaseT Ethernet Port Adapter
PA-8T1	3.6.1	8-port channelized T1
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-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-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

Table 6-54 Supported Modules for Cisco 7200 Series—Cisco ANA Version 3.7.1 (continued)

Module Name	ANA Version	Module Description
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
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 Service Adapter
WS-G5484	3.6.1	1000Base-ZX extended reach GBIC(singlemode)
WS-G5486	3.6.1	1000Base-ZX extended reach GBIC(singlemode)

Table 6-54 Supported Modules for Cisco 7200 Series—Cisco ANA Version 3.7.1 (continued)

Module Name	ANA Version	Module Description
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 ANA Version 3.7.1:

- [IP, page 6-182](#)
- [Routing Protocols, page 6-185](#)
- [Ethernet, page 6-188](#)
- [ATM, page 6-197](#)
- [Frame Relay, page 6-200](#)
- [PPP, page 6-202](#)
- [HDLC, page 6-204](#)
- [SONET/SDH, page 6-204](#)
- [TDM/DSx, page 6-206](#)
- [MPLS, page 6-210](#)
- [MPLS-TE, page 6-212](#)
- [VPN \(VRF\), page 6-215](#)
- [PWE3, page 6-217](#)
- [Security, page 6-218](#)
- [Hardware, page 6-220](#)
- [Serial, page 6-223](#)
- [Additional Technologies, page 6-224](#)
- [LocalSwitching, page 6-226](#)
- [BFD, page 6-227](#)
- [CDP, page 6-230](#)
- [Discovery Protocol, page 6-230](#)

Cisco 7200 Series—Supported Service Events

Table 6-55 Supported Service Events for Cisco 7200 Series—Cisco ANA Version 3.7.1

Event Name	ANA Version	Expedited
Active IP Interfaces Found	3.6.0	Y
All IP Interfaces Down	3.6.0	Y

Table 6-55 **Supported Service Events for Cisco 7200 Series—Cisco ANA Version 3.7.1 (continued)**

Event Name	ANA Version	Expedited
BGP link down due to admin	3.6.0	Y
BGP link down due to oper	3.6.0	Y
BGP Neighbor Down	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
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 Admin Down	3.6.7	N
EFP down due to error disabled	3.6.7	N
EFP Up/Down	3.6.7	N
High priority IMA Down	3.7	N
IMA Administratively down	3.7	N
IMA Operationally down	3.7	N
IMA Operationally up	3.7	N
Interface Status Down/Up	3.6.0	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 Down	3.6.0	N
Link up	3.6.0	N

Table 6-55 **Supported Service Events for Cisco 7200 Series—Cisco ANA Version 3.7.1 (continued)**

Event Name	ANA Version	Expedited
Low priority IMA Down	3.7	N
Medium priority IMA Down	3.7	N
Memory utilization exceeded upper threshold	3.6.0	N
MLPPP Administratively down	3.7	N
MLPPP Operationally 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 TE Tunnel Down/Flapping	3.6.0	N
Port Down	3.6.0	N
Port Flapping	3.6.0	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
Vlan Tagged Interface AdminDown	3.6.7	N
Vlan Tagged Interface Up/Down	3.6.7	N
VPN Leak	3.6.0	N
VSI Admin Down	3.6.7	N
VSI Down	3.6.7	N
VSI Up/Down	3.6.7	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

Table 6-55 **Supported Service Events for Cisco 7200 Series—Cisco ANA Version 3.7.1 (continued)**

Event Name	ANA Version	Expedited
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 down	3.7.1	N
EFP up	3.7.1	N
Interface status up	3.7.1	N
LAG down	3.7.1	N
LAG down	3.7.1	N
LAG Link 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
MPLS-TE tunnel down	3.7.1	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 down	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 7300 Series Routers

This section includes the following information about Cisco 7300 Series routers (for information on the NE types supported in Cisco ANA Version 3.7.1, see [Cisco 7300 Series Routers](#)):

This section contains the following topics:

- [Cisco 7300 Series—Supported Software Versions, page 6-80](#)
- [Cisco 7300 Series—Supported Topologies, page 6-82](#)
- [Cisco 7300 Series—Supported Modules, page 6-82](#)

- [Cisco 7300 Series—Supported Technologies, page 6-82](#)
- [Cisco 7300 Series—Supported Service Events, page 6-83](#)

Cisco 7300 Series—Supported Software Versions

Table 6-56 *Supported Software Versions for Cisco 7300 Series—Cisco ANA Version 3.7.1*

Software Version	ANA 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

Table 6-56 **Supported Software Versions for Cisco 7300 Series—Cisco ANA Version 3.7.1**

Software Version	ANA Version
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(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

^{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.

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

Cisco 7300 Series—Supported Topologies

Table 6-57 *Supported Topologies for Cisco 7300 Series—Cisco ANA Version 3.7.1*

Topology Type	Link Type	ANA Version
Business	Business	3.7
Ethernet	Ethernet	3.7
Physical Layer	Physical Layer	3.7
VPN (IPv6)	VPN	3.7

Cisco 7300 Series—Supported Modules

Table 6-58 *Supported Modules for Cisco 7300 Series—Cisco ANA Version 3.7.1*

Module Name	ANA Version	Module Description
NSE-150	3.7	
NSE-100	3.7	
SFP-OC3-MM	3.7	
SFP-OC3-IR1	3.7	
SFP-OC3-LR1	3.7	
7300-PA-CC	3.7	
C7304-MSC100-SPA	3.7	

Cisco 7300 Series—Supported Technologies

The following technologies are supported by the Cisco 7300 Series in Cisco ANA Version 3.7.1:

- [IP, page 6-182](#)
- [Routing Protocols, page 6-185](#)
- [Ethernet, page 6-188](#)
- [ATM, page 6-197](#)
- [HDLC, page 6-204](#)
- [SONET/SDH, page 6-204](#)
- [MPLS, page 6-210](#)
- [VPN \(VRF\), page 6-215](#)
- [Security, page 6-218](#)
- [Hardware, page 6-220](#)
- [Serial, page 6-223](#)
- [CDP, page 6-230](#)

- [Discovery Protocol, page 6-230](#)

Cisco 7300 Series—Supported Service Events

Table 6-59 *Supported Service Events for Cisco 7300 Series—Cisco ANA Version 3.7.1*

Event Name	ANA Version	Expedited
Active IP Interfaces Found	3.7	Y
All IP Interfaces Down	3.7	Y
BGP Neighbor Down	3.7	N
Card Down	3.7	Y
Card In	3.7	Y
Card Out	3.7	Y
Card Up	3.7	Y
Device Unreachable	3.7	N
Device Unsupported	3.7	N
Interface status down flapping	3.7	Y
Interface status down flapping update	3.7	Y
Link up	3.7	N
Port Down	3.7	N
Port Flapping	3.7	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 down	3.7.1	N
EFP up	3.7.1	N
Interface status up	3.7.1	N
LAG down	3.7.1	N
LAG down	3.7.1	N
LAG Link down	3.7.1	N
LAG Link down	3.7.1	N

Table 6-59 Supported Service Events for Cisco 7300 Series—Cisco ANA Version 3.7.1 (continued)

Event Name	ANA Version	Expedited
Local switching entry down	3.7.1	N
Local switching entry up	3.7.1	N
Logical port down	3.7.1	N
MPLS-TE tunnel down	3.7.1	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 down	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 7400 Series Routers

This section includes the following information about Cisco 7400 Series routers (for information on the NE types supported in Cisco ANA Version 3.7.1, see [Cisco 7400 Series Routers](#)):

This section contains the following topics:

- [Cisco 7400 Series—Supported Software Versions, page 6-84](#)
- [Cisco 7400 Series—Supported Topologies, page 6-86](#)
- [Cisco 7400 Series—Supported Modules, page 6-86](#)
- [Cisco 7400 Series—Supported Technologies, page 6-87](#)
- [Cisco 7400 Series—Supported Service Events, page 6-88](#)

Cisco 7400 Series—Supported Software Versions

Table 6-60 Supported Software Versions for Cisco 7400 Series—Cisco ANA Version 3.7.1

Software Version	ANA 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

Table 6-60 **Supported Software Versions for Cisco 7400 Series—Cisco ANA Version 3.7.1**

Software Version	ANA Version
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 6-61 Supported Topologies for Cisco 7400 Series—Cisco ANA Version 3.7.1

Topology Type	Link Type	ANA 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 6-62 Supported Modules for Cisco 7400 Series—Cisco ANA Version 3.7.1

Module Name	ANA 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
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

Table 6-62 **Supported Modules for Cisco 7400 Series—Cisco ANA Version 3.7.1 (continued)**

Module Name	ANA Version	Module Description
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 ANA Version 3.7.1:

- [IP, page 6-182](#)
- [Routing Protocols, page 6-185](#)
- [Ethernet, page 6-188](#)
- [ATM, page 6-197](#)
- [Frame Relay, page 6-200](#)
- [PPP, page 6-202](#)
- [HDLC, page 6-204](#)
- [SONET/SDH, page 6-204](#)
- [TDM/DSx, page 6-206](#)
- [MPLS, page 6-210](#)
- [MPLS-TE, page 6-212](#)
- [VPN \(VRF\), page 6-215](#)
- [PWE3, page 6-217](#)
- [Security, page 6-218](#)
- [Hardware, page 6-220](#)
- [Serial, page 6-223](#)
- [Additional Technologies, page 6-224](#)
- [LocalSwitching, page 6-226](#)
- [CDP, page 6-230](#)
- [Discovery Protocol, page 6-230](#)

Cisco 7400 Series—Supported Service Events

Table 6-63 Supported Service Events for Cisco 7400 Series—Cisco ANA Version 3.7.1

Event Name	ANA 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
Device Unreachable	3.6.0	N
Device Unsupported	3.6.0	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
Module Unsupported	3.6.0	N
Port Down	3.6.0	N
Port Flapping	3.6.0	N
Rx utilization exceeded upper threshold	3.6.0	N
Tx utilization exceeded upper threshold	3.6.0	N
VPN Leak	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

Table 6-63 **Supported Service Events for Cisco 7400 Series—Cisco ANA Version 3.7.1 (continued)**

Event Name	ANA 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 down	3.7.1	N
EFP up	3.7.1	N
Primary HSRP interface is active	3.7.1	N
Primary HSRP interface is not active	3.7.1	N
Secondary HSRP interface is active	3.7.1	N
Secondary HSRP interface is 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 down	3.7.1	N
LAG Link 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

Table 6-63 Supported Service Events for Cisco 7400 Series—Cisco ANA Version 3.7.1 (continued)

Event Name	ANA Version	Expedited
OSPF Neighbor Up	3.7.1	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 7500 Series Routers

This section includes the following information about Cisco 7500 Series routers (for information on the NE types supported in Cisco ANA Version 3.7.1, see [Cisco 7500 Series Routers](#)):

This section contains the following topics:

- [Cisco 7500 Series—Supported Software Versions, page 6-90](#)
- [Cisco 7500 Series—Supported Topologies, page 6-92](#)
- [Cisco 7500 Series—Supported Modules, page 6-92](#)
- [Cisco 7500 Series—Supported Technologies, page 6-92](#)
- [Cisco 7500 Series—Supported Service Events, page 6-93](#)

Cisco 7500 Series—Supported Software Versions

Table 6-64 Supported Software Versions for Cisco 7500 Series—Cisco ANA Version 3.7.1

Software Version	ANA 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

Table 6-64 Supported Software Versions for Cisco 7500 Series—Cisco ANA Version 3.7.1

Software Version	ANA Version
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
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

Table 6-64 Supported Software Versions for Cisco 7500 Series—Cisco ANA Version 3.7.1

Software Version	ANA Version
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 6-65 Supported Topologies for Cisco 7500 Series—Cisco ANA Version 3.7.1

Topology Type	Link Type	ANA Version
Business	Business	3.7
Ethernet	Ethernet	3.7
Physical Layer	Physical Layer	3.7

Cisco 7500 Series—Supported Modules

Table 6-66 Supported Modules for Cisco 7500 Series—Cisco ANA Version 3.7.1

Module Name	ANA 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 ANA Version 3.7.1:

- [IP, page 6-182](#)

- [Routing Protocols, page 6-185](#)
- [Ethernet, page 6-188](#)
- [ATM, page 6-197](#)
- [HDLC, page 6-204](#)
- [SONET/SDH, page 6-204](#)
- [MPLS, page 6-210](#)
- [VPN \(VRF\), page 6-215](#)
- [Security, page 6-218](#)
- [Hardware, page 6-220](#)
- [Serial, page 6-223](#)
- [CDP, page 6-230](#)
- [Discovery Protocol, page 6-230](#)

Cisco 7500 Series—Supported Service Events

Table 6-67 *Supported Service Events for Cisco 7500 Series—Cisco ANA Version 3.7.1*

Event Name	ANA Version	Expedited
Active IP Interfaces Found	3.7	Y
All IP Interfaces Down	3.7	Y
BGP Neighbor Down	3.7	N
Card Down	3.7	Y
Card In	3.7	Y
Card Out	3.7	Y
Card Up	3.7	Y
Device Unreachable	3.7	N
Device Unsupported	3.7	N
Interface status down flapping	3.7	Y
Interface status down flapping update	3.7	Y
Link Down	3.7	N
Link up	3.7	N
Port Down	3.7	N
Port Flapping	3.7	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

Table 6-67 **Supported Service Events for Cisco 7500 Series—Cisco ANA Version 3.7.1 (continued)**

Event Name	ANA Version	Expedited
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 down	3.7.1	N
EFP up	3.7.1	N
Interface status up	3.7.1	N
LAG down	3.7.1	N
LAG down	3.7.1	N
LAG Link 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
MPLS-TE tunnel down	3.7.1	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 down	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 7600 Series Routers

This section includes the following information about Cisco 7600 Series routers (for information on the NE types supported in Cisco ANA Version 3.7.1, see [Cisco 7600 Series Routers](#)):

This section contains the following topics:

- [Cisco 7600 Series—Supported Software Versions, page 6-95](#)
- [Cisco 7600 Series—Supported Topologies, page 6-96](#)
- [Cisco 7600 Series—Supported Modules, page 6-96](#)

- [Cisco 7600 Series—Supported Technologies](#), page 6-110
- [Cisco 7600 Series—Supported Service Events](#), page 6-111

Cisco 7600 Series—Supported Software Versions

Table 6-68 *Supported Software Versions for Cisco 7600 Series—Cisco ANA Version 3.7.1*

Software Version	ANA 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

Table 6-68 Supported Software Versions for Cisco 7600 Series—Cisco ANA Version 3.7.1

Software Version	ANA Version
IOS 12.2(33)SRE	3.7 ¹⁷
IOS 12.2(33)SRE0a	3.7.0.1
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

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

⁵12.2(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.

⁶12.2(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 6-69 Supported Topologies for Cisco 7600 Series—Cisco ANA Version 3.7.1

Topology Type	Link Type	ANA 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
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

Cisco 7600 Series—Supported Modules

Table 6-70 Supported Modules for Cisco 7600 Series—Cisco ANA Version 3.7.1

Module Name	ANA 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)

Table 6-70 Supported Modules for Cisco 7600 Series—Cisco ANA Version 3.7.1 (continued)

Module Name	ANA Version	Module Description
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
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

Table 6-70 Supported Modules for Cisco 7600 Series—Cisco ANA Version 3.7.1 (continued)

Module Name	ANA Version	Module Description
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
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

Table 6-70 Supported Modules for Cisco 7600 Series—Cisco ANA Version 3.7.1 (continued)

Module Name	ANA Version	Module Description
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-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-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
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-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-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-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-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-XENPAK-30.33	3.6.7	10GBASE-DWDM 1530.33 nm XENPAK (100-GHz ITU grid)

Table 6-70 Supported Modules for Cisco 7600 Series—Cisco ANA Version 3.7.1 (continued)

Module Name	ANA Version	Module Description
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)
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)

Table 6-70 Supported Modules for Cisco 7600 Series—Cisco ANA Version 3.7.1 (continued)

Module Name	ANA Version	Module Description
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)
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)

Table 6-70 **Supported Modules for Cisco 7600 Series—Cisco ANA Version 3.7.1 (continued)**

Module Name	ANA Version	Module Description
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)
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)

Table 6-70 Supported Modules for Cisco 7600 Series—Cisco ANA Version 3.7.1 (continued)

Module Name	ANA Version	Module Description
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)
FAN-MOD-4HS	3.7	High-speed fan module
FAN-MOD-6HS	3.7	High Speed Fan Module for CISCO7606 Chassis
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-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
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

Table 6-70 Supported Modules for Cisco 7600 Series—Cisco ANA Version 3.7.1 (continued)

Module Name	ANA Version	Module Description
PA-2CE/PRI	3.6.1	Not Found
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 3Cx1 (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 6-70 Supported Modules for Cisco 7600 Series—Cisco ANA Version 3.7.1 (continued)

Module Name	ANA 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-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-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
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 CEs SPA
SPA-2X1GE	3.6.0	2-port Gigabit Ethernet SPA, SFP Optics
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

Table 6-70 Supported Modules for Cisco 7600 Series—Cisco ANA Version 3.7.1 (continued)

Module Name	ANA Version	Module Description
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-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-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
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

Table 6-70 Supported Modules for Cisco 7600 Series—Cisco ANA Version 3.7.1 (continued)

Module Name	ANA Version	Module Description
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 (IDS2) 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
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

Table 6-70 Supported Modules for Cisco 7600 Series—Cisco ANA Version 3.7.1 (continued)

Module Name	ANA Version	Module Description
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
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

Table 6-70 Supported Modules for Cisco 7600 Series—Cisco ANA Version 3.7.1 (continued)

Module Name	ANA Version	Module Description
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-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
WS-C6K-13SLOT-FAN	3.7 ³³	Cisco 7613 fan tray, spare
FAN-MOD-3SHS	3.7 ³⁴	Spare High-speed fan module for Cisco 7603-S Chassis
FAN-MOD-6SHS	3.7 ³⁵	High Speed Fan Module for CISCO7606-S Chassis

Table 6-70 Supported Modules for Cisco 7600 Series—Cisco ANA Version 3.7.1 (continued)

Module Name	ANA Version	Module Description
FAN-MOD-9	3.7 ³⁶	High-speed fan module

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, 32Support Verified against XC Combo Cards in ANA 3.7

^{33, 34}Refer bug - CSCtg86953

^{35, 36}Tested by John C.Refer bug - CSCtg86953

Cisco 7600 Series—Supported Technologies

The following technologies are supported by the Cisco 7600 Series in Cisco ANA Version 3.7.1:

- [IP, page 6-182](#)
- [Routing Protocols, page 6-185](#)
- [Ethernet, page 6-188](#)
- [ATM, page 6-197](#)
- [Frame Relay, page 6-200](#)
- [PPP, page 6-202](#)
- [HDLC, page 6-204](#)
- [SONET/SDH, page 6-204](#)
- [TDM/DSx, page 6-206](#)
- [MPLS, page 6-210](#)
- [MPLS-TE, page 6-212](#)
- [VPN \(VRF\), page 6-215](#)
- [PWE3, page 6-217](#)
- [Security, page 6-218](#)
- [Hardware, page 6-220](#)
- [Serial, page 6-223](#)
- [Additional Technologies, page 6-224](#)
- [IPoDWDM, page 6-224](#)
- [LocalSwitching, page 6-226](#)
- [BFD, page 6-227](#)
- [Carrier Ethernet, page 6-228](#)
- [CDP, page 6-230](#)
- [Discovery Protocol, page 6-230](#)
- [Ethernet OAM, page 6-231](#)

Cisco 7600 Series—Supported Service Events

Table 6-71 Supported Service Events for Cisco 7600 Series—Cisco ANA Version 3.7.1

Event Name	ANA 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
BGP Neighbor Down	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
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 Admin Down	3.6.7	N
EFP down due to error disabled	3.6.7	N
EFP Up/Down	3.6.7	N
High priority IMA Down	3.7	N
IMA Administratively down	3.7	N
IMA Operationally down	3.7	N
IMA Operationally up	3.7	N
Interface Status Down/Up	3.6.0	N
Keepalive configured	3.7	N
Keepalive not configured	3.7	N

Table 6-71 **Supported Service Events for Cisco 7600 Series—Cisco ANA Version 3.7.1 (continued)**

Event Name	ANA Version	Expedited
Layer 2 Tunnel Down	3.6.0	N
LDP neighbor down	3.6.0	Y
Link Down	3.6.0	N
Link up	3.6.0	N
Low priority IMA Down	3.7	N
Medium priority IMA Down	3.7	N
Memory utilization exceeded upper threshold	3.6.0	N
MLPPP Administratively down	3.7	N
MLPPP Operationally 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 TE Tunnel Down/Flapping	3.6.0	N
Port Down	3.6.0	N
Port Flapping	3.6.0	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
Vlan Tagged Interface AdminDown	3.6.7	N
Vlan Tagged Interface Up/Down	3.6.7	N
VPN Leak	3.6.0	N
VSI Admin Down	3.6.7	N
VSI Down	3.6.7	N
VSI Up/Down	3.6.7	N
Device Managed	3.7.1	N

Table 6-71 **Supported Service Events for Cisco 7600 Series—Cisco ANA Version 3.7.1 (continued)**

Event Name	ANA Version	Expedited
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 down	3.7.1	N
EFP up	3.7.1	N
Interface status up	3.7.1	N
LAG down	3.7.1	N
LAG down	3.7.1	N
LAG Link 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
MPLS-TE tunnel down	3.7.1	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 down	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 10000 Series Routers

This section includes the following information about Cisco 10000 Series routers (for information on the NE types supported in Cisco ANA Version 3.7.1, see [Cisco 10000 Series Routers](#)):

This section contains the following topics:

- [Cisco 10000 Series—Supported Software Versions](#), page 6-114
- [Cisco 10000 Series—Supported Topologies](#), page 6-115
- [Cisco 10000 Series—Supported Modules](#), page 6-115
- [Cisco 10000 Series—Supported Technologies](#), page 6-116
- [Cisco 10000 Series—Supported Service Events](#), page 6-116

Cisco 10000 Series—Supported Software Versions

Table 6-72 *Supported Software Versions for Cisco 10000 Series—Cisco ANA Version 3.7.1*

Software Version	ANA 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

¹, ², ³, ⁴, ⁵, ⁶, ⁷, ⁸, ⁹, ¹⁰, ¹¹, ¹², ¹⁴ANA 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 6-73 Supported Topologies for Cisco 10000 Series—Cisco ANA Version 3.7.1

Topology Type	Link Type	ANA 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 6-74 Supported Modules for Cisco 10000 Series—Cisco ANA Version 3.7.1

Module Name	ANA Version	Module Description
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
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

Table 6-74 Supported Modules for Cisco 10000 Series—Cisco ANA Version 3.7.1 (continued)

Module Name	ANA Version	Module Description
SPA-2XCHOC12/DSO	3.7	2 port channelized OC12 to DS0 Shared Port Adapter
10000-SIP-600	3.7.1	Cisco 10000 SPA Interface Processor-600

Cisco 10000 Series—Supported Technologies

The following technologies are supported by the Cisco 10000 Series in Cisco ANA Version 3.7.1:

- [IP, page 6-182](#)
- [Routing Protocols, page 6-185](#)
- [Ethernet, page 6-188](#)
- [ATM, page 6-197](#)
- [Frame Relay, page 6-200](#)
- [PPP, page 6-202](#)
- [HDLC, page 6-204](#)
- [SONET/SDH, page 6-204](#)
- [TDM/DSx, page 6-206](#)
- [MPLS, page 6-210](#)
- [MPLS-TE, page 6-212](#)
- [VPN \(VRF\), page 6-215](#)
- [PWE3, page 6-217](#)
- [Security, page 6-218](#)
- [Hardware, page 6-220](#)
- [Serial, page 6-223](#)
- [Additional Technologies, page 6-224](#)
- [LocalSwitching, page 6-226](#)
- [Carrier Ethernet, page 6-228](#)
- [CDP, page 6-230](#)
- [Discovery Protocol, page 6-230](#)

Cisco 10000 Series—Supported Service Events

Table 6-75 Supported Service Events for Cisco 10000 Series—Cisco ANA Version 3.7.1

Event Name	ANA Version	Expedited
Active IP Interfaces Found	3.6.0	Y
All IP Interfaces Down	3.6.0	Y

Table 6-75 **Supported Service Events for Cisco 10000 Series—Cisco ANA Version 3.7.1**

Event Name	ANA Version	Expedited
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
Device Unsupported	3.6.0	N
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
Interface status down flapping	3.6.0	Y
Interface status down flapping update	3.6.0	Y
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	3.6.7	N
MLPPP Operationally down	3.6.7	N
MLPPP Up	3.6.7	N
Module Unsupported	3.6.0	N
MPLS Black Hole found	3.6.0	N
Port Down	3.6.0	N
Port Flapping	3.6.0	N
Rx utilization exceeded upper threshold	3.6.0	N

Table 6-75 Supported Service Events for Cisco 10000 Series—Cisco ANA Version 3.7.1

Event Name	ANA Version	Expedited
SONET Path down due to Admin	3.6.7	N
SONET Path down due to Oper	3.6.7	N
Sonet Path link down due to Admin down	3.6.7	N
Sonet Path link down due to Oper down	3.6.7	N
Sonet Path link Up	3.6.7	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
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 down	3.7.1	N
EFP up	3.7.1	N
Interface status up	3.7.1	N
LAG down	3.7.1	N
LAG down	3.7.1	N
LAG Link 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
MPLS-TE tunnel down	3.7.1	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

Table 6-75 Supported Service Events for Cisco 10000 Series—Cisco ANA Version 3.7.1

Event Name	ANA Version	Expedited
tx dormant	3.7.1	N
VSI down	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 12000 Series Routers

This section includes the following information about Cisco 12000 Series routers (for information on the NE types supported in Cisco ANA Version 3.7.1, see [Cisco 12000 Series Routers](#)):

This section contains the following topics:

- [Cisco 12000 Series—Supported Software Versions](#), page 6-119
- [Cisco 12000 Series—Supported Topologies](#), page 6-120
- [Cisco 12000 Series—Supported Modules](#), page 6-121
- [Cisco 12000 Series—Supported Technologies](#), page 6-126
- [Cisco 12000 Series—Supported Service Events](#), page 6-127

Cisco 12000 Series—Supported Software Versions

Table 6-76 Supported Software Versions for Cisco 12000 Series—Cisco ANA Version 3.7.1

Software Version	ANA 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 6-76 Supported Software Versions for Cisco 12000 Series—Cisco ANA Version 3.7.1

Software Version	ANA 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

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 6-77 Supported Topologies for Cisco 12000 Series—Cisco ANA Version 3.7.1

Topology Type	Link Type	ANA 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	3.6.0
LAG	LAG	3.6.2
MLPPP	MLPPP	3.7.1
VPN (IPv6)	VPN	3.7.1

Cisco 12000 Series—Supported Modules

Table 6-78 Supported Modules for Cisco 12000 Series—Cisco ANA Version 3.7.1

Module Name	ANA 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	24 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
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	5 port (Quad) OC-12 POS Card, Single Mode, Short Reach
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

Table 6-78 Supported Modules for Cisco 12000 Series—Cisco ANA Version 3.7.1 (continued)

Module Name	ANA Version	Module Description
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	5 Port (Quad) Enhanced OC-48 Long Reach FC Connector Line Card
4OC48E/POS-SR-SC	3.6.0	5 Port (Quad) Enhanced OC-48 Short Reach SC Connector Line Card
4XOC48POS/RPR	3.6.1	4-port OC48/STM16 POS/RPR Shared Port Adapter = SPA-4XOC48POS/RPR
6CT3-SMB	3.6.0	18 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	3.6.1	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-ADVNCDCSC	3.6.1	12010 Advanced Clock Scheduler Card
GSR10-ADVNCDSFC	3.6.1	12010 Advanced Switch Fabric Card
GSR10-ALRM	3.6.1	12410, 12010 Alarm Card
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

Table 6-78 Supported Modules for Cisco 12000 Series—Cisco ANA Version 3.7.1 (continued)

Module Name	ANA Version	Module Description
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-ADVNCDCSC	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
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

Table 6-78 Supported Modules for Cisco 12000 Series—Cisco ANA Version 3.7.1 (continued)

Module Name	ANA Version	Module Description
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
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

Table 6-78 Supported Modules for Cisco 12000 Series—Cisco ANA Version 3.7.1 (continued)

Module Name	ANA Version	Module Description
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 CEsP 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
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

Table 6-78 Supported Modules for Cisco 12000 Series—Cisco ANA Version 3.7.1 (continued)

Module Name	ANA Version	Module Description
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 ANA Version 3.7.1:

- [IP, page 6-182](#)
- [Routing Protocols, page 6-185](#)
- [Ethernet, page 6-188](#)
- [ATM, page 6-197](#)
- [Frame Relay, page 6-200](#)
- [PPP, page 6-202](#)
- [HDLC, page 6-204](#)
- [SONET/SDH, page 6-204](#)

- [TDM/DSx, page 6-206](#)
- [MPLS, page 6-210](#)
- [MPLS-TE, page 6-212](#)
- [VPN \(VRF\), page 6-215](#)
- [PWE3, page 6-217](#)
- [Security, page 6-218](#)
- [Hardware, page 6-220](#)
- [Serial, page 6-223](#)
- [Additional Technologies, page 6-224](#)
- [LocalSwitching, page 6-226](#)
- [Carrier Ethernet, page 6-228](#)
- [CDP, page 6-230](#)
- [Discovery Protocol, page 6-230](#)

Cisco 12000 Series—Supported Service Events

Table 6-79 *Supported Service Events for Cisco 12000 Series—Cisco ANA Version 3.7.1*

Event Name	ANA 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
Device Unreachable	3.6.0	N
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
Interface status down flapping	3.6.0	Y
Interface status down flapping update	3.6.0	Y
Keepalive configured	3.6.0	N

Table 6-79 Supported Service Events for Cisco 12000 Series—Cisco ANA Version 3.7.1

Event Name	ANA Version	Expedited
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 Operationally down	3.7	N
MLPPP Up	3.7	N
Module Unsupported	3.6.0	N
Port Down	3.6.0	N
Port Flapping	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
Vlan Tagged Interface AdminDown	3.6.7	N
Vlan Tagged Interface Up/Down	3.6.7	N
VPN Leak	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
Device Managed	3.7.1	N
Management Unreachable	3.7.1	N

Table 6-79 **Supported Service Events for Cisco 12000 Series—Cisco ANA Version 3.7.1**

Event Name	ANA Version	Expedited
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 down	3.7.1	N
EFP up	3.7.1	N
Primary HSRP interface is active	3.7.1	N
Primary HSRP interface is not active	3.7.1	N
Secondary HSRP interface is active	3.7.1	N
Secondary HSRP interface is 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 down	3.7.1	N
LAG Link 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
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

Table 6-79 Supported Service Events for Cisco 12000 Series—Cisco ANA Version 3.7.1

Event Name	ANA Version	Expedited
Low priority member down	3.7.1	N
Medium priority member down	3.7.1	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 ANA Version 3.7.1, see [Cisco XR 12000 Series Routers](#)):

This section contains the following topics:

- [Cisco XR 12000 Series—Supported Software Versions](#), page 6-130
- [Cisco XR 12000 Series—Supported Topologies](#), page 6-131
- [Cisco XR 12000 Series—Supported Modules](#), page 6-131
- [Cisco XR 12000 Series—Supported Technologies](#), page 6-137
- [Cisco XR 12000 Series—Supported Service Events](#), page 6-138
- [Cisco XR 12000 Series—Additional Information](#), page 6-141

Cisco XR 12000 Series—Supported Software Versions

Table 6-80 Supported Software Versions for Cisco XR 12000 Series—Cisco ANA Version 3.7.1

Software Version	ANA Version
IOX 3.4.0	3.6.0 ¹
IOX 3.4.1	3.6.0 ²
IOX 3.4.3	3.6.3 ³
IOX 3.5.0	3.6.1 ⁴
IOX 3.5.1	3.6.1 ⁵
IOX 3.6.0	3.6.3 ⁶
IOX 3.6.1	3.6.3 ⁷
IOX 3.6.2	3.6.5 ⁸
IOX 3.6.3	3.6.7 ⁹
IOX 3.7.0	3.6.4 ¹⁰
IOX 3.7.1	3.6.4 ¹¹
IOX 3.8.0	3.6.6 ¹²
IOX 3.8.1	3.6.7 ¹³
IOX 3.8.2	3.7 ¹⁴
IOX 3.8.4	3.7.1
IOX 3.9.0	3.7 ¹⁵

Table 6-80 Supported Software Versions for Cisco XR 12000 Series—Cisco ANA Version 3.7.1

Software Version	ANA Version
IOX 3.9.1	3.7.1

^{1, 2, 3, 4, 5, 8, 9, 10, 11, 13, 14, 15}ANA models pluggable ports for this IOS version.

^{6, 7, 12}ANA recognizes all maintenance builds in this IOS release train. ANA models pluggable ports for this IOS version.

Cisco XR 12000 Series—Supported Topologies

Table 6-81 Supported Topologies for Cisco XR 12000 Series—Cisco ANA Version 3.7.1

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

Cisco XR 12000 Series—Supported Modules

Table 6-82 Supported Modules for Cisco XR 12000 Series—Cisco ANA Version 3.7.1

Module Name	ANA 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	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	3.6.0	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

Table 6-82 **Supported Modules for Cisco XR 12000 Series—Cisco ANA Version 3.7.1 (continued)**

Module Name	ANA Version	Module Description
12410E-CSC	3.7.0.1	CISCO 12410 Enhanced Clock Scheduler Card
12410E-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	GSR 12810 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	24 Port Copper DS3 Interface Line Card
16OC3X/POS-I-LC-B	3.6.0	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	3.6.0	GSR 16-Port OC3/POS MM/I Eng3 Release B = 16OC3X/POS-IR-LC-B
16OC3X/POS-M-MJ-B	3.6.0	GSR16-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)
3GE-GBIC-SC	3.6.0	3 Port Gigabit Ethernet Line Card (trident)
4GE-SFP-LC	3.6.0	4 port-GE line card for Cisco 12000
4OC12/ATM-IR-SC	3.6.0	4-port OC12/STM4 ATM SM-IR ISE LC with SC connector
4OC12/ATM-MM-SC	3.6.0	4-port OC12/STM4 ATM MM ISE LC with SC connector
4OC12/ATM-MM-SC	3.6.0	GSR Edge Engine 48, ATM, 4 port OC12/STM4Multi Mode Short Reach Line Card
4OC12/POS-IR-SC	3.6.0	Enhanced 4 port OC-12 Intermediate Reach Line Card
4OC12/POS-IR-SC-B	3.6.0	Enhanced 4 port OC-12 Intermediate Reach Line Card
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	5 port (Quad) OC-12 POS Card, Single Mode, Short Reach
4OC3/ATM-IR-SC	3.6.0	4 port OC3/STM1 ATM line MM/IR card

Table 6-82 Supported Modules for Cisco XR 12000 Series—Cisco ANA Version 3.7.1 (continued)

Module Name	ANA Version	Module Description
4OC3/ATM-MM-SC	3.6.0	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	3.6.0	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 IR Eng3 release B
4OC48/POS-SR-SC	3.6.0	4 Port (Quad) Enhanced OC-48 Short Reach SC Connector Line Card
4OC48/POS-SR-SC	3.6.0	1 Port Packet Over Sonet OC-48, Single Mode, Short Reach, SC Connector Card
4XOC48POS/RPR	3.6.0	4-port OC48/STM16 POS/RPR Shared Port Adapter = SPA-4XOC48POS/RPR
6CT3-SMB	3.6.0	18 Port Copper DS3 Interface Line Card
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 MM/IR Eng3 Release B
8OC3X/POS-MM-MJ-B	3.6.0	GSR 8-Port OC3/POS MM/IR 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	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	GSR General Fan
EPA-GE/FE-BBRD	3.6.0	Modular Gigabit Ethernet Line Card
GSR10-AC-PDU	3.6.0	Cisco 12410 AC Power Distribution Unit (spare)
GSR10-ADVNCDCSC	3.6.0	12010 Advanced Clock Scheduler Card
GSR10-ADVNCDSFC	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

Table 6-82 Supported Modules for Cisco XR 12000 Series—Cisco ANA Version 3.7.1 (continued)

Module Name	ANA Version	Module Description
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-ADVNCDCSC	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
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

Table 6-82 Supported Modules for Cisco XR 12000 Series—Cisco ANA Version 3.7.1 (continued)

Module Name	ANA Version	Module Description
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	5 Port (Quad) Enhanced OC-48 Long Reach FC Connector Line Card
OC48E/POS-LR-SC	3.6.0	Enhanced OC-48 Long Reach SC Connector Line Card
OC48E/POS-SR-SC	3.6.0	5 Port (Quad) Enhanced OC-48 Short Reach SC Connector Line Card
OC48E/POS-SR-SC	3.6.0	Enhanced OC-48 Short Reach SC Connector 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	GSR, Edge Engine 48 Port OC-48 SRP Single Mode Long Reach Line Card
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
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-16c
SFP-OC48-LR2	3.6.1	OC-48c/STM-16c SFP, Long Reach (80km)
SPA-10X1GE	3.6.0	10-port 1 GbE Shared Port Adapter

Table 6-82 **Supported Modules for Cisco XR 12000 Series—Cisco ANA Version 3.7.1 (continued)**

Module Name	ANA Version	Module Description
SPA-10X1GE-V2	3.6.2	10-port 1GbE SPA (Fugu ASIC)
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	1-port 10GbE Shared Port Adapter XFP based V2
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
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

Table 6-82 **Supported Modules for Cisco XR 12000 Series—Cisco ANA Version 3.7.1 (continued)**

Module Name	ANA Version	Module Description
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

Cisco XR 12000 Series—Supported Technologies

The following technologies are supported by the Cisco XR 12000 Series in Cisco ANA Version 3.7.1:

- [IP](#), page 6-182
- [Routing Protocols](#), page 6-185
- [Ethernet](#), page 6-188
- [ATM](#), page 6-197
- [PPP](#), page 6-202
- [HDLC](#), page 6-204
- [SONET/SDH](#), page 6-204
- [TDM/DSx](#), page 6-206
- [MPLS](#), page 6-210
- [MPLS-TE](#), page 6-212
- [VPN \(VRF\)](#), page 6-215
- [PWE3](#), page 6-217
- [Security](#), page 6-218
- [Hardware](#), page 6-220
- [Serial](#), page 6-223
- [Additional Technologies](#), page 6-224
- [LocalSwitching](#), page 6-226
- [BFD](#), page 6-227
- [Carrier Ethernet](#), page 6-228

- [CDP, page 6-230](#)
- [Discovery Protocol, page 6-230](#)

Cisco XR 12000 Series—Supported Service Events

Table 6-83 Supported Service Events for Cisco XR 12000 Series—Cisco ANA Version 3.7.1

Event Name	ANA 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
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
EFP Up/Down	3.6.7	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 Operationally down	3.7	N
MLPPP Up	3.7	N

Table 6-83 **Supported Service Events for Cisco XR 12000 Series—Cisco ANA Version 3.7.1**

Event Name	ANA Version	Expedited
Module Unsupported	3.6.0	N
Port Down	3.6.0	N
Port Flapping	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
Vlan Tagged Interface AdminDown	3.6.7	N
Vlan Tagged Interface Up/Down	3.6.7	N
VPN Leak	3.6.0	N
VSI Admin Down	3.6.7	N
VSI Down	3.6.7	N
VSI Up/Down	3.6.7	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
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

Table 6-83 **Supported Service Events for Cisco XR 12000 Series—Cisco ANA Version 3.7.1**

Event Name	ANA Version	Expedited
DS3 Path up	3.7.1	N
EFP down	3.7.1	N
EFP down	3.7.1	N
EFP up	3.7.1	N
Primary HSRP interface is active	3.7.1	N
Primary HSRP interface is not active	3.7.1	N
Secondary HSRP interface is active	3.7.1	N
Secondary HSRP interface is 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 down	3.7.1	N
LAG Link 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
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 XR 12000 Series—Additional Information

This section contains additional information about the Cisco XR 12000 series and includes the following topics:

- [Cisco XR 12000 Series Prerequisite](#), page 6-141
- [SDR Support for XR 12000 Series](#), page 6-141

Cisco XR 12000 Series Prerequisite

As a prerequisite for the Cisco XR 12000 Series 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 XR 12000 Series

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

As a prerequisite for the XR 12000 Series VNE:

1. Install the Cisco IOS XR Manageability Package on top of the IOS-XR version.
2. Add the command `xml agent tty` to the device configuration.
3. 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`).

Cisco ANA uses the management network (if available) to manage the devices. The XR 12000 Series platform assigns specific management interfaces on the RP modules. 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/0/4/CPU0:12kXR#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 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 RP is active. In this environment, each 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:

```
RP/0/4/CPU0:12kXR#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 displays the modules that are associated with both the owner SDR and itself. However, it does not display the ports under the modules of the owner SDR in the Inventory window of Cisco ANA NetworkVision.

Cisco CRS-1 Carrier Routing System

This section includes the following information about Cisco Carrier Routing System (CRS-1) routers (for information on the NE types supported in Cisco ANA Version 3.7.1, see [Cisco CRS-1 Carrier Routing System](#)):

This section contains the following topics:

- [Cisco CRS-1—Supported Software Versions, page 6-142](#)
- [Cisco CRS-1—Supported Topologies, page 6-143](#)
- [Cisco CRS-1—Supported Modules, page 6-143](#)
- [Cisco CRS-1—Supported Technologies, page 6-148](#)
- [Cisco CRS-1—Supported Service Events, page 6-149](#)
- [Cisco CRS-1—Additional Information, page 6-151](#)

Cisco CRS-1—Supported Software Versions

Table 6-84 *Supported Software Versions for Cisco CRS-1—Cisco ANA Version 3.7.1*

Software Version	ANA Version
IOX 3.4.0	3.6.0 ¹
IOX 3.4.1	3.6.0 ²
IOX 3.4.3	3.6.3 ³
IOX 3.5.1	3.6.1 ⁴
IOX 3.6.0	3.6.3 ⁵
IOX 3.6.1	3.6.3 ⁶
IOX 3.6.2	3.6.4 ⁷
IOX 3.6.3	3.6.7 ⁸
IOX 3.7.0	3.6.4 ⁹
IOX 3.7.1	3.6.4 ¹⁰
IOX 3.8.0	3.6.6 ¹¹
IOX 3.8.1	3.6.7 ¹²
IOX 3.8.2	3.7 ¹³
IOX 3.8.4	3.7.1
IOX 3.9.0	3.7 ¹⁴
IOX 3.9.1	3.7.0.1

1, 2, 3, 4, 6, 7, 8, 9, 10, 12, 13 ANA models pluggable ports for this IOS XR version.

5, 11, 14 ANA recognizes all maintenance builds in this IOS XR release train. ANA models pluggable ports for this IOS XR version.

Cisco CRS-1—Supported Topologies

Table 6-85 Supported Topologies for Cisco CRS-1—Cisco ANA Version 3.7.1

Topology Type	Link Type	ANA 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
LAG	LAG	3.6.0
BFD	BFD	3.7.1

Cisco CRS-1—Supported Modules

Table 6-86 Supported Modules for Cisco CRS-1—Cisco ANA Version 3.7.1

Module Name	ANA Version	Module Description
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 (C-band) DPSK DWDM PLIM
1OC768-DPSK/C-O	3.6.2	1-Port OC-768/STM-256c (C-band) DPSK DWDM PLIM
1OC768-ITU/C	3.6.0	1 port OC768-POS-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
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

Table 6-86 Supported Modules for Cisco CRS-1—Cisco ANA Version 3.7.1 (continued)

Module Name	ANA Version	Module Description
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
4OC192-POS/DPT-LR	3.6.0	4OC192-POS DPT
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	4OC192-POS DPT
8-10GBE	3.6.0	8x10 Gigabite Ethernet port
8-10GBE-WL-XFP	3.7.1	Cisco CRS-1 Series 8xGbE WAN/LAN XFP Interface Module
8XOC3-OC12-PO	3.6.0	SPA POS 8XOC12 Card
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-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 6-86 Supported Modules for Cisco CRS-1—Cisco ANA Version 3.7.1 (continued)

Module Name	ANA 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-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-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-ADVSVC-PLIM	3.7.1	CRS Advances Services PLIM
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

Table 6-86 Supported Modules for Cisco CRS-1—Cisco ANA Version 3.7.1 (continued)

Module Name	ANA Version	Module Description
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	DC power shelf
CRS-FCC-SC/GEW	3.6.1	Module Crs 1 Fcc SC Ge
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-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-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	Cisco CRS-1 Series 8x10GbE Interface Module
OC192/POS-IR-SC	3.6.2	GSR 1 port Packet Over SONET OC-48c/STM-16 Single Mode Intermediate Reach with SC 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

Table 6-86 Supported Modules for Cisco CRS-1—Cisco ANA Version 3.7.1 (continued)

Module Name	ANA Version	Module Description
SPA-10X1GE	3.6.1	10-Port Gigabit Ethernet SPA
SPA-10X1GE-V2	3.6.1	10-Port Gigabit Ethernet SPA
SPA-1X10GE-L-V2	3.6.1	Cisco 1-Port 10GE LAN-PHY Shared Port Adapter
SPA-1X10GE-WL-V2	3.6.7	1-port 10 Gigabit Ethernet Wanphy Shared Port Adapter V2
SPA-1XCHOC12/DS0	3.6.2	1 port channelized OC12 to DS0 Shared Port Adapter
SPA-1XOC12-ATM-V2	3.6.4	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-1XOC192POS-XFP	3.6.0	1-port OC192/STM64 POS XFP Optics Shared Port Adapter
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	2-Port Channelized T3 SPA
SPA-2XOC12-POS	3.6.1	2-Port OC-3c/STM-1 and OC-12c/STM-4 POS SPA
SPA-2XOC48POS/RPR	3.6.1	3 Ports 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	3-port OC3c SFP Optics ATM Shared Port Adapter
SPA-4XOC12-POS	3.6.1	4-Port OC-3c/STM-1 and OC-12c/STM-4 POS SPA
SPA-4XOC3-POS	3.6.0	4-Port OC-3c/STM-1 POS SPA
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	4-Port T3/E3 Serial SPA
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	8-port Gigabit Ethernet Shared Port Adapter
SPA-8XCHT1/E1	3.6.1	8-Port Channelized T1/E1 SPA
SPA-8XOC12-POS	3.6.1	8-Port OC-12c/STM-4 Multirate POS SPA

Table 6-86 **Supported Modules for Cisco CRS-1—Cisco ANA Version 3.7.1 (continued)**

Module Name	ANA Version	Module Description
SPA-8XOC3-POS	3.6.0	8-Port OC-3c/STM-1 POS SPA
SPA-OC192POS-LR	3.6.1	1-PORT OC-192C/STM-64C POS/RPR SHARED PORT ADAPTER
SPA-OC192POS-VSR	3.6.1	1-PORT OC-192C/STM-64C POS/RPR SHARED PORT ADAPTER
SPA-OC192POS-XFP	3.6.0	1-port OC192/STM64 POS/RPR XFP Optics
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
XFP-10GER-OC192IR	3.6.7	Multirate XFP module for 10GBASE-IR and OC192 IR
XFP-10GZR-OC192LR	3.6.7	Multirate XFP module for 10GBASE-LR and OC192 LR

Cisco CRS-1—Supported Technologies

The following technologies are supported by the Cisco CRS-1 in Cisco ANA Version 3.7.1:

- [IP, page 6-182](#)
- [Routing Protocols, page 6-185](#)
- [Ethernet, page 6-188](#)
- [HDLC, page 6-204](#)
- [SONET/SDH, page 6-204](#)
- [TDM/DSx, page 6-206](#)
- [MPLS, page 6-210](#)
- [MPLS-TE, page 6-212](#)
- [VPN \(VRF\), page 6-215](#)
- [PWE3, page 6-217](#)
- [Security, page 6-218](#)
- [Hardware, page 6-220](#)
- [Serial, page 6-223](#)
- [Additional Technologies, page 6-224](#)
- [IPoDWDM, page 6-224](#)
- [LocalSwitching, page 6-226](#)
- [BFD, page 6-227](#)
- [Carrier Ethernet, page 6-228](#)

- [CDP, page 6-230](#)
- [Discovery Protocol, page 6-230](#)
- [CGN, page 6-235](#)

Cisco CRS-1—Supported Service Events

Table 6-87 *Supported Service Events for Cisco CRS-1—Cisco ANA Version 3.7.1*

Event Name	ANA 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
Cloud Problem	3.6.0	N
CPU utilization exceeded upper threshold	3.6.0	N
Device Unreachable	3.6.0	N
Device Unsupported	3.6.0	N
EFP Admin Down	3.6.7	N
EFP down due to error disabled	3.6.7	N
EFP Up/Down	3.6.7	N
Interface status down flapping	3.6.0	Y
Interface status down flapping update	3.6.0	Y
Layer 2 Tunnel Down	3.6.0	N
Link Down	3.6.0	N

Table 6-87 **Supported Service Events for Cisco CRS-1—Cisco ANA Version 3.7.1 (continued)**

Event Name	ANA Version	Expedited
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
Port Down	3.6.0	N
Port Flapping	3.6.0	N
Vlan Tagged Interface AdminDown	3.7.1	N
Vlan Tagged Interface Up/Down	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 down	3.7.1	N
EFP up	3.7.1	N
Interface status up	3.7.1	N
LAG down	3.7.1	N
LAG down	3.7.1	N
LAG Link 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
MPLS-TE tunnel down	3.7.1	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 down	3.7.1	N

Table 6-87 **Supported Service Events for Cisco CRS-1—Cisco ANA Version 3.7.1 (continued)**

Event Name	ANA Version	Expedited
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 CRS-1—Additional Information

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

- [Cisco Carrier Routing System \(CRS-1\) Prerequisite, page 6-151](#)
- [SDR Support for CRS-1, page 6-151](#)
- [Multichassis Support for CRS-1, page 6-152](#)

Cisco Carrier Routing System (CRS-1) Prerequisite

As a prerequisite for the CRS-1 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-1

Secure Domain Router (SDR) is supported as a separate, independent VNE, with its own IP and login sequence. When adding an SDR to Cisco ANA, it is treated like any other network element, that is, it is added as a new VNE using Cisco ANA Manage. 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-1 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:

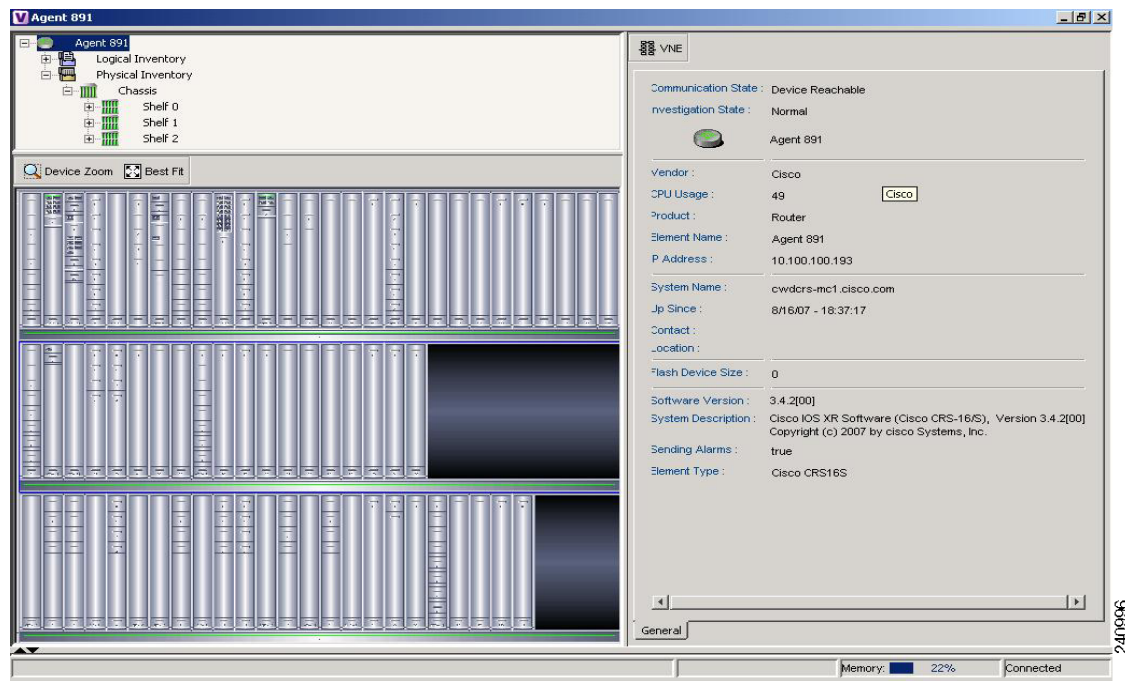
```
DRP/0/3/CPU0:CRS-PE1#show running-config ipv4 virtual address
ipv4 virtual address 10.52.123.11 255.255.255.0
```

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 ANA NetworkVision. It does not display the fabric, fan and power supply (namely, the shared modules).

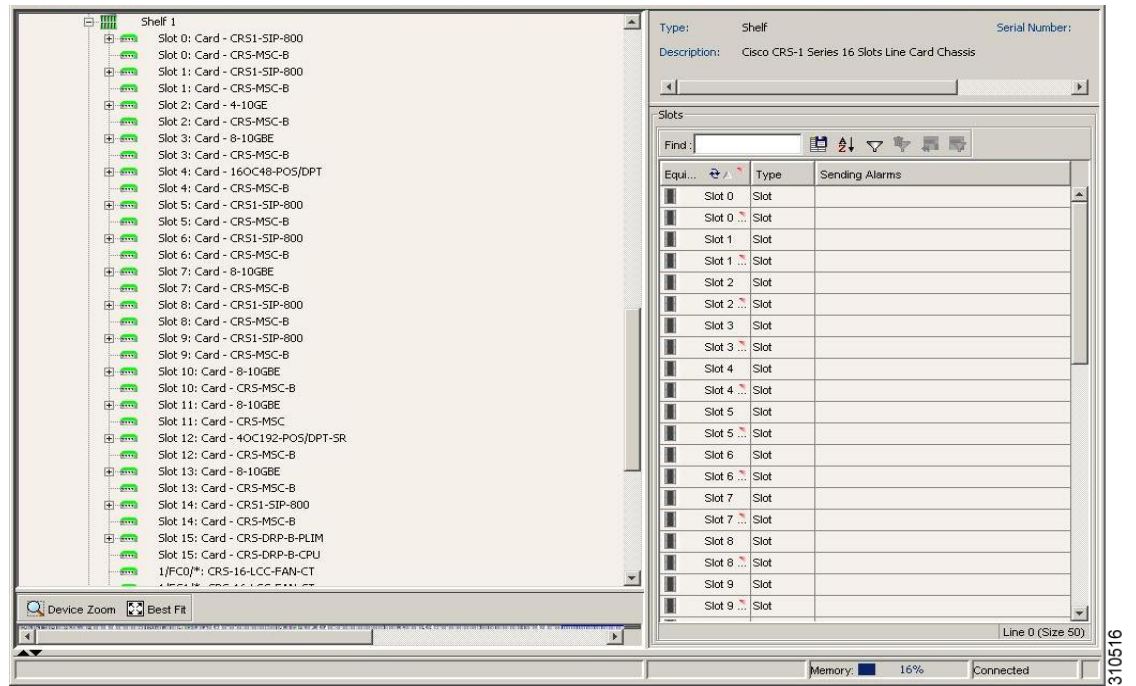
Multichassis Support for CRS-1

Multichassis support is available in Cisco ANA for 16-slot CRS-1 devices. As shown in [Figure 6-1](#), the chassis functions purely as a container for the shelves, which are treated as individual chassis and are numbered incrementally starting with 0.

Figure 6-1 CRS-1 Multichassis Support

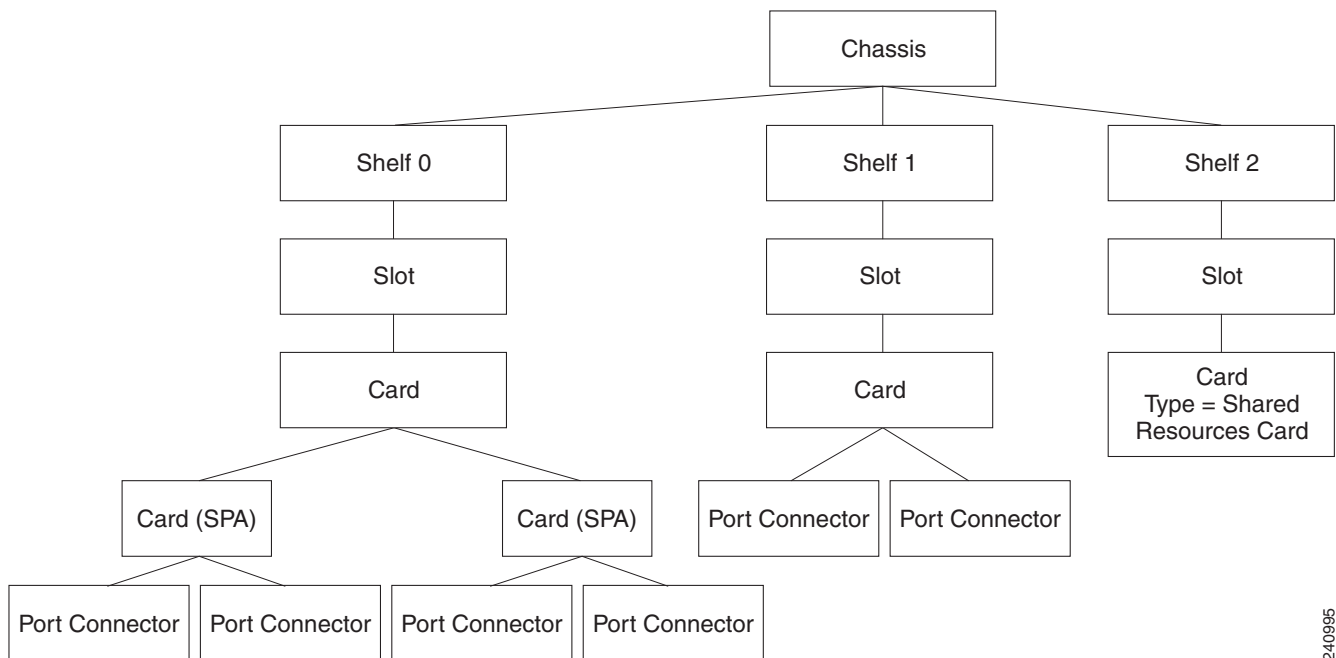


As shown in [Figure 6-2](#), expanding a shelf displays the modules that are installed on that shelf.

Figure 6-2 CRS-1 Multichassis Support—Expanded View

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.

Figure 6-3 describes the physical model for the CRS-1 multichassis.

Figure 6-3 CRS-1 Multichassis Physical Model

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

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 ANA Version 3.7.1, see [Cisco ASR 1000 Series Routers](#)):

This section contains the following topics:

- [Cisco ASR 1000 Series—Supported Software Versions, page 6-154](#)
- [Cisco ASR 1000 Series—Supported Topologies, page 6-155](#)
- [Cisco ASR 1000 Series—Supported Modules, page 6-155](#)
- [Cisco ASR 1000 Series—Supported Technologies, page 6-158](#)
- [Cisco ASR 1000 Series—Supported Service Events, page 6-159](#)

Cisco ASR 1000 Series—Supported Software Versions

Table 6-88 *Supported Software Versions for Cisco ASR 1000 Series—Cisco ANA Version 3.7.1*

Software Version	ANA Version
XE 2.2.3	3.6.6 ¹
XE 2.3.0	3.6.6 ²
XE 2.3.1	3.6.6 ³
XE 2.3.2	3.6.7 ⁴
XE 2.4.0	3.6.7 ⁵
XE 2.4.1	3.7 ⁶
XE 2.5.0	3.7 ⁷
XE 2.2.1	3.6.5 ⁸
XE 2.2.2	3.6.5 ⁹
XE 2.5.1	3.7.0.1 ¹⁰
XE 2.4.2	3.7.0.1
XE 2.4.3	3.7.0.1
XE 2.6.0	3.7.1
XE 3.1.0 S	3.7.1

^{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.
⁵ANA recognizes all maintenance builds in this IOS release trainANA models pluggable ports for this IOS version.

Cisco ASR 1000 Series—Supported Topologies

Table 6-89 Supported Topologies for Cisco ASR 1000 Series—Cisco ANA Version 3.7.1

Topology Type	Link Type	ANA Version
BGP	BGP	3.6.6
Ethernet	Ethernet	3.6.5
MPLS	MPLS	3.6.6
Physical Layer	Physical Layer	3.6.5
BFD	BFD	3.7.1
VPN (IPv6)	VPN	3.7.1

Cisco ASR 1000 Series—Supported Modules

Table 6-90 Supported Modules for Cisco ASR 1000 Series—Cisco ANA Version 3.7.1

Module Name	ANA Version	Module Description
4XGE-BUILT-IN	3.6.6	Cisco ASR1002 4 Port, Gigabit Ethernet SPA Card
ASR1000-ESP10	3.6.6	Cisco ASR 1000 10Gbps Embedded Services Processor
ASR1000-ESP20	3.6.6	Cisco ASR1000 Embedded Services Processor, 20G,Crypto
ASR1000-ESP5	3.6.5 ¹	ASR1K Embedded Services Processor,5Gbps,Crypto,ASR1002 only
ASR1000-RP1	3.6.5 ²	Cisco ASR1000 Route Processor 1, 2GB DRAM
ASR1000-RP2	3.6.6	Cisco ASR1000 Route Processor 2
ASR1000-SIP10	3.6.5 ³	Cisco ASR1000 SPA Interface Processor 10
ASR1002-PWR-AC	3.6.6	Cisco ASR 1002 AC Power Supply
ASR1002-PWR-DC	3.6.6	Cisco ASR1002 DC Power Supply
ASR1002-RP1	3.6.6	Cisco ASR1002 Route Processor 1
ASR1002-SIP10	3.6.6	Cisco ASR1002 SIP 10
ASR1004-PWR-AC	3.6.6	Cisco ASR 1004 AC Power Supply
ASR1004-PWR-DC	3.6.6	Cisco ASR 1004 DC Power Supply
ASR1006-PWR-AC	3.6.5	Cisco ASR1006 AC Power Supply
ASR1006-PWR-DC	3.6.6	Cisco ASR 1006 DC Power Supply
CWDM-SFP-1470	3.6.7	Cisco CWDM SFP 1470 nm;Gigabit Ethernet and 1G/2G FC
CWDM-SFP-1490	3.6.7	Cisco CWDM SFP 1490 nm;Gigabit Ethernet and 1G/2G FC

Table 6-90 **Supported Modules for Cisco ASR 1000 Series—Cisco ANA Version 3.7.1 (continued)**

Module Name	ANA Version	Module Description
CWDM-SFP-1510	3.6.7	Cisco CWDM SFP 1510 nm;Gigabit Ethernet and 1G/2G FC
CWDM-SFP-1530	3.6.7	Cisco CWDM SFP 1530 nm;Gigabit Ethernet and 1G/2G FC
CWDM-SFP-1550	3.6.7	Cisco CWDM SFP 1550 nm;Gigabit Ethernet and 1G/2G FC
CWDM-SFP-1570	3.6.7	Cisco CWDM SFP 1570 nm;Gigabit Ethernet and 1G/2G FC
CWDM-SFP-1590	3.6.7	Cisco CWDM SFP 1590 nm;Gigabit Ethernet and 1G/2G FC
CWDM-SFP-1610	3.6.7	Cisco CWDM SFP 1610 nm;Gigabit Ethernet and 1G/2G FC
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	3.6.7	100BASE-FX SFP module for Gigabit Ethernet ports, 1310 nm wavelength, 2 km over MMF
SFP-GE-L	3.6.6	Cisco SFP Gigabit Ethernet 1000Base LX
SFP-GE-S	3.6.6	SFP Gigabit Ethernet 1000Base SX
SFP-GE-T	3.6.6	SFP Gigabit Ethernet 1000Base Tx
SFP-GE-Z	3.6.6	SFP Gigabit Ethernet 1000Base Zx
SFP-OC12-IR1	3.6.6	SFP OC12 Intermediate Reach
SFP-OC12-LR1	3.6.6	SFP OC12 Long reach 1
SFP-OC12-LR2	3.6.6	Cisco OC 12 SFP Long Reach 2
SFP-OC12-MM	3.6.6	Cisco OC12 STM1 SFP Multimode
SFP-OC12-SR	3.6.6	Cisco OC12 STM1 SFP Short Reach
SFP-OC3-IR1	3.6.6	Cisco OC3 SFP Intermediate Reach
SFP-OC3-LR1	3.6.6	Cisco OC3 STM1 SFP Single Mode Fibre Long ReACH
SFP-OC3-LR2	3.6.6	Cisco OC3 STM1 SFP Single Mode Fibre Long Reach
SFP-OC3-MM	3.6.6	Cisco OC3 SFP Multimode
SFP-OC3-SR	3.6.6	Cisco OC 3 SFP Short Reach
SFP-OC48-IR1	3.6.6	Cisco OC 48 SFP Intermediate Reach 1
SFP-OC48-LR2	3.6.6	Cisco OC 48 SFP Long Reach 2
SFP-OC48-SR	3.6.6	SFP OC48 Short Reach
SPA-10XGE-V2	3.6.6	Cisco SPA 10 Port GE Version2

Table 6-90 Supported Modules for Cisco ASR 1000 Series—Cisco ANA Version 3.7.1 (continued)

Module Name	ANA Version	Module Description
SPA-1X10GE-L-V2	3.6.5 ⁴	Cisco 1-Port 10GE LAN-PHY Shared Port Adapter
SPA-1XCHSTM1/OC3	3.6.6	Cisco SPA 1 Port Channelized OC 3 STM 1
SPA-1XOC12-POS	3.6.6	Cisco 1 Port OC 12 POS
SPA-1XOC3-ATM-V2	3.6.6	Cisco SPA 1 Port OC3 ATM Version3
SPA-1XOC48POS	3.6.7	1-port OC48c/STM16c POS/RPR SFP Optics
SPA-1XOC48POS/RPR	3.6.6	Cisco SPA 1 Port Oc 48 POS RPR
SPA-2X1GE-V2	3.6.5 ⁵	Cisco 2-Port Gigabit Ethernet Shared Port Adapter, Version 2
SPA-2XCT3/DS0	3.6.6	Cisco SPA 2 Port Channelised T3/DS0
SPA-2XOC12-POS	3.6.7	2-Port OC-3c/STM-1 and OC-12c/STM-4 POS SPA
SPA-2XOC3-POS	3.6.6	Cisco SPA 2 Port OC3 POS
SPA-2XOC48POS/RPR	3.6.6	Cisco SPA 2 Port OC48 POS
SPA-2XT3/E3	3.6.6	Cisco SPA 2 Port T3/E3 Serial
SPA-3XOC3-ATM-V2	3.6.6	Cisco SPA 3 Port OC3 ATM Version 2
SPA-4X1FE-TX-V2	3.6.6	Cisco 4x 1 Port Fast Ethernet Tx V2
SPA-4XCT3/DS0	3.6.6	Cisco SPA 4 Port Channelised T3/DS0
SPA-4XOC12-POS	3.6.7	4-port OC-12/STM-4 POS Shared Port Adapters
SPA-4XOC3-POS	3.6.6	Cisco SPA 4 Port OC3 POS
SPA-4XOC48POS/RPR	3.6.6	Cisco SPA 4 Port Oc 48 POS RPR
SPA-4XT3/E3	3.6.6	Cisco SPA 4Port T3/E3
SPA-4XT-SERIAL	3.6.6	Cisco 4 Port Serial SPA
SPA-5X1GE-V2	3.6.6	Cisco SPA 5 x 1 Port Gigabit Ethernet V2
SPA-8X1FE-TX-V2	3.6.5 ⁶	Cisco 8-Port 10BASE-T/100BASE Fast Ethernet Shared Port Adapter, V-2
SPA-8X1GE-V2	3.6.6	Cisco SPA 8 x 1 Port Gigabit Ethernet V2
SPA-8XCHT1/E1	3.6.6	Cisco SPA 8 Port Channelized T1/E1
SPA-8XOC12-POS	3.6.7	8-Port OC-12c/STM-4 Multirate POS SPA
SPA-8XOC3-POS	3.6.7	8-Port OC-3c/STM-1 POS SPA
SPA-OC192POS-XFP	3.6.7	1-port OC192/STM64 POS/RPR XFP Optics
XFP-10GER-OC192IR	3.6.6	Multirate XFP module for 10GBASE-IR and OC192 IR
XFP-10GLR-OC192LR	3.6.7	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	3.6.5 ⁷	Multirate XFP module for 10GBASE-LR and OC192 SR-1

Table 6-90 **Supported Modules for Cisco ASR 1000 Series—Cisco ANA Version 3.7.1 (continued)**

Module Name	ANA Version	Module Description
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	Multirate XFP module for 10GBASE-LR and OC192 LR
SPA-1XCHOC12/DS0	3.7.1	1-Port Channelized OC-12/STM-4 Shared Port Adapter

^{1, 2, 3, 4, 5, 6, 7}Also tested on ASR1004

Cisco ASR 1000 Series—Supported Technologies

The following technologies are supported by the Cisco ASR 1000 Series in Cisco ANA Version 3.7.1:

- [IP, page 6-182](#)
- [Routing Protocols, page 6-185](#)
- [Ethernet, page 6-188](#)
- [ATM, page 6-197](#)
- [Frame Relay, page 6-200](#)
- [SONET/SDH, page 6-204](#)
- [TDM/DSx, page 6-206](#)
- [MPLS, page 6-210](#)
- [MPLS-TE, page 6-212](#)
- [VPN \(VRF\), page 6-215](#)
- [PWE3, page 6-217](#)
- [Security, page 6-218](#)
- [Hardware, page 6-220](#)
- [Serial, page 6-223](#)
- [Additional Technologies, page 6-224](#)
- [LocalSwitching, page 6-226](#)
- [BFD, page 6-227](#)
- [Carrier Ethernet, page 6-228](#)
- [CDP, page 6-230](#)
- [Discovery Protocol, page 6-230](#)
- [SBC, page 6-236](#)

Cisco ASR 1000 Series—Supported Service Events

Table 6-91 Supported Service Events for Cisco ASR 1000 Series—Cisco ANA Version 3.7.1

Event Name	ANA Version	Expedited
Active IP Interfaces Found	3.6.5	Y
All IP Interfaces Down	3.6.5	Y
BGP Neighbor Down	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
Cloud Problem	3.6.5	N
Device Unreachable	3.6.5	N
Device Unsupported	3.6.5	N
Dropped packet rate exceeded upper threshold	3.6.5	N
Interface status down flapping	3.6.5	Y
Interface status down flapping update	3.6.5	Y
Link Down	3.6.5	N
Link up	3.6.5	N
Port Down	3.6.5	N
Port Flapping	3.6.5	N
Vlan Tagged Interface AdminDown	3.6.7	N
Vlan Tagged Interface Up/Down	3.6.7	N
VSI Admin Down	3.6.7	N
VSI Down	3.6.7	N
VSI Up/Down	3.6.7	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 down	3.7.1	N

Table 6-91 **Supported Service Events for Cisco ASR 1000 Series—Cisco ANA Version 3.7.1**

Event Name	ANA Version	Expedited
EFP up	3.7.1	N
Interface status up	3.7.1	N
LAG down	3.7.1	N
LAG down	3.7.1	N
LAG Link 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
MPLS-TE tunnel down	3.7.1	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 down	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 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 ANA Version 3.7.1, see [Cisco ASR 9000 Series Aggregation Services Routers](#)):

This section contains the following topics:

- [Cisco ASR 9000—Supported Software Versions](#), page 6-161
- [Cisco ASR 9000—Supported Topologies](#), page 6-161
- [Cisco ASR 9000—Supported Modules](#), page 6-161
- [Cisco ASR 9000—Supported Technologies](#), page 6-163
- [Cisco ASR 9000—Supported Service Events](#), page 6-164

Cisco ASR 9000—Supported Software Versions

Table 6-92 Supported Software Versions for Cisco ASR 9000—Cisco ANA Version 3.7.1

Software Version	ANA Version
IOX 3.7.2	3.6.5 ¹
IOX 3.7.3	3.6.7 ²
IOX 3.9.0	3.7 ³
IOX 3.9.1	3.7.1

^{1, 2, 3}ANA models pluggable ports for this IOS version.

Cisco ASR 9000—Supported Topologies

Table 6-93 Supported Topologies for Cisco ASR 9000—Cisco ANA Version 3.7.1

Topology Type	Link Type	ANA 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 6-94 Supported Modules for Cisco ASR 9000—Cisco ANA Version 3.7.1

Module Name	ANA Version	Module Description
A9K-1.5KW-DC	3.6.6	ASR-9K 1.5kW DC Power Module
A9K-2KW-DC	3.6.6	ASR-9K 2kW DC Power Module
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-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

Table 6-94 Supported Modules for Cisco ASR 9000—Cisco ANA Version 3.7.1 (continued)

Module Name	ANA Version	Module Description
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-RSP-4G	3.6.6	Route Switch Processor 4G Memory Hard Disc Drive
A9K-SIP-700	3.7	QFP SIP 20G Line Card
ASR-9006-FAN	3.6.6	ASR-9006 Fan Tray
ASR-9010-FAN	3.6.5	ASR-9010 Fan Tray (Req 2)
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
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

Table 6-94 **Supported Modules for Cisco ASR 9000—Cisco ANA Version 3.7.1 (continued)**

Module Name	ANA Version	Module Description
SFP-OC12-SR	3.7	OC-12/STM-4 pluggable short-reach (2 km) transceiver module, 1310-nm wavelength, LC connector
SPA-2XCHOC12/DS0	3.7	2 port channelized OC12 to DS0 Shared Port Adapter
XFP-10GER-192IR+	3.6.6	Multirate XFP module for 10GBASE-IR and OC192 IR
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
A9K-8T-L	3.7.1	8-Port 10GE Low Queue Line Card, Requires XFPs
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
A9K-16T/8-B	3.7.0.1	16-Port 10GE Line Card, Requires SFP+

Cisco ASR 9000—Supported Technologies

The following technologies are supported by the Cisco ASR 9000 in Cisco ANA Version 3.7.1:

- [IP, page 6-182](#)
- [Routing Protocols, page 6-185](#)
- [Ethernet, page 6-188](#)
- [SONET/SDH, page 6-204](#)
- [MPLS, page 6-210](#)
- [MPLS-TE, page 6-212](#)
- [VPN \(VRF\), page 6-215](#)
- [PWE3, page 6-217](#)
- [Security, page 6-218](#)
- [Hardware, page 6-220](#)
- [Serial, page 6-223](#)
- [LocalSwitching, page 6-226](#)
- [BFD, page 6-227](#)
- [Carrier Ethernet, page 6-228](#)

- [CDP, page 6-230](#)
- [Discovery Protocol, page 6-230](#)
- [Ethernet OAM, page 6-231](#)

Cisco ASR 9000—Supported Service Events

Table 6-95 *Supported Service Events for Cisco ASR 9000—Cisco ANA Version 3.7.1*

Event Name	ANA Version	Expedited
Active IP Interfaces Found	3.6.5	Y
All IP Interfaces Down	3.6.5	Y
BFD neighbour loss	3.6.5	N
BGP link up	3.6.5	Y
BGP Neighbor Down	3.6.5	N
BGP process down	3.6.5	N
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
Cloud Problem	3.6.5	N
CPU utilization exceeded upper threshold	3.6.5	N
Device Unreachable	3.6.5	N
Device Unsupported	3.6.5	N
Dropped packet rate exceeded upper threshold	3.6.5	N
EFP Admin Down	3.6.7	N
EFP down due to error disabled	3.6.7	N
EFP Up/Down	3.6.7	N
Interface status down flapping	3.6.5	Y
Interface status down flapping update	3.6.5	Y
Link Down	3.6.5	N
Link up	3.6.5	N
Memory utilization exceeded upper threshold	3.6.5	N
Module Unsupported	3.6.5	N
Port Down	3.6.5	N
Port Flapping	3.6.5	N

Table 6-95 *Supported Service Events for Cisco ASR 9000—Cisco ANA Version 3.7.1 (continued)*

Event Name	ANA Version	Expedited
Rx utilization exceeded upper threshold	3.6.5	N
Tx utilization exceeded upper threshold	3.6.5	N
Vlan Tagged Interface AdminDown	3.6.7	N
Vlan Tagged Interface Up/Down	3.6.7	N
VSI Admin Down	3.6.7	N
VSI Down	3.6.7	N
VSI Up/Down	3.6.7	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 down	3.7.1	N
EFP up	3.7.1	N
Interface status up	3.7.1	N
LAG down	3.7.1	N
LAG down	3.7.1	N
LAG Link 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
MPLS-TE tunnel down	3.7.1	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 down	3.7.1	N

Table 6-95 Supported Service Events for Cisco ASR 9000—Cisco ANA Version 3.7.1 (continued)

Event Name	ANA Version	Expedited
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 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 ANA Version 3.7.1, see [Cisco MWR 2900 Series Mobile Wireless Routers](#)):

This section contains the following topics:

- [Cisco MWR 2941—Supported Software Versions](#), page 6-166
- [Cisco MWR 2941—Supported Topologies](#), page 6-166
- [Cisco MWR 2941—Supported Modules](#), page 6-167
- [Cisco MWR 2941—Supported Technologies](#), page 6-169
- [Cisco MWR 2941—Supported Service Events](#), page 6-170

Cisco MWR 2941—Supported Software Versions

Table 6-96 Supported Software Versions for Cisco MWR 2941—Cisco ANA Version 3.7.1

Software Version	ANA Version
12.2(33)MRA	3.7 ¹
12.4(19)MR2	3.6.6 ²
12.4(20)MR	3.6.7 ³

¹12.2(33)MRA(a.k.a)CSR 3.2; 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 MWR 2941—Supported Topologies

Table 6-97 Supported Topologies for Cisco MWR 2941—Cisco ANA Version 3.7.1

Topology Type	Link Type	ANA Version
ATM	ATM	3.6.6
BGP	BGP	3.6.6

Table 6-97 Supported Topologies for Cisco MWR 2941—Cisco ANA Version 3.7.1 (continued)

Topology Type	Link Type	ANA Version
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 6-98 Supported Modules for Cisco MWR 2941—Cisco ANA Version 3.7.1

Module Name	ANA Version	Module Description
ASM-M2900-TOP	3.6.6	Timing over Packet Accessory Service 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
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

Table 6-98 Supported Modules for Cisco MWR 2941—Cisco ANA Version 3.7.1 (continued)

Module Name	ANA Version	Module Description
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
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-SM-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

Table 6-98 **Supported Modules for Cisco MWR 2941—Cisco ANA Version 3.7.1 (continued)**

Module Name	ANA Version	Module Description
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 Category5 copper wire, extended operating temperature range and DOM support
SFP-GE-Z	3.7 ⁶	1000BASE-Zx Extended reach gigabit ethernet SFP.

^{1, 2, 3}Not Supported on 12.2(33)MRA (CSR3.2)

^{4, 5, 6}Supported on 12.2(33)MRA (CSR3.2)

Cisco MWR 2941—Supported Technologies

The following technologies are supported by the Cisco MWR 2941 in Cisco ANA Version 3.7.1:

- [IP](#), page 6-182
- [Routing Protocols](#), page 6-185
- [Ethernet](#), page 6-188
- [ATM](#), page 6-197
- [Frame Relay](#), page 6-200
- [PPP](#), page 6-202
- [TDM/DSx](#), page 6-206
- [MPLS](#), page 6-210
- [MPLS-TE](#), page 6-212
- [VPN \(VRF\)](#), page 6-215

- [PWE3, page 6-217](#)
- [Security, page 6-218](#)
- [Hardware, page 6-220](#)
- [Serial, page 6-223](#)
- [LocalSwitching, page 6-226](#)
- [BFD, page 6-227](#)
- [Carrier Ethernet, page 6-228](#)
- [CDP, page 6-230](#)
- [Discovery Protocol, page 6-230](#)
- [Ethernet OAM, page 6-231](#)

Cisco MWR 2941—Supported Service Events

Table 6-99 *Supported Service Events for Cisco MWR 2941—Cisco ANA Version 3.7.1*

Event Name	ANA 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
Cloud Problem	3.6.6	N
CPU utilization exceeded upper threshold	3.6.6	N
Device Unreachable	3.6.6	N
Device Unsupported	3.6.6	N
High priority IMA Down	3.7	N
IMA Administratively down	3.7	N
IMA Administratively up	3.7	N
IMA Operationally down	3.7	N
IMA Operationally up	3.7	N
Interface status down flapping	3.6.6	Y
Interface status down flapping update	3.6.6	Y
Layer 2 Tunnel Down	3.6.6	N
Link Down	3.6.6	N
Link up	3.6.6	N

Table 6-99 **Supported Service Events for Cisco MWR 2941—Cisco ANA Version 3.7.1 (continued)**

Event Name	ANA Version	Expedited
Low priority IMA Down	3.7	N
Memory utilization exceeded upper threshold	3.6.6	N
MLPPP Administratively down	3.7	N
MLPPP Operationally down	3.7	N
MLPPP Up	3.7	N
Module Unsupported	3.6.6	N
MPLS Black Hole found	3.6.6	N
Port Down	3.6.6	N
Port Flapping	3.6.6	N
Vlan Tagged Interface AdminDown	3.6.7	N
Vlan Tagged Interface Up/Down	3.6.7	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
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 down	3.7.1	N
EFP up	3.7.1	N
Primary HSRP interface is active	3.7.1	N
Primary HSRP interface is not active	3.7.1	N

Table 6-99 **Supported Service Events for Cisco MWR 2941—Cisco ANA Version 3.7.1 (continued)**

Event Name	ANA Version	Expedited
Secondary HSRP interface is active	3.7.1	N
Secondary HSRP interface is not active	3.7.1	N
ima operationaly 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 down	3.7.1	N
LAG Link 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 administatively 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
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 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 ANA Version 3.7.1, see [Cisco Universal Broadband Router 7200 Series](#)):

This section contains the following topics:

- [Cisco UBR7200 Series—Supported Software Versions](#), page 6-173
- [Cisco UBR7200 Series—Supported Topologies](#), page 6-173
- [Cisco UBR7200 Series—Supported Modules](#), page 6-173

- [Cisco UBR7200 Series—Supported Technologies, page 6-174](#)
- [Cisco UBR7200 Series—Supported Service Events, page 6-174](#)

Cisco UBR7200 Series—Supported Software Versions

Table 6-100 Supported Software Versions for Cisco UBR7200 Series—Cisco ANA Version 3.7.1

Software Version	ANA Version
IOS 12.3(21a)BC6	3.7.1

Cisco UBR7200 Series—Supported Topologies

Table 6-101 Supported Topologies for Cisco UBR7200 Series—Cisco ANA Version 3.7.1

Topology Type	Link Type	ANA 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 6-102 Supported Modules for Cisco UBR7200 Series—Cisco ANA Version 3.7.1

Module Name	ANA 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 ANA Version 3.7.1:

- [IP, page 6-182](#)
- [Routing Protocols, page 6-185](#)
- [Ethernet, page 6-188](#)
- [ATM, page 6-197](#)
- [Frame Relay, page 6-200](#)
- [PPP, page 6-202](#)
- [HDLC, page 6-204](#)
- [MPLS, page 6-210](#)
- [VPN \(VRF\), page 6-215](#)
- [Security, page 6-218](#)
- [Hardware, page 6-220](#)
- [Serial, page 6-223](#)
- [CDP, page 6-230](#)
- [Discovery Protocol, page 6-230](#)

Cisco UBR7200 Series—Supported Service Events

Table 6-103 Supported Service Events for Cisco UBR7200 Series—Cisco ANA Version 3.7.1

Event Name	ANA 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
DS0 Bundle Admin down	3.7.1	N
DS0 Bundle Oper down	3.7.1	N
DS0 Bundle Up	3.7.1	N

Table 6-103 **Supported Service Events for Cisco UBR7200 Series—Cisco ANA Version 3.7.1**

Event Name	ANA Version	Expedited
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
Interface status down flapping	3.7.1	Y
Interface status down flapping update	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 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 Operationally 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
Port Down	3.7.1	N
Port Flapping	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 down due to Oper	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
Vlan Tagged Interface AdminDown	3.7.1	N
Vlan Tagged Interface Up/Down	3.7.1	N
Device Managed		N
Management Unreachable		N
Device Partially Managed		N

Table 6-103 Supported Service Events for Cisco UBR7200 Series—Cisco ANA Version 3.7.1

Event Name	ANA Version	Expedited
DS3 Path Link down due to Card event		N
DS3 Path down due to Admin		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 down	3.7.1	N
EFP up	3.7.1	N
Interface status up	3.7.1	N
LAG down	3.7.1	N
LAG down	3.7.1	N
LAG Link 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
MPLS-TE tunnel down	3.7.1	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 down	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 Universal Broadband Router 10000 Series

This section includes the following information about Cisco UBR10000 Series routers (for information on the NE types supported in Cisco ANA Version 3.7.1, see [Cisco Universal Broadband Router 10000 Series](#)):

This section contains the following topics:

- [Cisco UBR10000 Series—Supported Software Versions](#), page 6-177

- [Cisco UBR10000 Series—Supported Topologies, page 6-177](#)
- [Cisco UBR10000 Series—Supported Modules, page 6-177](#)
- [Cisco UBR10000 Series—Supported Technologies, page 6-178](#)
- [Cisco UBR10000 Series—Supported Service Events, page 6-178](#)

Cisco UBR10000 Series—Supported Software Versions

Table 6-104 Supported Software Versions for Cisco UBR10000 Series—Cisco ANA Version 3.7.1

Software Version	ANA 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 6-105 Supported Topologies for Cisco UBR10000 Series—Cisco ANA Version 3.7.1

Topology Type	Link Type	ANA 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 6-106 Supported Modules for Cisco UBR10000 Series—Cisco ANA Version 3.7.1

Module Name	ANA Version	Module Description
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
UBR10-2XDS-SIP	3.7.1	2 bays I/O slot SPA interface processor
SPA-24XDS-SFP	3.7.1	1-Gbps wideband SPA for the CMTS
UBR10-MC5X20H-D	3.7.1	uBR10K High-Performance Card, 5DS w/upx, 20US, Spec An
10000-SIP-600	3.7.1	4 bay Cisco 10000 SPA Jacket Card
ESR-PRE4	3.7.1	Cisco 10000 Series Performance Routing Engine 4

Table 6-106 Supported Modules for Cisco UBR10000 Series—Cisco ANA Version 3.7.1 (continued)

Module Name	ANA Version	Module Description
SPA-1X10GE-L-V2	3.7.1	Cisco 1-Port 10 Gigabit Ethernet Shared Port Adapter
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-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-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
SFP-GE-T	3.7.1	1000BASE-T copper gigabit ethernet SFP.
UBR10-5X20S-D	3.7.1	Cisco 5x20S Broadband Processing Engine for the Cisco uBR10012 Universal Broadband Router

Cisco UBR10000 Series—Supported Technologies

The following technologies are supported by the Cisco UBR10000 Series in Cisco ANA Version 3.7.1:

- [IP, page 6-182](#)
- [Routing Protocols, page 6-185](#)
- [Ethernet, page 6-188](#)
- [MPLS, page 6-210](#)
- [VPN \(VRF\), page 6-215](#)
- [Security, page 6-218](#)
- [Hardware, page 6-220](#)
- [Serial, page 6-223](#)
- [CDP, page 6-230](#)
- [Discovery Protocol, page 6-230](#)

Cisco UBR10000 Series—Supported Service Events

Table 6-107 Supported Service Events for Cisco UBR10000 Series—Cisco ANA Version 3.7.1

Event Name	ANA Version	Expedited
Active IP Interfaces Found	3.7.1	Y
All IP Interfaces Down	3.7.1	Y

Table 6-107 **Supported Service Events for Cisco UBR10000 Series—Cisco ANA Version 3.7.1**

Event Name	ANA Version	Expedited
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
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
Interface status down flapping	3.7.1	Y
Interface status down flapping update	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 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 Operationally 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
Port Down	3.7.1	N
Port Flapping	3.7.1	N

Table 6-107 **Supported Service Events for Cisco UBR10000 Series—Cisco ANA Version 3.7.1**

Event Name	ANA Version	Expedited
SONET Path down due to Admin	3.7.1	N
SONET Path down due to Card	3.7.1	N
SONET Path down due to Oper	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
Vlan Tagged Interface AdminDown	3.7.1	N
Vlan Tagged Interface Up/Down	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 down	3.7.1	N
EFP up	3.7.1	N
Interface status up	3.7.1	N
LAG down	3.7.1	N
LAG down	3.7.1	N
LAG Link 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
MPLS-TE tunnel down	3.7.1	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

Table 6-107 **Supported Service Events for Cisco UBR10000 Series—Cisco ANA Version 3.7.1**

Event Name	ANA Version	Expedited
VSI down	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

Supported Technologies on Cisco Routers

The following sections list the objects and attributes that are supported on Cisco routers in Cisco ANA Version 3.7.1 per technology:

This section contains the following topics:

- [IP, page 6-182](#)
- [Routing Protocols, page 6-185](#)
- [Ethernet, page 6-188](#)
- [ATM, page 6-197](#)
- [Frame Relay, page 6-200](#)
- [PPP, page 6-202](#)
- [HDLC, page 6-204](#)
- [SONET/SDH, page 6-204](#)
- [TDM/DSx, page 6-206](#)
- [MPLS, page 6-210](#)
- [MPLS-TE, page 6-212](#)
- [VPN \(VRF\), page 6-215](#)
- [PWE3, page 6-217](#)
- [Security, page 6-218](#)
- [Hardware, page 6-220](#)
- [Serial, page 6-223](#)
- [Additional Technologies, page 6-224](#)
- [IPoDWDM, page 6-224](#)
- [LocalSwitching, page 6-226](#)
- [BFD, page 6-227](#)
- [Carrier Ethernet, page 6-228](#)
- [CDP, page 6-230](#)
- [Discovery Protocol, page 6-230](#)
- [Ethernet OAM, page 6-231](#)

- [CGN, page 6-235](#)
- [SBC, page 6-236](#)

IP

Table 6-108 *IP Attribute Support on Cisco Routers—Cisco ANA Version 3.7.1*

	800	1000	1600	1700	1800	2500	2600	2800	ISR2900	3600	3700	3800	ISR 3900	Cisco 4700	7200	7300	7400	7500	7600	10000	12000	XR 12000	CRS-1	ASR 1000	ASR 9000	MWR 2941	UBR7200	UBR10000
Attribute																												
IMO Name—IPIInterface																												
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
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
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
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
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
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
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
IP Multiplexing Table																												
IANA Type	Y		Y	Y		Y	Y	Y																				
Containing CTPs																												
Contained CTPs																												

Table 6-108 IP Attribute Support on Cisco Routers—Cisco ANA Version 3.7.1 (continued)

Attribute	800	1000	1600	1700	1800	2500	2600	2800	ISR2900	3600	3700	3800	ISR 3900	Cisco 4700	7200	7300	7400	7500	7600	10000	12000	XR 12000	CRS-1	ASR 1000	ASR 9000	MWR 2941	UBR7200	UBR10000
IMO Name—IIPMuxEntry																												
Termination Point	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
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
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
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
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
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
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
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
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
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
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
IMO Name—IARPEntity																												
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
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
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
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
IMO Name—IIPPool																												
IP Address Pool Entries																												
Name																												
Index																												
IMO Name—IIPRangeBasedIIPPoolEntry																												
Start IP Address																												

Table 6-108 IP Attribute Support on Cisco Routers—Cisco ANA Version 3.7.1 (continued)

Attribute	800	1000	1600	1700	1800	2500	2600	2800	ISR2900	3600	3700	3800	ISR 3900	Cisco 4700	7200	7300	7400	7500	7600	10000	12000	XR 12000	CRS-1	ASR 1000	ASR 9000	MWR 2941	UBR7200	UBR10000
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	Y	Y	Y			Y	Y		Y	Y	Y		Y		Y	Y	Y			Y		Y ¹	Y	Y
Port Description			Y	Y	Y	Y	Y	Y		Y	Y	Y	Y	Y	Y		Y		Y	Y	Y			Y		Y ²	Y	Y
Priority			Y	Y	Y	Y	Y	Y		Y	Y	Y	Y	Y	Y		Y		Y	Y	Y			Y		Y ³	Y	Y
Coupled Router			Y	Y	Y	Y	Y	Y		Y	Y	Y	Y	Y	Y		Y		Y	Y	Y			Y		Y ⁴	Y	Y
State			Y	Y	Y	Y	Y	Y		Y	Y	Y	Y	Y	Y		Y		Y	Y	Y			Y		Y ⁵	Y	Y
Tracking Interfaces																												
Virtual IP Address			Y	Y	Y	Y	Y	Y		Y	Y	Y	Y	Y	Y		Y		Y	Y	Y			Y		Y ⁶	Y	Y
Virtual MAC Address			Y	Y	Y	Y	Y	Y		Y	Y	Y	Y	Y	Y		Y		Y	Y	Y			Y		Y ⁷	Y	Y
IMO Name—ITunnelIGRE																												
Name	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		
IP Address	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									

Table 6-108 IP Attribute Support on Cisco Routers—Cisco ANA Version 3.7.1 (continued)

Attribute	800	1000	1600	1700	1800	2500	2600	2800	ISR2900	3600	3700	3800	ISR 3900	Cisco 4700	7200	7300	7400	7500	7600	10000	12000	XR 12000	CRS-1	ASR 1000	ASR 9000	MWR 2941	UBR7200	UBR10000
Keep Alive Retry															Y				Y									
IMO Name—IIPSLAResponderService																												
responderStatus																												
TWAMPResponderStatus																												
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 6-109 Routing Protocols Attribute Support on Cisco Routers—Cisco ANA Version 3.7.1

Attribute	800	1000	1600	1700	1800	2500	2600	2800	ISR2900	3600	3700	3800	ISR 3900	Cisco 4700	7200	7300	7400	7500	7600	10000	12000	XR 12000	CRS-1	ASR 1000	ASR 9000	MWR 2941	UBR7200	UBR10000
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
Neighbor Type				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
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
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

Table 6-109 Routing Protocols Attribute Support on Cisco Routers—Cisco ANA Version 3.7.1 (continued)

Attribute	800	1000	1600	1700	1800	2500	2600	2800	ISR2900	3600	3700	3800	ISR 3900	Cisco 4700	7200	7300	7400	7500	7600	10000	12000	XR 12000	CRS-1	ASR 1000	ASR 9000	MWR 2941	UBR7200	UBR10000
Peer AdminState												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
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
VrfName																						Y	Y			Y		
Address family													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
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
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
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
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
IMO Name—IospfProcess																												
Process Id													Y		Y				Y			Y						
OSPF Version													Y		Y				Y			Y						
Router Id													Y		Y				Y			Y						
IMO Name—IospfNeighbor																												
Neighbor Id													Y		Y				Y			Y						
Outgoing Interface													Y		Y				Y			Y						
State													Y		Y				Y			Y						
Neighbor Interface Address													Y		Y				Y			Y						
Area Id													Y		Y				Y			Y						
IMO Name—IospfInterface																												
Area Id													Y		Y				Y			Y						
Network Type													Y		Y				Y			Y						
Cost													Y		Y				Y			Y						
State													Y		Y				Y			Y						
Interface Address																									Y	Y		

Table 6-109 Routing Protocols Attribute Support on Cisco Routers—Cisco ANA Version 3.7.1 (continued)

Attribute	800	1000	1600	1700	1800	2500	2600	2800	ISR2900	3600	3700	3800	ISR 3900	Cisco 4700	7200	7300	7400	7500	7600	10000	12000	XR 12000	CRS-1	ASR 1000	ASR 9000	MWR 2941	UBR7200	UBR10000
Type													Y		Y				Y			Y						
IF Priority													Y		Y				Y			Y						
DR Id													Y		Y				Y			Y						
BDR Id													Y		Y				Y			Y						
IMO Name—IISpfTimers																												
Schedule Delay													Y		Y				Y			Y						
Min Hold Time													Y		Y				Y			Y						
Max Wait Time													Y		Y				Y			Y						
IMO Name—IISISProcess																												
ISIS Version																			Y			Y	Y		Y			
Manual Area Address																			Y			Y	Y		Y			
IS Type																			Y			Y	Y		Y			
System Id																			Y			Y	Y		Y			
Process Id																			Y			Y	Y		Y			
IMO Name—IISISMetric																												
IS Type																			Y			Y	Y		Y			
Metric Style																			Y			Y	Y		Y			
Metric Value																			Y			Y	Y		Y			
Address Family																			Y			Y	Y		Y			
IMO Name—IISISInterface																												
Interface Name																			Y			Y	Y		Y			
IMO Name—IISISNeighbor																												
IS Type																			Y			Y	Y		Y			
System Id																			Y			Y	Y		Y			
Admin State																			Y			Y	Y		Y			
Hold Time																			Y			Y	Y		Y			
SNPA																			Y			Y	Y		Y			

Table 6-109 Routing Protocols Attribute Support on Cisco Routers—Cisco ANA Version 3.7.1 (continued)

Attribute	800	1000	1600	1700	1800	2500	2600	2800	ISR2900	3600	3700	3800	ISR 3900	Cisco 4700	7200	7300	7400	7500	7600	10000	12000	XR 12000	CRS-1	ASR 1000	ASR 9000	MWR 2941	UBR7200	UBR10000
Interface Name																			Y			Y	Y		Y			
IP Address																			Y			Y	Y		Y			
Address Family																			Y			Y	Y		Y			

Ethernet

Table 6-110 Ethernet Attribute Support on Cisco Routers—Cisco ANA Version 3.7.1

Attribute	800	1000	1600	1700	1800	2500	2600	2800	ISR2900	3600	3700	3800	ISR 3900	Cisco 4700	7200	7300	7400	7500	7600	10000	12000	XR 12000	CRS-1	ASR 1000	ASR 9000	MWR 2941	UBR7200	UBR10000
IMO Name—ILinkAggregationGroup802dot3ad																												
dot3adAggMACAddress											Y		Y				Y ₁		Y		Y ₂	Y	Y		Y			
dot3adAggActorSystemPriority					Y						Y		Y				Y ₃		Y		Y ₄	Y	Y		Y			
dot3adAggActorSystemID											Y		Y				Y ₅		Y		Y ₆	Y	Y		Y			
dot3adAggActorAdminKey											Y		Y				Y ₇		Y		Y ₈	Y	Y		Y			
dot3adAggActorOperKey											Y		Y				Y ₉		Y		Y ₁₀	Y	Y		Y			
dot3adAggPartnerSystemID											Y		Y				Y ₁₁		Y		Y ₁₂	Y	Y		Y			
dot3adAggPartnerSystemPriority											Y		Y				Y ₁₃		Y		Y ₁₄	Y	Y		Y			
dot3adAggPartnerOperKey											Y		Y				Y ₁₅		Y		Y ₁₆	Y	Y		Y			
dot3adAggCollectorMaxDelay								Y			Y		Y				Y ₁₇		Y		Y ₁₈	Y	Y		Y			

Table 6-110 Ethernet Attribute Support on Cisco Routers—Cisco ANA Version 3.7.1 (continued)

Attribute	800	1000	1600	1700	1800	2500	2600	2800	ISR2900	3600	3700	3800	ISR 3900	Cisco 4700	7200	7300	7400	7500	7600	10000	12000	XR 12000	CRS-1	ASR 1000	ASR 9000	MWR 2941	UBR7200	UBR10000
GroupNumber											Y		Y				Y ¹⁹		Y		Y	Y	Y		Y			
AggregationProtocolType											Y		Y				Y ²⁰		Y		Y	Y	Y		Y			
MacAddress											Y		Y				Y ²¹		Y		Y	Y	Y		Y			
ChannelAdminStatus											Y		Y				Y ²²		Y		Y	Y	Y		Y			
ChannelOperStatus											Y		Y				Y ²³		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	
Duplex Mode																												
Output Flow Control																												
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									
isLOAMEnabled									Y				Y						Y						Y			
IMO Name—IVlanInterface																												
Mode																			Y							Y		
Native VLAN Identification				Y	Y																				Y			
Virtual LAN Table								Y																				
IANA Type				Y	Y							Y																
Containing CTPs																												
Contained CTPs																												
vlanAdminType																			Y		Y							

Table 6-110 Ethernet Attribute Support on Cisco Routers—Cisco ANA Version 3.7.1 (continued)

Attribute	800	1000	1600	1700	1800	2500	2600	2800	ISR2900	3600	3700	3800	ISR 3900	Cisco 4700	7200	7300	7400	7500	7600	10000	12000	XR 12000	CRS-1	ASR 1000	ASR 9000	MWR 2941	UBR7200	UBR10000
vlanencapType																			Y		Y							
getAccess																												
Allowed Vlans																			Y		Y							
IMO Name—IVlanEncapMux																												
IANA Type				Y	Y					Y									Y							Y		
Containing CTPs																												
Contained CTPs																												
IMO Name—IVlanMapping																												
direction													Y						Y									
vlanMatchCriteria													Y						Y									
vlanRewriteDefinition													Y						Y									
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
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
Containing CTPs																												
Contained CTPs																												
IMO Name—IStpService																												
StpProtocol	Y													Y			Y		Y						Y	Y		
StpMaxAge	Y											Y		Y			Y		Y				24			Y		
StpHelloTime	Y											Y		Y			Y		Y				25			Y		

Table 6-110 Ethernet Attribute Support on Cisco Routers—Cisco ANA Version 3.7.1 (continued)

Attribute	800	1000	1600	1700	1800	2500	2600	2800	ISR2900	3600	3700	3800	ISR 3900	Cisco 4700	7200	7300	7400	7500	7600	10000	12000	XR 12000	CRS-1	ASR 1000	ASR 9000	MWR 2941	UBR7200	UBR10000
StpBridgeForwardDelay	Y											Y		Y			Y		Y			²⁶			Y			
StpInstanceInfoTable	Y											Y		Y			Y		Y			²⁷		²⁸ Y	Y			
Same as ISystemService																												
StpUplinkFastState	Y											Y		Y			Y		Y							Y		
StpBackboneFastState	Y											Y		Y			Y		Y							Y		
StpForwardDelay	Y													Y			Y		Y					²⁹ Y	Y			
StpBridgeMaxAge	Y													Y			Y		Y					³⁰ Y	Y			
StpBridgeHelloTime	Y													Y			Y		Y					³¹ Y	Y			
IMO Name—IMstService																												
MstProperties																												
Same as IStpService																												
IMO Name—IPvstpService																												
UpLinkFast	Y													Y			Y		Y							Y		
BackboneFast	Y													Y			Y		Y							Y		
IMO Name—IMstProperties																												
MstForceVersion	Y													Y			Y		Y						Y	Y		
MstCfgIdFmtSel	Y													Y			Y		Y						Y	Y		
MstExternalRootCost	Y													Y			Y		Y						Y	Y		
MstMaxInstances	Y													Y			Y		Y						Y	Y		
MstCfgIdName	Y													Y			Y		Y							Y		
MstCfgIdRevLevel	Y													Y			Y		Y							Y		
IMO Name—IStpInstanceInfo																												
Object Identification																												
StpBridgeId	Y													Y			Y		Y							Y		

Table 6-110 Ethernet Attribute Support on Cisco Routers—Cisco ANA Version 3.7.1 (continued)

Attribute	800	1000	1600	1700	1800	2500	2600	2800	ISR2900	3600	3700	3800	ISR 3900	Cisco 4700	7200	7300	7400	7500	7600	10000	12000	XR 12000	CRS-1	ASR 1000	ASR 9000	MWR 2941	UBR7200	UBR10000
BridgePriority	Y													Y			Y		Y							Y		
Designated Parent and Root Bridges	Y											Y		Y			Y		Y						Y	Y		
StpRootCost	Y											Y		Y			Y		Y						Y	Y		
IsRoot	Y											Y		Y			Y		Y						Y	Y		
StpRootPort	Y											Y		Y			Y		Y						Y	Y		
StpPortInfoTable	Y													Y			Y		Y						Y	Y		
STP Instance Id	Y											Y		Y			Y		Y						Y	Y		
Vlan Id												Y													Y			
StpDesignatedBridge	Y													Y			Y		Y							Y		
StpDesignatedRoot	Y													Y			Y		Y							Y		
IMO Name—IMstInstanceInfo																												
MstVlanIds	Y													Y			Y		Y						Y	Y		
Same as IStpInstanceInfo	Y													Y			Y		Y						Y	Y		
IMO Name—IPvstpInstanceInfo																												
Protocol Type	Y											Y		Y			Y		Y							Y		
StpBridgeMaxAge	Y											Y		Y			Y		Y							Y		
StpBridgeHelloTime	Y											Y		Y			Y		Y							Y		
StpBridgeForwardDelay	Y											Y		Y			Y		Y							Y		
StpProtocolSpecification	Y													Y			Y		Y							Y		
StpVlanId	Y													Y			Y		Y							Y		
StpForwardDelay	Y													Y			Y		Y							Y		
StpMaxAge	Y													Y			Y		Y							Y		
IMO Name—IRstpInstanceInfo																												
StpForceVersion	Y													Y			Y		Y							Y		
Same as IStpInstanceInfo	Y													Y			Y		Y							Y		
IMO Name—IStpPortInfo																												
StpPort												Y		Y			Y		Y						Y	Y		

Table 6-110 Ethernet Attribute Support on Cisco Routers—Cisco ANA Version 3.7.1 (continued)

Attribute	800	1000	1600	1700	1800	2500	2600	2800	ISR2900	3600	3700	3800	ISR 3900	Cisco 4700	7200	7300	7400	7500	7600	10000	12000	XR 12000	CRS-1	ASR 1000	ASR 9000	MWR 2941	UBR7200	UBR10000
StpPortPriority												Y		Y			Y		Y					Y	Y			
StpPortState												Y		Y			Y		Y					Y	Y			
StpPortPathCost												Y		Y			Y		Y					Y	Y			
StpPortEdgePort												Y		Y			Y		Y					Y	Y			
StpPortPointToPoint												Y		Y			Y		Y					Y	Y			
StpPortRole												Y		Y			Y		Y					Y	Y			
StpDesignatedPortIdentifier														Y			Y		Y							Y		
StpDesignatedBridge														Y			Y		Y							Y		
StpPortIdentifier														Y			Y		Y							Y		
StpPortBpduGuardState														Y			Y		Y							Y		
StpPortBpduFilterState														Y			Y		Y							Y		
IMO Name—IMstPortInfo																												
MstPortHelloTime														Y			Y		Y						Y	Y ³²		
Same as IStpPortInfo														Y			Y		Y						Y	Y ³³		
IMO Name—IPvstpPortInfo																												
PvstpPortFastState														Y			Y		Y							Y ³⁴		
IMO Name—IEthernetChannel																												
Group Number	Y					Y	Y	Y	Y	Y	Y	Y			Y ³⁵		Y ³⁶		Y		Y	Y ³⁷	Y ³⁸	Y	Y			
Bandwidth	Y								Y	Y	Y	Y			Y ³⁹		Y ⁴⁰		Y		Y	Y ⁴¹	Y ⁴²	Y	Y			
Aggregation Protocol									Y	Y	Y	Y			Y ⁴³		Y ⁴⁴		Y		Y	Y ⁴⁵	Y ⁴⁶	Y	Y			
IANA Type	Y		Y	Y		Y	Y		Y	Y	Y	Y			Y ⁴⁷		Y ⁴⁸		Y	Y	Y	Y ⁴⁹	Y ⁵⁰	Y	Y			
Containing CTPs																												

Table 6-110 Ethernet Attribute Support on Cisco Routers—Cisco ANA Version 3.7.1 (continued)

Attribute	800	1000	1600	1700	1800	2500	2600	2800	ISR2900	3600	3700	3800	ISR 3900	Cisco 4700	7200	7300	7400	7500	7600	10000	12000	XR 12000	CRS-1	ASR 1000	ASR 9000	MWR 2941	UBR7200	UBR10000
Contained CTPs																												
Mac Address															Y ⁵¹				Y				Y					
Admin Status															Y ⁵²				Y				Y					
Oper Status															Y ⁵³				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						Y					Y						⁵⁴			
OperatingMode					Y			Y						Y					Y						⁵⁵			
DomainName					Y			Y						Y					Y						⁵⁶			
ConfigurationRevision					Y			Y						Y					Y						⁵⁷			
isPruningEnabled					Y			Y						Y					Y						⁵⁸			
isAuthenticationEnabled					Y			Y						Y					Y						⁵⁹			
IMO Name—IREPService																												
version																			Y							Y ⁶⁰		
administrativeVlan																			Y							Y ⁶¹		
notificationEnabled																			Y							Y ⁶²		

Table 6-110 Ethernet Attribute Support on Cisco Routers—Cisco ANA Version 3.7.1 (continued)

Attribute	800	1000	1600	1700	1800	2500	2600	2800	ISR2900	3600	3700	3800	ISR 3900	Cisco 4700	7200	7300	7400	7500	7600	10000	12000	XR 12000	CRS-1	ASR 1000	ASR 9000	MWR 2941	UBR7200	UBR10000
IMO Name—IREPSegmentInfo																												
segmentId																			Y							Y ⁶³		
segmentComplete																			Y							Y ⁶⁴		
IMO Name—IREPPortInfo																												
portName																			Y							Y ⁶⁵		
portKey																			Y							Y ⁶⁶		
segmentId																			Y							Y ⁶⁷		
portType																			Y							Y ⁶⁸		
portRole																			Y							Y ⁶⁹		
operStatus																			Y							Y ⁷⁰		
blockedVlans																			Y							Y ⁷¹		
preemptTimer																			Y							Y ⁷²		
lslAgeoutTimer																			Y							Y ⁷³		
remoteDeviceName																			Y							Y ⁷⁴		
remoteDeviceMac																			Y							Y ⁷⁵		
remotePortName																			Y							Y ⁷⁶		

Table 6-110 Ethernet Attribute Support on Cisco Routers—Cisco ANA Version 3.7.1 (continued)

Attribute	800	1000	1600	1700	1800	2500	2600	2800	ISR2900	3600	3700	3800	ISR 3900	Cisco 4700	7200	7300	7400	7500	7600	10000	12000	XR 12000	CRS-1	ASR 1000	ASR 9000	MWR 2941	UBR7200	UBR10000
IMO Name—IIBridgeLan																												
Id																								Y				
IMO Name—IIBBridgeEntry																												
IS Id																								Y				
IBridge																								Y				
BBridge																								Y				

^{1, 2, 3, 4, 5, 6, 7}Supported 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, 25}Supported in IOS versions 12.2(33)SRD1 and 12.2(40)T only.

^{26, 27, 28, 29, 30, 31, 32, 33, 34}LAG is not supported for 12.0(33)S1

^{35, 36, 37, 38}Added show lacp bundle from ANA 3.6.3.1

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, 47}Array of Spanning Tree Protocol Bridge information

^{43, 44, 45, 46}SNMP supported with ANA 3.6.0. The `show lacp bundle` command is supported with ANA 3.6.3 and later.

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, 56}The MIB provides data by default, but the device does not support VTP.

^{57, 58, 59}Supported only for 12.2(33)MRA

^{60, 61, 62, 63, 64, 65, 66, 67, 68, 69, 70, 71, 72, 73, 74, 75, 76}REP Supported only on IOS 12.2(33)MRA(CSR 3.2)

ATM

Table 6-111 *ATM Attribute Support on Cisco Routers—Cisco ANA Version 3.7.1*

Attribute	800	1000	1600	1700	1800	2500	2600	2800	ISR2900	3600	3700	3800	ISR 3900	Cisco 4700	7200	7300	7400	7500	7600	10000	12000	XR 12000	CRS-1	ASR 1000	ASR 9000	MWR 2941	UBR7200	UBR10000
IMO Name—IATm																												
ATM Address			Y	Y	Y	Y	Y				Y		Y	Y	Y	Y	Y	Y	Y					Y		Y	Y	
Interface Type															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	
Cross-Connect Table																												
IANA Type		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	
Tx Maximum Bandwidth													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	
Tx CBR Allocated Bandwidth													Y	Y	Y	Y		Y	Y		Y			Y		Y	Y	
Rx Allocated Bandwidth													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	
Rx UBR Allocated Bandwidth													Y	Y	Y	Y		Y	Y		Y			Y		Y	Y	
Rx CBR Allocated Bandwidth													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	
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	
Shaping Profile																												

Table 6-111 ATM Attribute Support on Cisco Routers—Cisco ANA Version 3.7.1 (continued)

Attribute	800	1000	1600	1700	1800	2500	2600	2800	ISR2900	3600	3700	3800	ISR 3900	Cisco 4700	7200	7300	7400	7500	7600	10000	12000	XR 12000	CRS-1	ASR 1000	ASR 9000	MWR 2941	UBR7200	UBR10000
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	
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	
Ingress Traffic Descriptor	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	
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	
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	
IANA Type	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	
Service Category			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	
Cell Delay Variation								Y																				
Cell Delay Variation Tolerance			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	
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	
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	
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	
Name																												
Index				Y									Y	Y		Y		Y	Y	Y	Y	Y		Y		Y		

Table 6-111 **ATM Attribute Support on Cisco Routers—Cisco ANA Version 3.7.1 (continued)**

Attribute	800	1000	1600	1700	1800	2500	2600	2800	ISR2900	3600	3700	3800	ISR 3900	Cisco 4700	7200	7300	7400	7500	7600	10000	12000	XR 12000	CRS-1	ASR 1000	ASR 9000	MWR 2941	UBR7200	UBR10000
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													Y	Y	Y				Y			Y				Y		
crossConnectTableSize													Y		Y				Y			Y				Y		

Table 6-111 ATM Attribute Support on Cisco Routers—Cisco ANA Version 3.7.1 (continued)

Attribute	800	1000	1600	1700	1800	2500	2600	2800	ISR2900	3600	3700	3800	ISR 3900	Cisco 4700	7200	7300	7400	7500	7600	10000	12000	XR 12000	CRS-1	ASR 1000	ASR 9000	MWR 2941	UBR7200	UBR10000
Logical Sons																					Y							
IMO Name—IIMAGroup																												
AdminStatus													Y		Y				Y							Y		
OperStatus													Y		Y				Y							Y		
GroupNumber													Y		Y				Y							Y		
ImaVersion													Y		Y				Y							Y		
Speed													Y		Y				Y							Y		
ConfiguredBandwidth													Y		Y				Y							Y		
NumberOfLinks													Y		Y				Y							Y		
NumberOfActiveLinks													Y		Y				Y							Y		
MinimumNumberOfTxLinks													Y		Y				Y							Y		
MinimumNumberOfRxLinks													Y		Y				Y							Y		
ClockMode													Y		Y				Y							Y		
FrameLength													Y		Y				Y							Y		
interfaceName													Y		Y				Y							Y		
groupStatus													Y		Y				Y							Y		

Frame Relay

Table 6-112 Frame Relay Attribute Support on Cisco Routers—Cisco ANA Version 3.7.1

Attribute	800	1000	1600	1700	1800	2500	2600	2800	ISR2900	3600	3700	3800	ISR 3900	Cisco 4700	7200	7300	7400	7500	7600	10000	12000	XR 12000	CRS-1	ASR 1000	ASR 9000	MWR 2941	UBR7200	UBR10000
IMO Name—Iframerelay/IfrTrunk																												
Protocol Type		Y									Y			Y		Y		Y	Y	Y			Y			Y		

Table 6-112 **Frame Relay Attribute Support on Cisco Routers—Cisco ANA Version 3.7.1 (continued)**

Attribute	800	1000	1600	1700	1800	2500	2600	2800	ISR2900	3600	3700	3800	ISR 3900	Cisco 4700	7200	7300	7400	7500	7600	10000	12000	XR 12000	CRS-1	ASR 1000	ASR 9000	MWR 2941	UBR7200	UBR10000
VC Table		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	
Traffic Descriptor		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	
Egress Traffic Descriptor		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	
Operational Status		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																												
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	
Excess Burst Rate		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															Y												Y	
Oper Status															Y												Y	

Table 6-112 Frame Relay Attribute Support on Cisco Routers—Cisco ANA Version 3.7.1 (continued)

Attribute	800	1000	1600	1700	1800	2500	2600	2800	ISR2900	3600	3700	3800	ISR 3900	Cisco 4700	7200	7300	7400	7500	7600	10000	12000	XR 12000	CRS-1	ASR 1000	ASR 9000	MWR 2941	UBR7200	UBR10000
Same as IFrameRelay																	Y			Y								
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—Iframerelay/IfrTrunk																												
Protocol Type	Y																											
VC Table	Y																											
Cross-Connect Table																												
IANA Type																												
Containing CTPs																												
Contained CTPs																												

PPP

Table 6-113 PPP Attribute Support on Cisco Routers—Cisco ANA Version 3.7.1

Attribute	800	1000	1600	1700	1800	2500	2600	2800	ISR2900	3600	3700	3800	ISR 3900	Cisco 4700	7200	7300	7400	7500	7600	10000	12000	XR 12000	CRS-1	ASR 1000	ASR 9000	MWR 2941	UBR7200	UBR10000
IMO Name—IVcBasedEncapsulation																												
Virtual Connection								Y														Y						
Binding Information				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	
IANA Type		Y	Y	Y	Y		Y			Y	Y		Y	Y	Y		Y		Y	Y	Y	Y				Y	Y	
Containing CTPs																						Y						

Table 6-113 *PPP Attribute Support on Cisco Routers—Cisco ANA Version 3.7.1 (continued)*

Attribute	800	1000	1600	1700	1800	2500	2600	2800	ISR2900	3600	3700	3800	ISR 3900	Cisco 4700	7200	7300	7400	7500	7600	10000	12000	XR 12000	CRS-1	ASR 1000	ASR 9000	MWR 2941	UBR7200	UBR10000
Contained CTPs																					Y							
IMO Name—IMLPPP																												
InterfaceName															Y				Y	Y	Y	Y				Y		
GroupNumber															Y				Y	Y	Y	Y				Y		
MTU															Y				Y	Y	Y	Y				Y		
FragmentDelay															Y				Y	Y	Y					Y		
FragmentDisable															Y				Y	Y	Y	Y				Y		
FragmentMaximum															Y				Y	Y	Y					Y		
FragmentSize															Y				Y	Y	Y					Y		
Interleave															Y				Y	Y	Y	Y				Y		
Keepalive															Y				Y	Y	Y	Y				Y		
KeepaliveTime															Y				Y	Y	Y	Y				Y		
KeepaliveRetry															Y				Y	Y	Y					Y		
ActiveLink															Y				Y	Y	Y	Y				Y		
MinimumConfiguredLink															Y				Y	Y	Y					Y		
MaximumConfiguredLink															Y				Y	Y	Y					Y		
LocalMRRU															Y				Y	Y	Y	Y				Y		
RemoteMRRU															Y				Y	Y	Y	Y				Y		
LoadThreshold															Y				Y	Y	Y					Y		
LCPSStatus															Y				Y	Y	Y	Y				Y		
AdminStatus															Y				Y	Y	Y	Y				Y		
OperStatus															Y				Y	Y	Y	Y				Y		

HDLC

Table 6-114 HDLC Attribute Support on Cisco Routers—Cisco ANA Version 3.7.1

Attribute	800	1000	1600	1700	1800	2500	2600	2800	ISR2900	3600	3700	3800	ISR 3900	Cisco 4700	7200	7300	7400	7500	7600	10000	12000	XR 12000	CRS-1	ASR 1000	ASR 9000	MWR 2941	UBR7200	UBR10000
IMO Name—Iencapsulation (HDLC/PPP)																												
Virtual Connection		Y	Y					Y				Y		Y	Y	Y	Y	Y	Y	Y						Y ¹		
Binding Information								Y				Y		Y	Y		Y	Y								Y ²		
Binding Status		Y	Y	Y	Y		Y	Y				Y		Y	Y	Y	Y	Y	Y	Y	Y	Y				Y ³		
IANA Type		Y	Y	Y	Y		Y							Y		Y		Y	Y	Y						Y ⁴		
Containing CTPs																												
Contained CTPs																												
IMO Name—IEncapsulation (HDLC/PPP)																												
Virtual Connection	Y																											
Binding Information	Y																											
Binding Status	Y																											
IANA Type	Y																											
Containing CTPs																												
Contained CTPs																												

^{1, 2, 3, 4}HDLC is not supported

SONET/SDH

Table 6-115 SONET/SDH Attribute Support on Cisco Routers—Cisco ANA Version 3.7.1

Attribute	800	1000	1600	1700	1800	2500	2600	2800	ISR2900	3600	3700	3800	ISR 3900	Cisco 4700	7200	7300	7400	7500	7600	10000	12000	XR 12000	CRS-1	ASR 1000	ASR 9000	MWR 2941	UBR7200	UBR10000
IMO Name—IsonetSdh																												
Specific Type																												

Table 6-115 SONET/SDH Attribute Support on Cisco Routers—Cisco ANA Version 3.7.1 (continued)

Attribute	800	1000	1600	1700	1800	2500	2600	2800	ISR2900	3600	3700	3800	ISR 3900	Cisco 4700	7200	7300	7400	7500	7600	10000	12000	XR 12000	CRS-1	ASR 1000	ASR 9000	MWR 2941	UBR7200	UBR10000
Loopback Type						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					
Same as IPPhysicalLayer																Y		Y										
TCAThresholdB1																						Y	Y					
TCAThresholdB2																						Y	Y					
TCAThresholdB3																						Y	Y					
clocking																						Y	Y					
IMO Name—IDS1PdhChannelized																												
Au4Number															Y				Y	Y	Y							
Au3Number															Y				Y	Y	Y							
Sts1Number																			Y	Y	Y	Y						
Tug3Number															Y				Y	Y	Y							
Tug2Number															Y				Y	Y	Y							
VtNumber																			Y	Y	Y	Y						
C11Number																			Y	Y	Y							
C12Number															Y				Y	Y	Y							
Vt15Number																			Y	Y	Y	Y						
Vt2Number																			Y	Y	Y							
T1Number															Y				Y	Y	Y	Y						
E1Number															Y				Y	Y	Y	Y						
PathType															Y				Y	Y	Y	Y						
Description															Y				Y	Y	Y	Y						
IMO Name—ISonetSdhHop																												
Description															Y				Y	Y	Y	Y						
AppliqueType															Y				Y	Y	Y	Y						
PathType															Y				Y	Y	Y	Y						

Table 6-115 SONET/SDH Attribute Support on Cisco Routers—Cisco ANA Version 3.7.1 (continued)

Attribute	800	1000	1600	1700	1800	2500	2600	2800	ISR2900	3600	3700	3800	ISR 3900	Cisco 4700	7200	7300	7400	7500	7600	10000	12000	XR 12000	CRS-1	ASR 1000	ASR 9000	MWR 2941	UBR7200	UBR10000
IMO Name—ISonetSts1																												
Sts1Number																			Y	Y	Y	Y						
IMO Name—ISdhAu4																												
Au4Number															Y				Y	Y	Y							
IMO Name—ISdhAu3																												
Au3Number															Y				Y	Y	Y							

TDM/DSx

Table 6-116 TDM/DSx Attribute Support on Cisco Routers—Cisco ANA Version 3.7.1

Attribute	800	1000	1600	1700	1800	2500	2600	2800	ISR2900	3600	3700	3800	ISR 3900	Cisco 4700	7200	7300	7400	7500	7600	10000	12000	XR 12000	CRS-1	ASR 1000	ASR 9000	MWR 2941	UBR7200	UBR10000
IMO Name—IDS0Bundle																												
Bundled Time Slots	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						
IANA Type	Y	Y	Y	Y	Y			Y				Y	Y	Y					Y			Y						
Containing CTPs																												
Contained CTPs																												
AdminStatus													Y	Y	Y				Y			Y						
OperStatus													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	Y	Y ¹		Y		Y	Y	Y			Y		Y ²		
Same as IPhysicalLayer																												

Table 6-116 TDM/DSx Attribute Support on Cisco Routers—Cisco ANA Version 3.7.1 (continued)

Attribute	800	1000	1600	1700	1800	2500	2600	2800	ISR2900	3600	3700	3800	ISR 3900	Cisco 4700	7200	7300	7400	7500	7600	10000	12000	XR 12000	CRS-1	ASR 1000	ASR 9000	MWR 2941	UBR7200	UBR10000
portDescription					Y			Y					Y	Y	Y				Y			Y	Y			Y ³		
internationalBit					Y			Y					Y	Y					Y							Y ⁴		
nationalBits					Y			Y					Y	Y					Y							Y ⁵		
framing					Y			Y					Y	Y	Y				Y							Y ⁶		
lineCode					Y			Y					Y	Y	Y ⁷				Y							Y ⁸		
cableLength					Y			Y					Y	Y	Y ⁹				Y							Y ¹⁰		
recoveredClockingId					Y								Y	Y	Y ¹¹				Y							Y ¹²		
clocking					Y			Y					Y	Y	Y				Y			Y	Y			Y ¹³		
loopback					Y			Y					Y	Y	Y				Y							Y ¹⁴		
alarmState					Y								Y	Y	Y ¹⁵				Y			Y				Y ¹⁶		
IMO Name—IClockService																												
ActiveClockSource																			Y							Y		
NcsMode																			Y							Y		
HoldTimeout																			Y							Y		
UseStratum4																			Y							Y		
Mode																			Y							Y		
NcsPriorityList																			Y							Y		
PtpService																			Y							Y		
IMO Name—IClockSource																												
Priority																			Y							Y		
Source																			Y							Y		
Status																			Y							Y		
Type																			Y							Y		

Table 6-116 TDM/DSx Attribute Support on Cisco Routers—Cisco ANA Version 3.7.1 (continued)

Attribute	800	1000	1600	1700	1800	2500	2600	2800	ISR2900	3600	3700	3800	ISR 3900	Cisco 4700	7200	7300	7400	7500	7600	10000	12000	XR 12000	CRS-1	ASR 1000	ASR 9000	MWR 2941	UBR7200	UBR10000
IMO Name—IPtpService																												
Mode																										Y		
ClockId																										Y		
Domain																										Y		
Priority1																										Y		
Priority2																										Y		
PtpEnabled																										Y		
PtpInterfaceList																										Y		
IMO Name—IPtpInterface																												
Version																										Y		
AnnounceInterval																										Y		
AnnounceTimeout																										Y		
DestinationAddress																										Y		
SourceAddress																										Y		
DelayReq																										Y		
MasterMode																										Y		
SlaveMode																										Y		
SyncInterval																										Y		
SyncLimit																										Y		
InterfaceXid																										Y		
IMO Name—IACRService																												
RecoveredClockSource																			Y							Y		
RecoveredClockMode																			Y							Y		
CemInterface																			Y							Y		
RecoveredClockList																			Y							Y		
IMO Name—IRecoveredClock																												
ClockId																			Y							Y		

Table 6-116 TDM/DSx Attribute Support on Cisco Routers—Cisco ANA Version 3.7.1 (continued)

Attribute	800	1000	1600	1700	1800	2500	2600	2800	ISR2900	3600	3700	3800	ISR 3900	Cisco 4700	7200	7300	7400	7500	7600	10000	12000	XR 12000	CRS-1	ASR 1000	ASR 9000	MWR 2941	UBR7200	UBR10000
RecoveredClockMode																			Y							Y		
Port																			Y							Y		
Cem																			Y							Y		
Status																			Y							Y		
FrequencyOffset																			Y							Y		
IMO Name—ICEMEncap																												
cemIfName																			Y					Y		Y		
IMO Name—ICEMGroup																												
IdlePattern																			Y					Y		Y		
IdleCAS																			Y					Y		Y		
DeJitter																			Y					Y		Y		
PayloadSize																			Y					Y		Y		
RTP																			Y					Y		Y		
RTPHeader																			Y					Y		Y		
TimeSlots																			Y					Y		Y		
AdminStatus																			Y					Y		Y		
OperStatus																			Y					Y		Y		
IMO Name—ISyncE																												
synchronousMode																			Y									
equipmentClock																			Y									
clockMode																			Y									
ssmOption																			Y									
esmcMode																			Y									
holdOffTimer																			Y									
waitToRestore																			Y									
Revertive																			Y									

Table 6-116 TDM/DSx Attribute Support on Cisco Routers—Cisco ANA Version 3.7.1 (continued)

Attribute	800	1000	1600	1700	1800	2500	2600	2800	ISR2900	3600	3700	3800	ISR 3900	Cisco 4700	7200	7300	7400	7500	7600	10000	12000	XR 12000	CRS-1	ASR 1000	ASR 9000	MWR 2941	UBR7200	UBR10000
IMO Name—ISyncEInterface																												
selectionInput																			Y									
ingressESMCMode																			Y									
egressESMCMode																			Y									
ingressQLMode																			Y									
ingressQuality																			Y									
egressQLMode																			Y									
egressQuality																			Y									
waitToRestore																			Y									
holdOffTimer																			Y									

1, 2, 3, 4, 5Supported only for DS1

6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16Not Supported on IOS 12.2(33)MRA (CSR3.2)

MPLS

Table 6-117 MPLS Attribute Support on Cisco Routers—Cisco ANA Version 3.7.1

Attribute	800	1000	1600	1700	1800	2500	2600	2800	ISR2900	3600	3700	3800	ISR 3900	Cisco 4700	7200	7300	7400	7500	7600	10000	12000	XR 12000	CRS-1	ASR 1000	ASR 9000	MWR 2941	UBR7200	UBR10000
IMO Name—IMpls																												
Distribution Protocol										Y	Y	Y			Y		Y		Y	Y	Y	Y	Y	Y	Y	Y	Y	Y
Outer and Inner Labels																						Y	Y		Y			
Traffic Engineering Properties										Y	Y			Y	Y		Y		Y	Y	Y			Y		Y		
Resource reservation Properties																												

Table 6-117 MPLS Attribute Support on Cisco Routers—Cisco ANA Version 3.7.1 (continued)

Attribute	800	1000	1600	1700	1800	2500	2600	2800	ISR2900	3600	3700	3800	ISR 3900	Cisco 4700	7200	7300	7400	7500	7600	10000	12000	XR 12000	CRS-1	ASR 1000	ASR 9000	MWR 2941	UBR7200	UBR10000
IANA Type										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
MPLS Aggregate Table											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	
LDP Service														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—ILdpService																												
Local Identification Status														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
IMO Name—ILdpPeer																												
Peer Identification										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
Distribution Method										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
Path Vector Limit											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
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
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
IMO Name—ILdpDiscoverySource																												
Interface Name										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
Type										Y	Y			Y	Y		Y		Y	Y	Y	Y	Y	Y	Y	Y	Y	Y

Table 6-117 MPLS Attribute Support on Cisco Routers—Cisco ANA Version 3.7.1 (continued)

Attribute	800	1000	1600	1700	1800	2500	2600	2800	ISR2900	3600	3700	3800	ISR 3900	Cisco 4700	7200	7300	7400	7500	7600	10000	12000	XR 12000	CRS-1	ASR 1000	ASR 9000	MWR 2941	UBR7200	UBR10000
IMO Name—IMplsEntry																												
Incoming Label										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
Switching Action										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
Destination Mask										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
IMO Name—IMplsAggregateEntry																												
Virtual Routing Entity										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
Outgoing Interface and Label										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
Next Hop IP Address										Y	Y			Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y

MPLS-TE

Table 6-118 MPLS-TE Attribute Support on Cisco Routers—Cisco ANA Version 3.7.1

Attribute	800	1000	1600	1700	1800	2500	2600	2800	ISR2900	3600	3700	3800	ISR 3900	Cisco 4700	7200	7300	7400	7500	7600	10000	12000	XR 12000	CRS-1	ASR 1000	ASR 9000	MWR 2941	UBR7200	UBR10000
IMO Name—IMplsTETunnel																												
Destination Address										Y	Y	Y		Y	Y		Y		Y	Y	Y	Y	Y	Y	Y	Y ¹		
Outgoing Interface and Label										Y	Y	Y		Y	Y		Y		Y	Y	Y	Y	Y	Y	Y	Y ²		
LSP Identification										Y	Y	Y		Y	Y		Y		Y	Y	Y	Y	Y	Y	Y	Y ³		

Table 6-118 MPLS-TE Attribute Support on Cisco Routers—Cisco ANA Version 3.7.1 (continued)

Attribute	800	1000	1600	1700	1800	2500	2600	2800	ISR2900	3600	3700	3800	ISR 3900	Cisco 4700	7200	7300	7400	7500	7600	10000	12000	XR 12000	CRS-1	ASR 1000	ASR 9000	MWR 2941	UBR7200	UBR10000
Requested Bandwidth										Y	Y	Y		Y	Y		Y		Y	Y	Y	Y	Y	Y	Y	Y ⁴		
Measured Average Burst and Peak Bandwidth										Y	Y	Y		Y	Y		Y		Y	Y	Y	Y	Y	Y	Y	Y ⁵		
Setup and Hold Priority										Y	Y	Y		Y	Y		Y		Y	Y	Y	Y	Y	Y	Y	Y ⁶		
Affinity Bits and Mask										Y	Y	Y		Y	Y		Y		Y	Y	Y	Y	Y	Y	Y	Y ⁷		
Automatic Route Announcement Status										Y	Y	Y		Y	Y		Y		Y	Y	Y	Y	Y	Y	Y	Y ⁸		
Optimization Lock Down Status										Y	Y	Y		Y	Y		Y		Y	Y	Y	Y	Y	Y	Y	Y ⁹		
Path Option										Y	Y	Y		Y	Y		Y		Y	Y	Y	Y	Y	Y	Y	Y ¹⁰		
Name										Y	Y	Y		Y	Y		Y		Y	Y	Y	Y	Y	Y	Y	Y ¹¹		
Description										Y	Y	Y		Y	Y		Y		Y	Y	Y	Y	Y	Y	Y	Y ¹²		
Administrative Status										Y	Y	Y		Y	Y		Y		Y	Y	Y	Y	Y	Y	Y	Y ¹³		
Operational Status										Y	Y	Y		Y	Y		Y		Y	Y	Y	Y	Y	Y	Y	Y ¹⁴		
IANA Type										Y	Y	Y		Y	Y		Y		Y	Y	Y	Y	Y	Y	Y	Y ¹⁵		
is FRR Enabled										Y	Y	Y		Y	Y		Y		Y	Y	Y	Y	Y	Y	Y	Y ¹⁶		
IMO Name—IMplsTEProperties																												
Administrative Weight										Y	Y			Y	Y		Y		Y	Y	Y	Y ¹⁷	Y ¹⁸	Y	Y	Y ¹⁹		
Attributes Identifier																						Y ²⁰	Y ²¹		Y			
Signaling Protocol										Y	Y	Y		Y	Y		Y		Y	Y	Y	Y ²²	Y ²³	Y	Y	Y ²⁴		

Table 6-118 MPLS-TE Attribute Support on Cisco Routers—Cisco ANA Version 3.7.1 (continued)

Attribute	800	1000	1600	1700	1800	2500	2600	2800	ISR2900	3600	3700	3800	ISR 3900	Cisco 4700	7200	7300	7400	7500	7600	10000	12000	XR 12000	CRS-1	ASR 1000	ASR 9000	MWR 2941	UBR7200	UBR10000
Available Physical and Reservable Bandwidth										Y	Y	Y		Y	Y		Y		Y	Y	Y	Y ² ₅	Y ² ₆	Y	Y	Y ² ₇		
Reserved Bandwidth										Y	Y	Y		Y	Y		Y		Y	Y	Y	Y ² ₈	Y ² ₉	Y	Y	Y ³ ₀		
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	Y ³ ₁		
Measured Average Burst and Peak Bandwidth										Y	Y			Y	Y		Y		Y	Y	Y	Y	Y	Y	Y	Y ³ ₂		
LSP Identification										Y	Y			Y	Y		Y		Y	Y	Y	Y	Y	Y	Y	Y ³ ₃		
Name										Y	Y			Y	Y		Y		Y	Y	Y	Y	Y	Y	Y	Y ³ ₄		
FRRTunnelName										Y	Y	Y		Y	Y		Y		Y	Y	Y	Y	Y	Y	Y	Y ³ ₅		
FRRTunnelState										Y	Y	Y		Y	Y		Y		Y	Y	Y	Y	Y	Y	Y	Y ³ ₆		
AverageBandwidth										Y	Y			Y	Y		Y		Y	Y	Y	Y	Y	Y	Y	Y ³ ₇		
In Interface										Y	Y			Y	Y		Y		Y	Y	Y	Y	Y	Y	Y	Y ³ ₈		
Out interface										Y	Y			Y	Y		Y		Y	Y	Y	Y	Y	Y	Y	Y ³ ₉		
In Label										Y	Y			Y	Y		Y		Y	Y	Y	Y	Y	Y	Y	Y ⁴ ₀		
Out Label										Y	Y			Y	Y		Y		Y	Y	Y	Y	Y	Y	Y	Y ⁴ ₁		

Table 6-118 MPLS-TE Attribute Support on Cisco Routers—Cisco ANA Version 3.7.1 (continued)

Attribute	800	1000	1600	1700	1800	2500	2600	2800	ISR2900	3600	3700	3800	ISR 3900	Cisco 4700	7200	7300	7400	7500	7600	10000	12000	XR 12000	CRS-1	ASR 1000	ASR 9000	MWR 2941	UBR7200	UBR10000
Source address										Y	Y			Y	Y		Y		Y	Y	Y	Y	Y	Y	Y	Y ⁴ ₂		
Destination address										Y	Y			Y	Y		Y		Y	Y	Y	Y	Y	Y	Y	Y ⁴ ₃		

^{1, 2, 3, 4, 5, 7, 8, 9, 10}ANA 3.6.2 and earlier: show mpls traffic-eng link-management bandwidth-allocation \$telnetString\$. ANA 3.6.3 and later: show mpls traffic-eng link-management bandwidth-allocation interface \$telnetString\$.

⁶Till ANA 3.6.2 - show mpls traffic-eng link-management bandwidth-allocation \$telnetString\$ From ANA 3.6.3 - show mpls traffic-eng link-management bandwidth-allocation interface \$telnetString\$ For ANA 3.6.6(XR 3.8.0) -show mpls traffic-eng link-management interfaces \$telnetString\$(Administrative weight) First Registration Name for XR version less than 3.8.0 and second one is for XR version 3.8.0. Same for query too.

^{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}Not Supported in IOS 12.2(33)MRA (CSR3.2)

VPN (VRF)

Table 6-119 VPN (VRF) Attribute Support on Cisco Routers—Cisco ANA Version 3.7.1

Attribute	800	1000	1600	1700	1800	2500	2600	2800	ISR2900	3600	3700	3800	ISR 3900	Cisco 4700	7200	7300	7400	7500	7600	10000	12000	XR 12000	CRS-1	ASR 1000	ASR 9000	MWR 2941	UBR7200	UBR10000
IMO Name—IVrf																												
Virtual Routing Table														Y	Y		Y		Y	Y			Y	Y	Y	Y	Y	Y
Exported Route Targets												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
Route Distinguisher										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
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
Description											Y	Y		Y	Y		Y		Y	Y	Y	Y	Y	Y	Y	Y	Y	Y
Import Route-Map											Y	Y		Y	Y		Y		Y	Y	Y	Y	Y	Y	Y	Y	Y	Y
Export Route-Map											Y	Y		Y	Y		Y		Y	Y	Y	Y	Y	Y	Y	Y	Y	Y

Table 6-119 VPN (VRF) Attribute Support on Cisco Routers—Cisco ANA Version 3.7.1 (continued)

Attribute	800	1000	1600	1700	1800	2500	2600	2800	ISR2900	3600	3700	3800	ISR 3900	Cisco 4700	7200	7300	7400	7500	7600	10000	12000	XR 12000	CRS-1	ASR 1000	ASR 9000	MWR 2941	UBR7200	UBR10000
IMO Name—IVrfEntry																												
Next Hop BGP Address										Y	Y	Y		Y	Y		Y		Y	Y	Y	Y	Y	Y	Y	Y	Y	Y
Incoming and Outgoing Inner Label										Y	Y	Y		Y	Y		Y		Y	Y	Y	Y	Y	Y	Y	Y	Y	Y
Outer Label										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
Next Hop IP Address										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
Routing Protocol Type										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
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
Local Autonomous System					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
BGP Neighbors					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
IMO Name—ICrossVrf																												
Virtual Routing Entries														Y	Y		Y		Y	Y	Y	Y	Y	Y	Y	Y	Y	
Virtual Routing Entity Name														Y	Y		Y		Y	Y	Y	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
Next Hop IP Address										Y	Y				Y		Y		Y	Y	Y			Y		Y	Y	Y
Type										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

Table 6-119 VPN (VRF) Attribute Support on Cisco Routers—Cisco ANA Version 3.7.1 (continued)

Attribute	800	1000	1600	1700	1800	2500	2600	2800	ISR2900	3600	3700	3800	ISR 3900	Cisco 4700	7200	7300	7400	7500	7600	10000	12000	XR 12000	CRS-1	ASR 1000	ASR 9000	MWR 2941	UBR7200	UBR10000
Outgoing Interface Name																												

PWE3

Table 6-120 PWE3 Attribute Support on Cisco Routers—Cisco ANA Version 3.7.1

Attribute	800	1000	1600	1700	1800	2500	2600	2800	ISR2900	3600	3700	3800	ISR 3900	Cisco 4700	7200	7300	7400	7500	7600	10000	12000	XR 12000	CRS-1	ASR 1000	ASR 9000	MWR 2941	UBR7200	UBR10000
IMO Name—IPTPLayer2MplsTunnel																												
Local and Remote Router Addresses										Y	Y	Y		Y	Y		Y		Y	Y	Y	Y ¹	Y ²	Y	Y	Y ³		
Local and Remote Virtual Connection Labels										Y	Y			Y	Y		Y		Y	Y	Y	Y ⁴	Y ⁵	Y	Y	Y ⁶		
Tunnel Identification										Y	Y	Y		Y	Y		Y		Y	Y	Y	Y ⁷	Y ⁸	Y	Y	Y ⁹		
Tunnel Status										Y	Y	Y		Y	Y		Y		Y	Y	Y	Y ¹ ₀	Y ¹ ₁	Y	Y	Y ¹ ₂		
Local and Remote Tunnel Interface												Y										Y ¹ ₃						
IANA Type										Y	Y			Y	Y		Y		Y	Y	Y	Y ¹ ₄	Y	Y	Y	Y ¹ ₅		
Containing CTPs																												
Contained CTPs																												
PsuedowireType														Y	Y				Y		Y	Y	Y	Y	Y	Y ¹ ₆		
PreferredPathTunnel														Y	Y				Y		Y	Y	Y	Y	Y	Y ¹ ₇		
LocalMTU														Y	Y				Y		Y	Y	Y	Y	Y	Y ¹ ₈		

Table 6-120 PWE3 Attribute Support on Cisco Routers—Cisco ANA Version 3.7.1 (continued)

Attribute	800	1000	1600	1700	1800	2500	2600	2800	ISR2900	3600	3700	3800	ISR 3900	Cisco 4700	7200	7300	7400	7500	7600	10000	12000	XR 12000	CRS-1	ASR 1000	ASR 9000	MWR 2941	UBR7200	UBR10000
RemoteMTU														Y	Y				Y		Y	Y	Y	Y	Y	Y ¹ ₉		
PeerStatus														Y	Y				Y		Y	Y	Y	Y	Y	Y ² ₀		
SignalingProtocol														Y	Y				Y		Y	Y	Y	Y	Y	Y ² ₁		
VFIName														Y	Y				Y		Y	Y	Y	Y	Y	Y ² ₂		

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, ²²Supported only on IOS 12.2(33)MRA (CSR3.2)

Security

Table 6-121 Security Attribute Support on Cisco Routers—Cisco ANA Version 3.7.1

Attribute	800	1000	1600	1700	1800	2500	2600	2800	ISR2900	3600	3700	3800	ISR 3900	Cisco 4700	7200	7300	7400	7500	7600	10000	12000	XR 12000	CRS-1	ASR 1000	ASR 9000	MWR 2941	UBR7200	UBR10000
IMO Name—IAccessList																												
Type	Y						Y	Y	Y	Y	Y		Y	Y	Y	Y	Y	Y	Y	Y	Y	Y ¹	Y ²	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	Y	Y	Y ³	Y ⁴	Y	Y	Y	Y	Y
Name or Id	Y						Y	Y	Y	Y	Y		Y	Y	Y	Y	Y	Y	Y	Y	Y	Y ⁵	Y ⁶	Y	Y	Y	Y	Y
Index	Y						Y	Y	Y	Y	Y		Y	Y	Y	Y	Y	Y	Y	Y	Y	Y ⁷	Y ⁸	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	Y	Y	Y ⁹	Y ¹ ₀	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	Y	Y	Y ¹ ₁	Y ¹ ₂	Y	Y	Y	Y	Y

Table 6-121 Security Attribute Support on Cisco Routers—Cisco ANA Version 3.7.1 (continued)

Attribute	800	1000	1600	1700	1800	2500	2600	2800	ISR2900	3600	3700	3800	ISR 3900	Cisco 4700	7200	7300	7400	7500	7600	10000	12000	XR 12000	CRS-1	ASR 1000	ASR 9000	MWR 2941	UBR7200	UBR10000
Source and Destination Address	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y ¹ ₃	Y ¹ ₄	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	Y	Y ¹ ₅	Y ¹ ₆	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	Y	Y	Y	Y ¹ ₇	Y ¹ ₈	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	Y	Y ¹ ₉	Y ² ₀	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	Y	Y ² ₁	Y ² ₂	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	Y	Y ² ₃	Y ² ₄	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	Y	Y ² ₅	Y ² ₆	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	Y	Y ² ₇	Y ² ₈	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	Y	Y ² ₉	Y ³ ₀	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	Y	Y ³ ₁	Y ³ ₂	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 ANA 3.6.0 and earlier: show access-lists ipv4. ANA 3.6.1 and later: show running-config ipv4 access-list.

Hardware

Table 6-122 Hardware Attribute Support on Cisco Routers—Cisco ANA Version 3.7.1

Attribute	800	1000	1600	1700	1800	2500	2600	2800	ISR2900	3600	3700	3800	ISR 3900	Cisco 4700	7200	7300	7400	7500	7600	10000	12000	XR 12000	CRS-1	ASR 1000	ASR 9000	MWR 2941	UBR7200	UBR10000
IMO Name—IChassis																												
Description	Y		Y		Y	Y	Y	Y	Y ¹	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
Contained Equipment Holders																												
Contained Equipments																							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
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	Y	Y ²	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
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
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
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
Managed IP Address																												
Redundant Equipment																					Y	Y						
Configured Redundancy																			Y		Y	Y	Y	Y	Y			
Redundancy Status	Y		Y	Y		Y	Y					Y			Y				Y		Y	Y	Y	Y	Y	Y	Y	

Table 6-122 Hardware Attribute Support on Cisco Routers—Cisco ANA Version 3.7.1 (continued)

Attribute	800	1000	1600	1700	1800	2500	2600	2800	ISR2900	3600	3700	3800	ISR 3900	Cisco 4700	7200	7300	7400	7500	7600	10000	12000	XR 12000	CRS-1	ASR 1000	ASR 9000	MWR 2941	UBR7200	UBR10000
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	
Supported Physical Termination Points		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
Slots Number								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
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
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
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
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
Device Name	Y	Y	Y	Y	Y	Y	Y	Y	Y ³	Y	Y	Y		Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	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
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
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
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
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
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
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
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
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
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
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
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
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
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

Table 6-122 Hardware Attribute Support on Cisco Routers—Cisco ANA Version 3.7.1 (continued)

Attribute	800	1000	1600	1700	1800	2500	2600	2800	ISR2900	3600	3700	3800	ISR 3900	Cisco 4700	7200	7300	7400	7500	7600	10000	12000	XR 12000	CRS-1	ASR 1000	ASR 9000	MWR 2941	UBR7200	UBR10000
File Systems																						Y	Y		Y			
IMO Name—IContext																												
Name						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	
IMO Name—IBridge																												
Bridge Table	Y									Y			Y				Y		Y	Y		Y			Y	Y		
Type	Y												Y				Y		Y	Y		Y			Y	Y		
MAC Address	Y												Y				Y		Y	Y					Y	Y		
IP Interface	Y												Y				Y		Y	Y		Y			Y	Y		
Name	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		
Vlan Type																						Y						
IMO Name—IBridgeEntry																												
Destination MAC	Y					Y	Y			Y			Y				Y		Y	Y		Y			Y	Y		
Outgoing Interface	Y					Y	Y			Y			Y				Y		Y	Y		Y			Y	Y		

¹Supported only for version 12.2(50)SE

²Device Name is Mapped to Element Name in GUI

³Blower modules are supported in XR versions 3.7.1 and above. PEM Modules are supported in XR versions 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.

Serial

Table 6-123 Serial Attribute Support on Cisco Routers—Cisco ANA Version 3.7.1

Attribute	800	1000	1600	1700	1800	2500	2600	2800	ISR2900	3600	3700	3800	ISR 3900	Cisco 4700	7200	7300	7400	7500	7600	10000	12000	XR 12000	CRS-1	ASR 1000	ASR 9000	MWR 2941	UBR7200	UBR10000
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
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
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
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
Discarded Bandwidth																												
Dropped Bandwidth																												
Input Bandwidth			Y	Y		Y	Y	Y			Y																	
Output Bandwidth			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
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
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
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
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
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	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
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

Table 6-123 Serial Attribute Support on Cisco Routers—Cisco ANA Version 3.7.1 (continued)

Attribute	800	1000	1600	1700	1800	2500	2600	2800	ISR2900	3600	3700	3800	ISR 3900	Cisco 4700	7200	7300	7400	7500	7600	10000	12000	XR 12000	CRS-1	ASR 1000	ASR 9000	MWR 2941	UBR7200	UBR10000
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
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
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
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
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
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

Additional Technologies

Table 6-124 Additional Technologies Attribute Support on Cisco Routers—Cisco ANA Version 3.7.1

Attribute	800	1000	1600	1700	1800	2500	2600	2800	ISR2900	3600	3700	3800	ISR 3900	Cisco 4700	7200	7300	7400	7500	7600	10000	12000	XR 12000	CRS-1	ASR 1000	ASR 9000	MWR 2941	UBR7200	UBR10000
IMO Name—POS																												
POS	Y	Y		Y	Y	Y	Y	Y		Y	Y				Y		Y		Y	Y	Y	Y	Y	Y				

IPoDWDM

Table 6-125 IPoDWDM Attribute Support on Cisco Routers—Cisco ANA Version 3.7.1

Attribute	800	1000	1600	1700	1800	2500	2600	2800	ISR2900	3600	3700	3800	ISR 3900	Cisco 4700	7200	7300	7400	7500	7600	10000	12000	XR 12000	CRS-1	ASR 1000	ASR 9000	MWR 2941	UBR7200	UBR10000
IMO Name—IDWDM																												
laserStatus																												
txPower																							Y					
rxPower																							Y					

Table 6-125 IPoDWDM Attribute Support on Cisco Routers—Cisco ANA Version 3.7.1 (continued)

Attribute	800	1000	1600	1700	1800	2500	2600	2800	ISR2900	3600	3700	3800	ISR 3900	Cisco 4700	7200	7300	7400	7500	7600	10000	12000	XR 12000	CRS-1	ASR 1000	ASR 9000	MWR 2941	UBR7200	UBR10000
loopback																						Y						
controllerStatus																						Y						
wavelengthBand																						Y						
msaItuChannel																						Y						
frequency																						Y						
wavelength																						Y						
g709Status																						Y						
detectedAlarms																						Y						
assertedAlarms																						Y						
opticsType																						Y						
rxLosThreshold																						Y						
location														Y					Y			Y						
IMO Name—IDwdmG709Info																												
Location														Y					Y			Y						
Status														Y					Y			Y						
OtuAlarmCounters														Y					Y			Y						
OduAlarmCounters														Y					Y			Y						
OtuAlarmReporting														Y					Y			Y						
OduAlarmReporting														Y					Y			Y						
OtuAssertedAlarms														Y					Y			Y						
OduAssertedAlarms														Y					Y			Y						
OtuDetectedAlarms														Y					Y			Y						
OduDetectedAlarms														Y					Y			Y						
OtuBerCounters														Y					Y			Y						
OtuBerReporting														Y					Y			Y						
OtuAssertedBers														Y					Y			Y						
OtuDetectedBers														Y					Y			Y						

Table 6-125 IPoDWDM Attribute Support on Cisco Routers—Cisco ANA Version 3.7.1 (continued)

Attribute	800	1000	1600	1700	1800	2500	2600	2800	ISR2900	3600	3700	3800	ISR 3900	Cisco 4700	7200	7300	7400	7500	7600	10000	12000	XR 12000	CRS-1	ASR 1000	ASR 9000	MWR 2941	UBR7200	UBR10000
OtuBerThreshold																						Y						
OtuTTI																						Y						
OduTTI														Y					Y			Y						
FecInfo														Y					Y			Y						
FecMode														Y					Y			Y						
IMO Name—IDwdmPmSettings																												
Location																						Y						
IntervalType																						Y						
FecPmSettings																						Y						
OpticsPmSettings																						Y						
OtnPmSettings																						Y						

LocalSwitching

Table 6-126 LocalSwitching Attribute Support on Cisco Routers—Cisco ANA Version 3.7.1

Attribute	800	1000	1600	1700	1800	2500	2600	2800	ISR2900	3600	3700	3800	ISR 3900	Cisco 4700	7200	7300	7400	7500	7600	10000	12000	XR 12000	CRS-1	ASR 1000	ASR 9000	MWR 2941	UBR7200	UBR10000
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		
PWSwitchingTable																			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		
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		
Segment 1	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		
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		

Table 6-126 LocalSwitching Attribute Support on Cisco Routers—Cisco ANA Version 3.7.1 (continued)

Attribute	800	1000	1600	1700	1800	2500	2600	2800	ISR2900	3600	3700	3800	ISR 3900	Cisco 4700	7200	7300	7400	7500	7600	10000	12000	XR 12000	CRS-1	ASR 1000	ASR 9000	MWR 2941	UBR7200	UBR10000
Segment 2	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		
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		

BFD

Table 6-127 BFD Attribute Support on Cisco Routers—Cisco ANA Version 3.7.1

Attribute	800	1000	1600	1700	1800	2500	2600	2800	ISR2900	3600	3700	3800	ISR 3900	Cisco 4700	7200	7300	7400	7500	7600	10000	12000	XR 12000	CRS-1	ASR 1000	ASR 9000	MWR 2941	UBR7200	UBR10000
IMO Name—IBfdService																												
Status				Y					Y				Y	Y	Y							Y	Y	Y	Y	Y		
IMO Name—IBfdSession																												
SourceIp				Y					Y				Y	Y	Y				Y			Y	Y ¹	Y	Y	Y		
DestinationIp				Y					Y				Y	Y	Y				Y			Y	Y ²	Y	Y	Y		
Interval				Y					Y				Y	Y	Y				Y			Y	Y ³	Y	Y	Y		
Multiplier				Y					Y				Y	Y	Y				Y			Y	Y ⁴	Y	Y	Y		
Protocol				Y					Y				Y	Y	Y				Y			Y	Y ⁵	Y	Y	Y		
State				Y					Y				Y	Y	Y				Y			Y	Y ⁶	Y	Y	Y		
Interface				Y					Y				Y	Y	Y				Y			Y	Y ⁷	Y	Y	Y		
Process				Y					Y				Y	Y	Y				Y			Y	Y ⁸	Y	Y	Y		

1, 2, 3, 4, 5, 6, 7, 8BFD Support on IPv6 is available only on CRS-1 devices.

Carrier Ethernet

Table 6-128 Carrier Ethernet Attribute Support on Cisco Routers—Cisco ANA Version 3.7.1

Attribute	800	1000	1600	1700	1800	2500	2600	2800	ISR2900	3600	3700	3800	ISR 3900	Cisco 4700	7200	7300	7400	7500	7600	10000	12000	XR 12000	CRS-1	ASR 1000	ASR 9000	MWR 2941	UBR7200	UBR10000
IMO Name—IVsi																												
vsiInstanceName													Y						Y			Y	Y	Y	Y	Y ¹		
vpnId													Y						Y			Y	Y	Y	Y	Y ²		
discoveryMode													Y						Y			Y	Y	Y	Y	Y ³		
vsiMode													Y						Y			Y	Y	Y	Y	Y ⁴		
Operational state													Y						Y			Y	Y	Y	Y	Y ⁵		
Administrative state													Y						Y			Y	Y	Y	Y	Y ⁶		
IMO Name—IPseudowireProperties																												
isSplitHorizonEnabled																			Y			Y		Y	Y			
isAutoDiscovered																			Y			Y		Y	Y			
IMO Name—IVLANTaggedInterface																												
InterfaceName									Y				Y	Y					Y	Y ⁷	Y ⁸	Y ⁹	Y	Y	Y	Y ¹ ₀		
Inner Vlan Id									Y				Y	Y					Y	Y ¹ ₁	Y ¹ ₂	Y ¹ ₃	Y	Y	Y	Y ¹ ₄		
Outer Vlan Id									Y				Y	Y					Y	Y ¹ ₅	Y ¹ ₆	Y ¹ ₇	Y	Y	Y	Y ¹ ₈		
Encap Type									Y				Y	Y					Y	Y ¹ ₉	Y ² ₀	Y ² ₁	Y	Y	Y	Y ² ₂		
Operational state									Y				Y	Y					Y	Y ² ₃	Y ² ₄	Y ² ₅	Y	Y	Y	Y ² ₆		
Administrative state									Y				Y	Y					Y	Y ² ₇	Y ² ₈	Y ² ₉	Y	Y	Y	Y ³ ₀		
ConfiguredDescription									Y				Y						Y	Y ³ ₁	Y ³ ₂	Y	Y	Y	Y	Y ³ ₃		

Table 6-128 Carrier Ethernet Attribute Support on Cisco Routers—Cisco ANA Version 3.7.1 (continued)

Attribute	800	1000	1600	1700	1800	2500	2600	2800	ISR2900	3600	3700	3800	ISR 3900	Cisco 4700	7200	7300	7400	7500	7600	10000	12000	XR 12000	CRS-1	ASR 1000	ASR 9000	MWR 2941	UBR7200	UBR10000
IMO Name—IEfp																												
EfpId																			Y ³ ₄			Y ³ ₅			Y			
RewriteParams																			Y ³ ₆			Y ³ ₇			Y			
EncapsParams																			Y ³ ₈			Y ³ ₉			Y			
AdminStatus																			Y ⁴ ₀			Y ⁴ ₁			Y			
OperStatus																			Y ⁴ ₂			Y ⁴ ₃			Y			
SplitHorizonGroup																			Y ⁴ ₄			Y ⁴ ₅						
MatchCriteria																			Y ⁴ ₆			Y ⁴ ₇			Y			
ConfiguredDescription																			Y			Y			Y			
GetServiceInstanceId																			Y ⁴ ₈			Y ⁴ ₉			Y			
SetServiceInstanceId																			Y ⁵ ₀			Y ⁵ ₁			Y			

1, 2, 3, 4, 5, 6, 7, 8, 9SNMP is used for versions greater than SRD.

10, 11, 12, 13, 14, 15, 16Supported in IOS versions 12.2(28)SB1 and above.

17, 18, 19, 20, 21, 22, 23Supported in IOS versions 12.0(31)S and above only.

24, 25, 26, 27, 28, 29, 30, 31, 32, 33, 34, 35, 36, 37, 38Supported for versions greater than IOX 3.8

39, 40, 41, 42, 43, 44Supported only on IOS 12.2(33)MRA (CSR3.2)

45, 46, 47, 48, 49, 50, 51Not Supported in IOS 12.2(33)MRA (CSR3.2)

CDP

Table 6-129 CDP Attribute Support on Cisco Routers—Cisco ANA Version 3.7.1

Attribute	800	1000	1600	1700	1800	2500	2600	2800	ISR2900	3600	3700	3800	ISR 3900	Cisco 4700	7200	7300	7400	7500	7600	10000	12000	XR 12000	CRS-1	ASR 1000	ASR 9000	MWR 2941	UBR7200	UBR10000
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
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
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
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
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
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
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
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
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

Discovery Protocol

Table 6-130 Discovery Protocol Attribute Support on Cisco Routers—Cisco ANA Version 3.7.1

Attribute	800	1000	1600	1700	1800	2500	2600	2800	ISR2900	3600	3700	3800	ISR 3900	Cisco 4700	7200	7300	7400	7500	7600	10000	12000	XR 12000	CRS-1	ASR 1000	ASR 9000	MWR 2941	UBR7200	UBR10000
IMO Name—IDiscoveryProtocol																												
DiscoveryProtocolType	Y	Y	Y	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

Ethernet OAM

Table 6-131 Ethernet OAM Attribute Support on Cisco Routers—Cisco ANA Version 3.7.1

Attribute	800	1000	1600	1700	1800	2500	2600	2800	ISR2900	3600	3700	3800	ISR 3900	Cisco 4700	7200	7300	7400	7500	7600	10000	12000	XR 12000	CRS-1	ASR 1000	ASR 9000	MWR 2941	UBR7200	UBR10000
IMO Name—ICfmService																												
cacheSize													Y						Y						Y	Y ¹		
maximumCacheSize													Y						Y							Y ²		
holdTime													Y						Y						Y	Y ³		
version													Y						Y						Y	Y ⁴		
maintenanceIntermediatePointsTable													Y						Y						Y	Y ⁵		
maintenanceDomain													Y						Y						Y	Y ⁶		
IMO Name—IMaintenanceDomain																												
name													Y						Y						Y	Y ⁷		
level													Y						Y						Y	Y ⁸		
Id													Y						Y						Y	Y ⁹		
maintenanceAssociation													Y						Y							Y ¹⁰		
IMO Name—IMaintenanceEndPoint																												
macAddress													Y						Y						Y	Y ¹¹		
Interface													Y						Y						Y	Y ¹²		
continuityCheckStatus													Y						Y						Y	Y ¹³		
direction													Y						Y						Y	Y ¹⁴		
IMO Name—IMaintenanceAssociation																												
name													Y						Y						Y	Y ¹⁵		

Table 6-131 Ethernet OAM Attribute Support on Cisco Routers—Cisco ANA Version 3.7.1 (continued)

Attribute	800	1000	1600	1700	1800	2500	2600	2800	ISR2900	3600	3700	3800	ISR 3900	Cisco 4700	7200	7300	7400	7500	7600	10000	12000	XR 12000	CRS-1	ASR 1000	ASR 9000	MWR 2941	UBR7200	UBR10000
associationType													Y						Y						Y	Y ¹ ₆		
maximalMeps													Y						Y						Y	Y ¹ ₇		
continuityCheckInterval													Y						Y						Y	Y ¹ ₈		
continuityCheckEnable													Y						Y						Y	Y ¹ ₉		
crossCheckEnable													Y						Y						Y	Y ² ₀		
direction													Y						Y						Y	Y ² ₁		
bridge													Y						Y						Y	Y ² ₂		
maintenanceEndPoints													Y						Y						Y	Y ² ₃		
cfmRemoteMaintenanceEndPoints													Y						Y						Y	Y ² ₄		
IMO Name—IMaintenanceIntermediatePoint																												
level																			Y						Y	Y ² ₅		
cfmInterface																			Y						Y	Y ² ₆		
isAutocreated																			Y						Y	Y ² ₇		
Vlans																			Y						Y	Y ² ₈		
macAddress																			Y						Y	Y ² ₉		

Table 6-131 Ethernet OAM Attribute Support on Cisco Routers—Cisco ANA Version 3.7.1 (continued)

Attribute	800	1000	1600	1700	1800	2500	2600	2800	ISR2900	3600	3700	3800	ISR 3900	Cisco 4700	7200	7300	7400	7500	7600	10000	12000	XR 12000	CRS-1	ASR 1000	ASR 9000	MWR 2941	UBR7200	UBR10000
IMO Name—IRemoteMaintenanceEndPoint																												
mepId													Y						Y						Y	Y ³ ₀		
macAddress													Y						Y						Y	Y ³ ₁		
level													Y						Y						Y	Y ³ ₂		
maintenanceEndPointStatus													Y						Y						Y	Y ³ ₃		
maintenanceEndPointOid													Y						Y						Y	Y ³ ₄		
IMO Name—IOAMData																												
adminState									Y				Y						Y						Y	Y		
pduMaxRate									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		

Table 6-131 Ethernet OAM Attribute Support on Cisco Routers—Cisco ANA Version 3.7.1 (continued)

Attribute	800	1000	1600	1700	1800	2500	2600	2800	ISR2900	3600	3700	3800	ISR 3900	Cisco 4700	7200	7300	7400	7500	7600	10000	12000	XR 12000	CRS-1	ASR 1000	ASR 9000	MWR 2941	UBR7200	UBR10000
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		
remoteLoopback									Y				Y						Y						Y	Y		
IMO Name—IUNIProperties																												
UNIId																			Y							Y		
isServiceMultiplexing																			Y							Y		
isBundlingEnabled																			Y							Y		
bundlingType																			Y							Y		
IMO Name—IEthernetLMI																												
isGlobalEnabled																										Y		
mode																										Y		
ELMIInterfaces																			Y							Y		
deviceEVCs																			Y							Y		
IMO Name—IDeviceEVC																												
EVCName																			Y							Y		
EVCStatus																			Y							Y		
EVCType																			Y							Y		
cfmMaName																			Y							Y		
configuredRemoteUNICount																			Y							Y		
activeRemoteUNICount																			Y							Y		
UNIInterfaces																			Y							Y		
IMO Name—IUNIInterfaces																												
UNIStatus																			Y							Y		

Table 6-131 Ethernet OAM Attribute Support on Cisco Routers—Cisco ANA Version 3.7.1 (continued)

Attribute	800	1000	1600	1700	1800	2500	2600	2800	ISR2900	3600	3700	3800	ISR 3900	Cisco 4700	7200	7300	7400	7500	7600	10000	12000	XR 12000	CRS-1	ASR 1000	ASR 9000	MWR 2941	UBR7200	UBR10000
UNIID																			Y							Y		
interfaceName																			Y							Y		
vlanList																			Y							Y		
ImiLinkStatus																			Y							Y		
IMO Name—IELMIInterfaces																												
interfaceName																			Y							Y		
T391																			Y							Y		
T392																			Y							Y		
N391																			Y							Y		
N393																			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, 34CFM Supported only on IOS 12.2(33)MRA(CSR 3.2)

CGN

Table 6-132 CGN Attribute Support on Cisco Routers—Cisco ANA Version 3.7.1

Attribute	800	1000	1600	1700	1800	2500	2600	2800	ISR2900	3600	3700	3800	ISR 3900	Cisco 4700	7200	7300	7400	7500	7600	10000	12000	XR 12000	CRS-1	ASR 1000	ASR 9000	MWR 2941	UBR7200	UBR10000
IMO Name—ICgnService																												
cgnName																							Y					
statistics																							Y					
addressPools																							Y					
prefferedLocations																							Y					
associatedInterfaces																							Y					
IMO Name—ICgnStatsEntry																												
statisticsName																							Y					

Table 6-132 CGN Attribute Support on Cisco Routers—Cisco ANA Version 3.7.1 (continued)

Attribute	800	1000	1600	1700	1800	2500	2600	2800	ISR2900	3600	3700	3800	ISR 3900	Cisco 4700	7200	7300	7400	7500	7600	10000	12000	XR 12000	CRS-1	ASR 1000	ASR 9000	MWR 2941	UBR7200	UBR10000
statisticsValue																						Y						
IMO Name—ICgnServiceAddressPool																												
outsideVrf																						Y						
addressPool																						Y						
insideVrf																						Y						
addressFamily																						Y						
IMO Name—ICgnServiceLocation																												
instanceName																						Y						
location																						Y						
infraInterface																						Y						
locationType																						Y						
IMO Name—ICgnIPInterface																												
interface																						Y						

SBC

Table 6-133 SBC Attribute Support on Cisco Routers—Cisco ANA Version 3.7.1

Attribute	800	1000	1600	1700	1800	2500	2600	2800	ISR2900	3600	3700	3800	ISR 3900	Cisco 4700	7200	7300	7400	7500	7600	10000	12000	XR 12000	CRS-1	ASR 1000	ASR 9000	MWR 2941	UBR7200	UBR10000
IMO Name—ISbcService																												
sbcMode																							Y					
releaseVersion																							Y					
applicationVersion																							Y					
haStatus																							Y					
IMO Name—ISBE																												
callRedirectLimit																							Y					

Table 6-133 SBC Attribute Support on Cisco Routers—Cisco ANA Version 3.7.1 (continued)

Attribute	800	1000	1600	1700	1800	2500	2600	2800	ISR2900	3600	3700	3800	ISR 3900	Cisco 4700	7200	7300	7400	7500	7600	10000	12000	XR 12000	CRS-1	ASR 1000	ASR 9000	MWR 2941	UBR7200	UBR10000	
onholdTimeout																							Y						
IMO Name—IDBE																													
dbeLocationID																							Y						
dbeType																							Y						
IMO Name—IDbeMediaInterface																													
addressRange																							Y						
vrfName																							Y						
managedBy																							Y						
portRange																							Y						
serviceClass																							Y						
status																							Y						
natMode																							Y						
termination																							Y						
IMO Name—ISbcAccount																													
name																							Y						
adjacencyList																							Y						
IMO Name—ISbeAaalInterface																													
networkId																							Y						
vrf																							Y						
IMO Name—ISbeBillingProperties																													
ldrCheckTime																							Y						
adminStatus																							Y						
operationStatus																							Y						
billingMethod																							Y						
localBillingAddress																							Y						
cachePath																							Y						
cacheMaxSize																							Y						

Table 6-133 SBC Attribute Support on Cisco Routers—Cisco ANA Version 3.7.1 (continued)

Attribute	800	1000	1600	1700	1800	2500	2600	2800	ISR2900	3600	3700	3800	ISR 3900	Cisco 4700	7200	7300	7400	7500	7600	10000	12000	XR 12000	CRS-1	ASR 1000	ASR 9000	MWR 2941	UBR7200	UBR10000
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					
radiusMode																							Y					
IMO Name—ISbcRadiusServerProperties																												
serverPriority																							Y					
serverKey																							Y					
portNumber																							Y					
IMO Name—ISbcAdjacencyEnd																												
peerSubnetRestriction																							Y					
isMediaPassthrough																							Y					
isHuntingTriggerDisabled																							Y					
huntingTriggers																							Y					
vrf																							Y					

Table 6-133 SBC Attribute Support on Cisco Routers—Cisco ANA Version 3.7.1 (continued)

Attribute	800	1000	1600	1700	1800	2500	2600	2800	ISR2900	3600	3700	3800	ISR 3900	Cisco 4700	7200	7300	7400	7500	7600	10000	12000	XR 12000	CRS-1	ASR 1000	ASR 9000	MWR 2941	UBR7200	UBR10000
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				
instancename																								Y				
IMO Name—ISbeConfiguredBlackListEntry																												
eventType																								Y				
triggerSize																								Y				
triggerPeriod																								Y				
blackListingPeriod																								Y				
isDefaultTriggerSize																								Y				

Chapter 6 Support Information for Cisco Routers

Attribute	800	1000	1600	1700	1800	2500	2600	2800	ISR2900	3600	3700	3800	ISR 3900	Cisco 4700	7200	7300	7400	7500	7600	10000	12000	XR 12000	CRS-1	ASR 1000	ASR 9000	MWR 2941	UBR7200	UBR10000
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—ISbcH248ControllInterface																												
ipAddress																								Y				
transport																								Y				
port																								Y				
IMO Name—ISbeGlobalHuntingTriggerList																												
huntingMode																								Y				

Table 6-133 SBC Attribute Support on Cisco Routers—Cisco ANA Version 3.7.1 (continued)

Attribute	800	1000	1600	1700	1800	2500	2600	2800	ISR2900	3600	3700	3800	ISR 3900	Cisco 4700	7200	7300	7400	7500	7600	10000	12000	XR 12000	CRS-1	ASR 1000	ASR 9000	MWR 2941	UBR7200	UBR10000	
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					

Table 6-133 SBC Attribute Support on Cisco Routers—Cisco ANA Version 3.7.1 (continued)

Attribute	800	1000	1600	1700	1800	2500	2600	2800	ISR2900	3600	3700	3800	ISR 3900	Cisco 4700	7200	7300	7400	7500	7600	10000	12000	XR 12000	CRS-1	ASR 1000	ASR 9000	MWR 2941	UBR7200	UBR10000		
IMO Name—ISbePolicyTable																														
matchType																								Y						
name																								Y						
description																								Y						
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						

Table 6-133 SBC Attribute Support on Cisco Routers—Cisco ANA Version 3.7.1 (continued)

Attribute	800	1000	1600	1700	1800	2500	2600	2800	ISR2900	3600	3700	3800	ISR 3900	Cisco 4700	7200	7300	7400	7500	7600	10000	12000	XR 12000	CRS-1	ASR 1000	ASR 9000	MWR 2941	UBR7200	UBR10000
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					
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					



CHAPTER 7

Support Information for Cisco Switches

This chapter contains support information for Virtual Network Elements (VNEs) that manage Cisco switches in Cisco ANA Version 3.7.1. For more information about the objects and attributes described in this chapter, see Part 2: Technology Support and Information Model Objects.

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 7-10](#)
- [Cisco Catalyst 3550 Series Switches, page 7-12](#)
- [Cisco Catalyst 3560 Series Switches, page 7-15](#)
- [Cisco ME 3600X Ethernet Access Switch, page 7-18](#)
- [Cisco Catalyst 3750 Series Switches, page 7-21](#)
- [Cisco Catalyst 3750 Metro Series Switches, page 7-24](#)
- [Cisco ME 3800X Carrier Ethernet Switches, page 7-29](#)
- [Cisco Catalyst 4000 Series Switches, page 7-33](#)
- [Cisco Catalyst 4500 Series Switches, page 7-36](#)
- [Cisco ACE 4700 Series Access Control Engine, page 7-43](#)
- [Cisco Catalyst 4900 Series Switches, page 7-49](#)
- [Cisco ME 4900 Series Ethernet Switch, page 7-57](#)
- [Cisco Catalyst 5000 Series Switches, page 7-63](#)
- [Cisco Catalyst 6500 Series \(CatOS\) Switches, page 7-65](#)
- [Cisco Catalyst 6500 Series \(IOS\) Switches, page 7-70](#)
- [Cisco ME 6500 Series Ethernet Switches \(6524\), page 7-82](#)
- [Cisco Nexus 7000 Series Switches, page 7-85](#)
- [Cisco Service Control Engines, page 7-87](#)
- [Supported Technologies on Cisco Switches, page 7-89](#)

Cisco Catalyst 1900 Series Switches

This section includes the following information about Catalyst 1900 switches (for information on the NE types supported in Cisco ANA Version 3.7.1, 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 ANA Version 3.7.1*

Software Version	ANA 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 ANA Version 3.7.1*

Topology Type	Link Type	ANA 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 ANA Version 3.7.1:

- [IP, page 7-90](#)
- [Ethernet, page 7-95](#)
- [Hardware, page 7-118](#)
- [Serial, page 7-120](#)
- [CDP, page 7-125](#)
- [Discovery Protocol, page 7-125](#)

Catalyst 1900—Supported Service Events

Table 7-3 *Supported Service Events for Catalyst 1900—Cisco ANA Version 3.7.1*

Event Name	ANA 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
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

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 ANA Version 3.7.1, 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 Commands, page 7-6](#)

Cisco Catalyst 2900 Series—Supported Software Versions

Table 7-4 *Supported Software Versions for Cisco Catalyst 2900 Series—Cisco ANA Version 3.7.1*

Software Version	ANA 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 ANA Version 3.7.1*

Topology Type	Link Type	ANA 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 ANA Version 3.7.1*

Module Name	ANA 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 ANA Version 3.7.1:

- [IP, page 7-90](#)
- [Ethernet, page 7-95](#)
- [Hardware, page 7-118](#)
- [Serial, page 7-120](#)
- [LLDP, page 7-124](#)
- [CDP, page 7-125](#)
- [Discovery Protocol, page 7-125](#)

Cisco Catalyst 2900 Series—Supported Service Events

Table 7-7 *Supported Service Events for Cisco Catalyst 2900 Series—Cisco ANA Version 3.7.1*

Event Name	ANA 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
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

Cisco Catalyst 2900 Series—Supported Commands

Table 7-8 Supported Commands for Cisco Catalyst 2900 Series—Cisco ANA Version 3.7.1

Command	ANA Version
Show REP Segment Information	3.7

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 ANA Version 3.7.1, 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 7-8
- [Cisco ME 3400 Series—Supported Technologies](#), page 7-8
- [Cisco ME 3400 Series—Supported Service Events](#), page 7-9
- [Cisco ME 3400 Series—Supported Commands](#), page 7-9

Cisco ME 3400 Series—Supported Software Versions

Table 7-9 Supported Software Versions for Cisco ME 3400 Series—Cisco ANA Version 3.7.1

Software Version	ANA 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

Table 7-9 **Supported Software Versions for Cisco ME 3400 Series—Cisco ANA Version 3.7.1**

Software Version	ANA Version
12.2(52)SE	3.6.7 ¹⁵
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

^{1, 2, 3, 4, 5, 6, 7, 8, 10, 11, 12, 13, 17, 18, 19, 20, 21}ANA models pluggable ports for this IOS version.

⁹Tested 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 7-10 **Supported Topologies for Cisco ME 3400 Series—Cisco ANA Version 3.7.1**

Topology Type	Link Type	ANA Version
Ethernet	Ethernet	3.6.1
Physical Layer	Physical Layer	3.6.1
LAG	LAG	3.6.1

Cisco ME 3400 Series—Supported Modules

Table 7-11 *Supported Modules for Cisco ME 3400 Series—Cisco ANA Version 3.7.1*

Module Name	ANA Version	Module Description
GLC-EX-SMD	3.6.7	1000BASE-EX extended SFP transceiver module
GLC-FE-100FX	3.6.7	100BaseFX-SFP module for 100 MB ports, 1310 -nm wavelength ,2 Km over MMF
GLC-FE-100LX	3.6.7	100BaseLX10-SFP module for 100 MB ports, 1310 -nm wavelength ,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 ANA Version 3.7.1:

- [IP, page 7-90](#)
- [Routing Protocols, page 7-93](#)
- [Ethernet, page 7-95](#)
- [Security, page 7-117](#)
- [Hardware, page 7-118](#)
- [Serial, page 7-120](#)
- [Additional Technologies, page 7-121](#)
- [LLDP, page 7-124](#)
- [CDP, page 7-125](#)
- [Discovery Protocol, page 7-125](#)
- [Ethernet OAM, page 7-126](#)

Cisco ME 3400 Series—Supported Service Events

Table 7-12 Supported Service Events for Cisco ME 3400 Series—Cisco ANA Version 3.7.1

Event Name	ANA 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 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
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	N
MPLS Black Hole found	3.6.1	N

Cisco ME 3400 Series—Supported Commands

Table 7-13 Supported Commands for Cisco ME 3400 Series—Cisco ANA Version 3.7.1

Command	ANA Version
CFM Configure Domain	3.7
CFM Configure Global Params	3.7
CFM Configure MIP	3.7
CFM Define Continuity Check	3.7
CFM Configure ServiceID	3.7
CFM Configure MEP	3.7
CFM Enable Continuity Check	3.7
CFM Enable SNMP Server Traps	3.7
CFM Diag MEP Status	3.7
CFM CrossCheck Status	3.7
CFM Diag Ping MAC	3.7
CFM Diag Ping MPID	3.7

Table 7-13 **Supported Commands for Cisco ME 3400 Series—Cisco ANA Version 3.7.1 (continued)**

Command	ANA Version
CFM Diag Ping Multicast	3.7
CFM Diag MAC TraceRoute	3.7
CFM Diag MPID TraceRoute	3.7
CFM Configure MEP	3.7 ¹
Enable E-LMI Global	3.7
Configure MultiPoint To MultiPoint or Point To Point EVC	3.7
Configure UNI in an Interface	3.7
Enable E-LMI on Interface	3.7
Configure Service Instance Vlan Id on Interface	3.7
Apply Template on Interface	3.7
Create Template on Interface	3.7
Disable OAM on Interface	3.7
Enable OAM on Interface	3.7
Configure OAM Parameter on Interface	3.7
Start Remote Loopback	3.7
Stop Remote Loopback	3.7
Show REP Segment Information	3.7

¹ Specific to IOS 12.2(53)SE.

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 ANA Version 3.7.1, see [Cisco Catalyst 3500 XL Series Switches](#)):

- [Cisco Catalyst 3500 XL Series—Supported Software Versions, page 7-11](#)
- [Cisco Catalyst 3500 XL Series—Supported Topologies, page 7-11](#)
- [Cisco Catalyst 3500 XL Series—Supported Modules, page 7-11](#)
- [Cisco Catalyst 3500 XL Series—Supported Technologies, page 7-11](#)
- [Cisco Catalyst 3500 XL Series—Supported Service Events, page 7-12](#)

Cisco Catalyst 3500 XL Series—Supported Software Versions

Table 7-14 *Supported Software Versions for Cisco Catalyst 3500 XL Series—Cisco ANA Version 3.7.1*

Software Version	ANA Version
Cat IOS 12.0(5)WC9a	3.6.0

Cisco Catalyst 3500 XL Series—Supported Topologies

Table 7-15 *Supported Topologies for Cisco Catalyst 3500 XL Series—Cisco ANA Version 3.7.1*

Topology Type	Link Type	ANA 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 7-16 *Supported Modules for Cisco Catalyst 3500 XL Series—Cisco ANA Version 3.7.1*

Module Name	ANA 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 ANA Version 3.7.1:

- [IP, page 7-90](#)
- [Ethernet, page 7-95](#)
- [Hardware, page 7-118](#)
- [Serial, page 7-120](#)
- [CDP, page 7-125](#)
- [Discovery Protocol, page 7-125](#)

Cisco Catalyst 3500 XL Series—Supported Service Events

Table 7-17 Supported Service Events for Cisco Catalyst 3500 XL Series—Cisco ANA Version 3.7.1

Event Name	ANA 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
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

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 ANA Version 3.7.1, see [Cisco Catalyst 3550 Series Switches](#)):

- [Cisco Catalyst 3550 Series—Supported Software Versions, page 7-13](#)
- [Cisco Catalyst 3550 Series—Supported Topologies, page 7-13](#)
- [Cisco Catalyst 3550 Series—Supported Technologies, page 7-13](#)
- [Cisco Catalyst 3550 Series—Supported Service Events, page 7-14](#)

Cisco Catalyst 3550 Series—Supported Software Versions

Table 7-18 *Supported Software Versions for Cisco Catalyst 3550 Series—Cisco ANA Version 3.7.1*

Software Version	ANA 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 7-19 *Supported Topologies for Cisco Catalyst 3550 Series—Cisco ANA Version 3.7.1*

Topology Type	Link Type	ANA 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 ANA Version 3.7.1:

- [IP, page 7-90](#)
- [Ethernet, page 7-95](#)
- [Hardware, page 7-118](#)
- [Serial, page 7-120](#)
- [Additional Technologies, page 7-121](#)
- [CDP, page 7-125](#)
- [Discovery Protocol, page 7-125](#)

Cisco Catalyst 3550 Series—Supported Service Events

Table 7-20 *Supported Service Events for Cisco Catalyst 3550 Series—Cisco ANA Version 3.7.1*

Event Name	ANA 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 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
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

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 ANA Version 3.7.1, see [Cisco Catalyst 3560 Series Switches](#)):

- [Cisco Catalyst 3560 Series—Supported Software Versions, page 7-15](#)
- [Cisco Catalyst 3560 Series—Supported Topologies, page 7-15](#)
- [Cisco Catalyst 3560 Series—Supported Modules, page 7-16](#)
- [Cisco Catalyst 3560 Series—Supported Technologies, page 7-16](#)
- [Cisco Catalyst 3560 Series—Supported Service Events, page 7-17](#)
- [Cisco Catalyst 3560 Series—Supported Commands, page 7-17](#)

Cisco Catalyst 3560 Series—Supported Software Versions

Table 7-21 *Supported Software Versions for Cisco Catalyst 3560 Series—Cisco ANA Version 3.7.1*

Software Version	ANA 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

Cisco Catalyst 3560 Series—Supported Topologies

Table 7-22 *Supported Topologies for Cisco Catalyst 3560 Series—Cisco ANA Version 3.7.1*

Topology Type	Link Type	ANA 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 7-23 *Supported Modules for Cisco Catalyst 3560 Series—Cisco ANA Version 3.7.1*

Module Name	ANA 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 ANA Version 3.7.1:

- [IP, page 7-90](#)
- [Routing Protocols, page 7-93](#)
- [Ethernet, page 7-95](#)
- [VPN \(VRF\), page 7-114](#)
- [Hardware, page 7-118](#)
- [Serial, page 7-120](#)
- [Additional Technologies, page 7-121](#)
- [CDP, page 7-125](#)
- [Discovery Protocol, page 7-125](#)

Cisco Catalyst 3560 Series—Supported Service Events

Table 7-24 Supported Service Events for Cisco Catalyst 3560 Series—Cisco ANA Version 3.7.1

Event Name	ANA 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
Rx utilization exceeded upper threshold	3.6.0	N
Tx utilization exceeded upper threshold	3.6.0	N

Cisco Catalyst 3560 Series—Supported Commands

Table 7-25 Supported Commands for Cisco Catalyst 3560 Series—Cisco ANA Version 3.7.1

Command	ANA Version
Show REP Segment Information	3.7

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 ANA Version 3.7.1, see [Cisco ME 3600X Ethernet Access Switch](#)):

- [Cisco ME 3600X—Supported Software Versions](#), page 7-18
- [Cisco ME 3600X—Supported Topologies](#), page 7-18
- [Cisco ME 3600X—Supported Modules](#), page 7-19
- [Cisco ME 3600X—Supported Technologies](#), page 7-20
- [Cisco ME 3600X—Supported Service Events](#), page 7-21

Cisco ME 3600X—Supported Software Versions

Table 7-26 *Supported Software Versions for Cisco ME 3600X—Cisco ANA Version 3.7.1*

Software Version	ANA Version
IOS 12.2(52)EY	3.7.1

Cisco ME 3600X—Supported Topologies

Table 7-27 *Supported Topologies for Cisco ME 3600X—Cisco ANA Version 3.7.1*

Topology Type	Link Type	ANA Version
BGP	BGP	3.7.1
Ethernet	Ethernet	3.7.1
MPLS	MPLS	3.7.1
PPP/HDLC	PPP or HDLC	3.7.1
LAG	LAG	3.7.1

Cisco ME 3600X—Supported Modules

Table 7-28 Supported Modules for Cisco ME 3600X—Cisco ANA Version 3.7.1

Module Name	ANA 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 10km Downlink over SMF
GLC-FE-100BX-U	3.7.1	Fiber Fast Ethernet bi-directional 10km Uplink over SMF
GLC-FE-100EX	3.7.1	100 BaseEX Fiber Fast Ethernet
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	Long wavelength gigabit ethernet SFP
GLC-SX-MM	3.7.1	Short wavelength 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 3600X—Supported Technologies

The following technologies are supported by the Cisco ME 3600X in Cisco ANA Version 3.7.1:

- [IP, page 7-90](#)
- [Routing Protocols, page 7-93](#)
- [Ethernet, page 7-95](#)
- [MPLS, page 7-111](#)
- [MPLS-TE, page 7-113](#)
- [VPN \(VRF\), page 7-114](#)
- [PWE3, page 7-116](#)
- [Security, page 7-117](#)
- [Hardware, page 7-118](#)
- [BFD, page 7-122](#)
- [Carrier Ethernet, page 7-123](#)
- [LLDP, page 7-124](#)
- [CDP, page 7-125](#)
- [Discovery Protocol, page 7-125](#)
- [Ethernet OAM, page 7-126](#)

Cisco ME 3600X—Supported Service Events

Table 7-29 *Supported Service Events for Cisco ME 3600X—Cisco ANA Version 3.7.1*

Event Name	ANA 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	3.6.0	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	N
MPLS Black Hole found	3.7.1	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 ANA Version 3.7.1, see [Cisco Catalyst 3750 Series Switches](#)):

- [Cisco 3750 Series—Supported Software Versions, page 7-22](#)
- [Cisco 3750 Series—Supported Topologies, page 7-22](#)
- [Cisco 3750 Series—Supported Technologies, page 7-22](#)
- [Cisco 3750 Series—Supported Service Events, page 7-23](#)
- [Cisco 3750 Series—Supported Commands, page 7-23](#)

Cisco 3750 Series—Supported Software Versions

Table 7-30 *Supported Software Versions for Cisco 3750 Series—Cisco ANA Version 3.7.1*

Software Version	ANA 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

Cisco 3750 Series—Supported Topologies

Table 7-31 *Supported Topologies for Cisco 3750 Series—Cisco ANA Version 3.7.1*

Topology Type	Link Type	ANA Version
Ethernet	Ethernet	3.6.0
Physical Layer	Physical Layer	3.6.0
LAG	LAG	3.6.2

Cisco 3750 Series—Supported Technologies

The following technologies are supported by the Cisco 3750 Series in Cisco ANA Version 3.7.1:

- [IP, page 7-90](#)
- [Ethernet, page 7-95](#)
- [Hardware, page 7-118](#)
- [Serial, page 7-120](#)
- [LLDP, page 7-124](#)
- [CDP, page 7-125](#)
- [Discovery Protocol, page 7-125](#)

Cisco 3750 Series—Supported Service Events

Table 7-32 Supported Service Events for Cisco 3750 Series—Cisco ANA Version 3.7.1

Event Name	ANA 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
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

Cisco 3750 Series—Supported Commands

Table 7-33 Supported Commands for Cisco 3750 Series—Cisco ANA Version 3.7.1

Command	ANA Version
Show REP Segment Information	3.7

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 ANA Version 3.7.1, see [Cisco Catalyst 3750 Metro Series Switches](#)):

- [Cisco Catalyst 3750 Metro Series—Supported Software Versions, page 7-24](#)
- [Cisco Catalyst 3750 Metro Series—Supported Topologies, page 7-25](#)
- [Cisco Catalyst 3750 Metro Series—Supported Modules, page 7-25](#)
- [Cisco Catalyst 3750 Metro Series—Supported Technologies, page 7-26](#)
- [Cisco Catalyst 3750 Metro Series—Supported Service Events, page 7-27](#)
- [Cisco Catalyst 3750 Metro Series—Supported Commands, page 7-28](#)

Cisco Catalyst 3750 Metro Series—Supported Software Versions

Table 7-34 *Supported Software Versions for Cisco Catalyst 3750 Metro Series—Cisco ANA Version 3.7.1*

Software Version	ANA 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

^{1, 2, 3, 4, 5, 6, 7, 8, 9, 10}ANA models pluggable ports for this IOS version.

^{11, 12, 13, 14}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 7-35 Supported Topologies for Cisco Catalyst 3750 Metro Series—Cisco ANA Version 3.7.1

Topology Type	Link Type	ANA Version
BGP	BGP	3.6.0
Ethernet	Ethernet	3.6.0
MPLS	MPLS	3.6.0
PPP/HDLC	PPP or HDLC	3.6.0
LAG	LAG	3.6.3

Cisco Catalyst 3750 Metro Series—Supported Modules

Table 7-36 Supported Modules for Cisco Catalyst 3750 Metro Series—Cisco ANA Version 3.7.1

Module Name	ANA 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
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
ME-C3750-24TE-FAN 0	3.7 ¹	Fan Module for ME-C3750-24TE

¹Tested 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 ANA Version 3.7.1:

- [IP, page 7-90](#)
- [Routing Protocols, page 7-93](#)
- [Ethernet, page 7-95](#)
- [MPLS, page 7-111](#)
- [MPLS-TE, page 7-113](#)
- [VPN \(VRF\), page 7-114](#)
- [PWE3, page 7-116](#)
- [Security, page 7-117](#)
- [Hardware, page 7-118](#)
- [Serial, page 7-120](#)
- [Additional Technologies, page 7-121](#)
- [LocalSwitching, page 7-122](#)
- [BFD, page 7-122](#)
- [LLDP, page 7-124](#)
- [CDP, page 7-125](#)
- [Discovery Protocol, page 7-125](#)
- [Ethernet OAM, page 7-126](#)

Cisco Catalyst 3750 Metro Series—Supported Service Events

Table 7-37 *Supported Service Events for Cisco Catalyst 3750 Metro Series—Cisco ANA Version 3.7.1*

Event Name	ANA 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	3.7	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	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

Cisco Catalyst 3750 Metro Series—Supported Commands

Table 7-38 Supported Commands for Cisco Catalyst 3750 Metro Series—Cisco ANA Version 3.7.1

Command	ANA Version
CFM Configure Domain	3.7
CFM Configure Global Params	3.7
CFM Configure MIP	3.7
CFM Define Continuity Check	3.7
CFM Configure ServiceID	3.7
CFM Configure MEP	3.7
CFM Enable Continuity Check	3.7
CFM Enable SNMP Server Traps	3.7
CFM Diag MEP Status	3.7
CFM CrossCheck Status	3.7
CFM Diag Ping MAC	3.7
CFM Diag Ping MPID	3.7
CFM Diag Ping Multicast	3.7
CFM Diag MAC TraceRoute	3.7
CFM Diag MPID TraceRoute	3.7
CFM Configure MEP	3.7 ¹
Enable E-LMI Global	3.7
Configure MultiPoint To MultiPoint or Point To Point EVC	3.7
Configure UNI in an Interface	3.7
Enable E-LMI on Interface	3.7
Configure Service Instance Vlan Id on Interface	3.7
Apply Template on Interface	3.7
Create Template on Interface	3.7
Disable OAM on Interface	3.7
Enable OAM on Interface	3.7
Configure OAM Parameter on Interface	3.7
Start Remote Loopback	3.7
Stop Remote Loopback	3.7
Show REP Segment Information	3.7

¹ Specific to IOS 12.2(53)SE.

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 ANA Version 3.7.1, see [Cisco ME 3800X Carrier Ethernet Switches](#)):

- [Cisco ME 3800X—Supported Software Versions, page 7-29](#)
- [Cisco ME 3800X—Supported Topologies, page 7-29](#)
- [Cisco ME 3800X—Supported Modules, page 7-30](#)
- [Cisco ME 3800X—Supported Technologies, page 7-31](#)
- [Cisco ME 3800X—Supported Service Events, page 7-32](#)
- [Cisco ME 3800X—Supported Commands, page 7-32](#)

Cisco ME 3800X—Supported Software Versions

Table 7-39 *Supported Software Versions for Cisco ME 3800X—Cisco ANA Version 3.7.1*

Software Version	ANA Version
IOS 12.2(52)EY	3.7.1

Cisco ME 3800X—Supported Topologies

Table 7-40 *Supported Topologies for Cisco ME 3800X—Cisco ANA Version 3.7.1*

Topology Type	Link Type	ANA Version
BGP	BGP	3.7.1
Ethernet	Ethernet	3.7.1
MPLS	MPLS	3.7.1
PPP/HDLC	PPP or HDLC	3.7.1
LAG	LAG	3.7.1

Cisco ME 3800X—Supported Modules

Table 7-41 Supported Modules for Cisco ME 3800X—Cisco ANA Version 3.7.1

Module Name	ANA 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 10km Downlink over SMF
GLC-FE-100BX-U	3.7.1	Fiber Fast Ethernet bi-directional 10km Uplink over SMF
GLC-FE-100EX	3.7.1	100 BaseEX Fiber Fast Ethernet
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	Long wavelength gigabit ethernet SFP
GLC-SX-MM	3.7.1	Short wavelength 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 ANA Version 3.7.1:

- [IP, page 7-90](#)
- [Routing Protocols, page 7-93](#)
- [Ethernet, page 7-95](#)
- [MPLS, page 7-111](#)
- [MPLS-TE, page 7-113](#)
- [VPN \(VRF\), page 7-114](#)
- [PWE3, page 7-116](#)
- [Security, page 7-117](#)
- [Hardware, page 7-118](#)
- [BFD, page 7-122](#)
- [Carrier Ethernet, page 7-123](#)
- [LLDP, page 7-124](#)
- [CDP, page 7-125](#)
- [Discovery Protocol, page 7-125](#)
- [Ethernet OAM, page 7-126](#)

Cisco ME 3800X—Supported Service Events

Table 7-42 *Supported Service Events for Cisco ME 3800X—Cisco ANA Version 3.7.1*

Event Name	ANA 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	3.6.0	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	N
MPLS Black Hole found	3.7.1	N

Cisco ME 3800X—Supported Commands

Table 7-43 *Supported Commands for Cisco ME 3800X—Cisco ANA Version 3.7.1*

Command	ANA Version
Apply Template on Interface	3.7.1
Create Template on Interface	3.7.1
Disable OAM on Interface	3.7.1
Enable OAM on Interface	3.7.1
Configure OAM Parameter on Interface	3.7.1
Start Remote Loopback	3.7.1
Stop Remote Loopback	3.7.1
Show REP Segment Information	3.7.1

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 ANA Version 3.7.1, see [Cisco Catalyst 4000 Series Switches](#)):

- [Cisco Catalyst 4000 Series—Supported Software Versions, page 7-33](#)
- [Cisco Catalyst 4000 Series—Supported Topologies, page 7-33](#)
- [Cisco Catalyst 4000 Series—Supported Modules, page 7-34](#)
- [Cisco Catalyst 4000 Series—Supported Technologies, page 7-35](#)
- [Cisco Catalyst 4000 Series—Supported Service Events, page 7-35](#)
- [Cisco Catalyst 4000 Series—Supported Commands, page 7-36](#)

Cisco Catalyst 4000 Series—Supported Software Versions

Table 7-44 *Supported Software Versions for Cisco Catalyst 4000 Series—Cisco ANA Version 3.7.1*

Software Version	ANA 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 7-45 *Supported Topologies for Cisco Catalyst 4000 Series—Cisco ANA Version 3.7.1*

Topology Type	Link Type	ANA 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 7-46 Supported Modules for Cisco Catalyst 4000 Series—Cisco ANA Version 3.7.1

Module Name	ANA Version	Module Description
CWDM-SFP-1470	3.6.0	CWDM SFP 1470 nm, Gigabit Ethernet and 1G/2G FC
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)

Table 7-46 Supported Modules for Cisco Catalyst 4000 Series—Cisco ANA Version 3.7.1

Module Name	ANA Version	Module Description
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
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 ANA Version 3.7.1:

- [IP, page 7-90](#)
- [Ethernet, page 7-95](#)
- [Hardware, page 7-118](#)
- [Serial, page 7-120](#)
- [CDP, page 7-125](#)
- [Discovery Protocol, page 7-125](#)

Cisco Catalyst 4000 Series—Supported Service Events

Table 7-47 Supported Service Events for Cisco Catalyst 4000 Series—Cisco ANA Version 3.7.1

Event Name	ANA 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

Table 7-47 Supported Service Events for Cisco Catalyst 4000 Series—Cisco ANA Version 3.7.1

Event Name	ANA Version	Expedited
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

Cisco Catalyst 4000 Series—Supported Commands

Table 7-48 Supported Commands for Cisco Catalyst 4000 Series—Cisco ANA Version 3.7.1

Command	ANA Version
Show REP Segment Information	3.7

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 ANA Version 3.7.1, see [Cisco Catalyst 4500 Series Switches](#)):

- [Cisco Catalyst 4500 Series—Supported Software Versions, page 7-37](#)
- [Cisco Catalyst 4500 Series—Supported Topologies, page 7-37](#)
- [Cisco Catalyst 4500 Series—Supported Modules, page 7-38](#)
- [Cisco Catalyst 4500 Series—Supported Technologies, page 7-42](#)
- [Cisco Catalyst 4500 Series—Supported Service Events, page 7-43](#)
- [Cisco Catalyst 4500 Series—Supported Commands, page 7-43](#)

Cisco Catalyst 4500 Series—Supported Software Versions

Table 7-49 *Supported Software Versions for Cisco Catalyst 4500 Series—Cisco ANA Version 3.7.1*

Software Version	ANA 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
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

^{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 7-50 *Supported Topologies for Cisco Catalyst 4500 Series—Cisco ANA Version 3.7.1*

Topology Type	Link Type	ANA 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 7-51 Supported Modules for Cisco Catalyst 4500 Series—Cisco ANA Version 3.7.1

Module Name	ANA 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 7-51 Supported Modules for Cisco Catalyst 4500 Series—Cisco ANA Version 3.7.1

Module Name	ANA 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 7-51 Supported Modules for Cisco Catalyst 4500 Series—Cisco ANA Version 3.7.1

Module Name	ANA 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 7-51 Supported Modules for Cisco Catalyst 4500 Series—Cisco ANA Version 3.7.1

Module Name	ANA 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 7-51 Supported Modules for Cisco Catalyst 4500 Series—Cisco ANA Version 3.7.1

Module Name	ANA 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

¹Tested 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 ANA Version 3.7.1:

- [IP, page 7-90](#)
- [Routing Protocols, page 7-93](#)
- [Ethernet, page 7-95](#)
- [VPN \(VRF\), page 7-114](#)
- [Security, page 7-117](#)
- [Hardware, page 7-118](#)
- [Serial, page 7-120](#)
- [LLDP, page 7-124](#)
- [CDP, page 7-125](#)
- [Discovery Protocol, page 7-125](#)

Cisco Catalyst 4500 Series—Supported Service Events

Table 7-52 Supported Service Events for Cisco Catalyst 4500 Series—Cisco ANA Version 3.7.1

Event Name	ANA 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

Cisco Catalyst 4500 Series—Supported Commands

Table 7-53 Supported Commands for Cisco Catalyst 4500 Series—Cisco ANA Version 3.7.1

Command	ANA Version
Show REP Segment Information	3.7

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 ANA Version 3.7.1, see [Cisco ACE 4700 Series Access Control Engine](#)):

- [Cisco ACE 4700—Supported Software Versions, page 7-44](#)
- [Cisco ACE 4700—Supported Topologies, page 7-44](#)
- [Cisco ACE 4700—Supported Technologies, page 7-44](#)
- [Cisco ACE 4700—Supported Service Events, page 7-45](#)

Cisco ACE 4700—Supported Software Versions

Table 7-54 *Supported Software Versions for Cisco ACE 4700—Cisco ANA Version 3.7.1*

Software Version	ANA Version
ACE Appliance SW 3.2	3.7.1

Cisco ACE 4700—Supported Topologies

Table 7-55 *Supported Topologies for Cisco ACE 4700—Cisco ANA Version 3.7.1*

Topology Type	Link Type	ANA 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 ANA Version 3.7.1:

- [IP, page 7-90](#)
- [Hardware, page 7-118](#)
- [Serial, page 7-120](#)

Cisco ACE 4700—Supported Service Events

Table 7-56 Supported Service Events for Cisco ACE 4700—Cisco ANA Version 3.7.1

Event Name	ANA 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
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

Table 7-56 *Supported Service Events for Cisco ACE 4700—Cisco ANA Version 3.7.1 (continued)*

Event Name	ANA Version	Expedited
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
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

Table 7-56 **Supported Service Events for Cisco ACE 4700—Cisco ANA Version 3.7.1 (continued)**

Event Name	ANA Version	Expedited
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
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

Table 7-56 *Supported Service Events for Cisco ACE 4700—Cisco ANA Version 3.7.1 (continued)*

Event Name	ANA Version	Expedited
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
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

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 ANA Version 3.7.1, see [Cisco Catalyst 4900 Series Switches](#)):

- [Cisco Catalyst 4900 Series—Supported Software Versions, page 7-49](#)
- [Cisco Catalyst 4900 Series—Supported Topologies, page 7-50](#)
- [Cisco Catalyst 4900 Series—Supported Modules, page 7-50](#)
- [Cisco Catalyst 4900 Series—Supported Technologies, page 7-53](#)
- [Cisco Catalyst 4900 Series—Supported Service Events, page 7-54](#)
- [Cisco Catalyst 4900 Series—Supported Commands, page 7-56](#)

Cisco Catalyst 4900 Series—Supported Software Versions

Table 7-57 **Supported Software Versions for Cisco Catalyst 4900 Series—Cisco ANA Version 3.7.1**

Software Version	ANA 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

^{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 7-58 Supported Topologies for Cisco Catalyst 4900 Series—Cisco ANA Version 3.7.1

Topology Type	Link Type	ANA 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 7-59 Supported Modules for Cisco Catalyst 4900 Series—Cisco ANA Version 3.7.1

Module Name	ANA 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 7-59 Supported Modules for Cisco Catalyst 4900 Series—Cisco ANA Version 3.7.1

Module Name	ANA 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 7-59 Supported Modules for Cisco Catalyst 4900 Series—Cisco ANA Version 3.7.1

Module Name	ANA 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 7-59 **Supported Modules for Cisco Catalyst 4900 Series—Cisco ANA Version 3.7.1**

Module Name	ANA 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

1, 2, 3, 4, 5, 6, 7, 8, 9, 10 Support verified in ANA 3.7.

Cisco Catalyst 4900 Series—Supported Technologies

The following technologies are supported by the Cisco Catalyst 4900 Series in Cisco ANA Version 3.7.1:

- [IP, page 7-90](#)
- [Routing Protocols, page 7-93](#)
- [Ethernet, page 7-95](#)
- [VPN \(VRF\), page 7-114](#)
- [Security, page 7-117](#)
- [Hardware, page 7-118](#)
- [Serial, page 7-120](#)
- [Additional Technologies, page 7-121](#)
- [LLDP, page 7-124](#)
- [CDP, page 7-125](#)
- [Discovery Protocol, page 7-125](#)

Cisco Catalyst 4900 Series—Supported Service Events

Table 7-60 *Supported Service Events for Cisco Catalyst 4900 Series—Cisco ANA Version 3.7.1*

Event Name	ANA 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 7-60 *Supported Service Events for Cisco Catalyst 4900 Series—Cisco ANA Version 3.7.1*

Event Name	ANA Version	Expedited
I2tp peer is removed	3.6.1	N
I2tp 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 7-60 *Supported Service Events for Cisco Catalyst 4900 Series—Cisco ANA Version 3.7.1*

Event Name	ANA 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

Cisco Catalyst 4900 Series—Supported Commands

Table 7-61 *Supported Commands for Cisco Catalyst 4900 Series—Cisco ANA Version 3.7.1*

Command	ANA Version
Show REP Segment Information	3.7

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 ANA Version 3.7.1, see [Cisco ME 4900 Series Ethernet Switch](#)):

- [Cisco 4924 ME—Supported Software Versions, page 7-57](#)
- [Cisco 4924 ME—Supported Topologies, page 7-57](#)
- [Cisco 4924 ME—Supported Modules, page 7-58](#)
- [Cisco 4924 ME—Supported Technologies, page 7-59](#)
- [Cisco 4924 ME—Supported Service Events, page 7-60](#)
- [Cisco 4924 ME—Supported Commands, page 7-62](#)

Cisco 4924 ME—Supported Software Versions

Table 7-62 *Supported Software Versions for Cisco 4924 ME—Cisco ANA Version 3.7.1*

Software Version	ANA 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

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

Cisco 4924 ME—Supported Topologies

Table 7-63 *Supported Topologies for Cisco 4924 ME—Cisco ANA Version 3.7.1*

Topology Type	Link Type	ANA Version
Ethernet	Ethernet	3.6.1
Physical Layer	Physical Layer	3.6.1

Cisco 4924 ME—Supported Modules

Table 7-64 Supported Modules for Cisco 4924 ME—Cisco ANA Version 3.7.1

Module Name	ANA 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	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

Table 7-64 **Supported Modules for Cisco 4924 ME—Cisco ANA Version 3.7.1 (continued)**

Module Name	ANA Version	Module Description
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

Cisco 4924 ME—Supported Technologies

The following technologies are supported by the Cisco 4924 ME in Cisco ANA Version 3.7.1:

- [IP, page 7-90](#)
- [Routing Protocols, page 7-93](#)
- [Ethernet, page 7-95](#)
- [VPN \(VRF\), page 7-114](#)
- [Security, page 7-117](#)
- [Hardware, page 7-118](#)
- [Serial, page 7-120](#)
- [Additional Technologies, page 7-121](#)
- [LLDP, page 7-124](#)
- [CDP, page 7-125](#)
- [Discovery Protocol, page 7-125](#)

Cisco 4924 ME—Supported Service Events

Table 7-65 *Supported Service Events for Cisco 4924 ME—Cisco ANA Version 3.7.1*

Event Name	ANA 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 7-65 **Supported Service Events for Cisco 4924 ME—Cisco ANA Version 3.7.1 (continued)**

Event Name	ANA Version	Expedited
I2tp peer is removed	3.6.1	N
I2tp 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 7-65 Supported Service Events for Cisco 4924 ME—Cisco ANA Version 3.7.1 (continued)

Event Name	ANA 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

Cisco 4924 ME—Supported Commands

Table 7-66 Supported Commands for Cisco 4924ME—Cisco ANA Version 3.7.1

Command	ANA Version
Show REP Segment Information	3.7

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 ANA Version 3.7.1, see [Cisco Catalyst 5000 Series Switches](#)):

- [Cisco 5000 Series—Supported Software Versions, page 7-63](#)
- [Cisco 5000 Series—Supported Topologies, page 7-63](#)
- [Cisco 5000 Series—Supported Technologies, page 7-63](#)
- [Cisco 5000 Series—Supported Service Events, page 7-64](#)

Cisco 5000 Series—Supported Software Versions

Table 7-67 *Supported Software Versions for Cisco 5000 Series—Cisco ANA Version 3.7.1*

Software Version	ANA Version
4.5(15)	3.7

Cisco 5000 Series—Supported Topologies

Table 7-68 *Supported Topologies for Cisco 5000 Series—Cisco ANA Version 3.7.1*

Topology Type	Link Type	ANA 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 ANA Version 3.7.1:

- [IP, page 7-90](#)
- [Ethernet, page 7-95](#)
- [Hardware, page 7-118](#)
- [Serial, page 7-120](#)
- [CDP, page 7-125](#)
- [Discovery Protocol, page 7-125](#)

Cisco 5000 Series—Supported Service Events

Table 7-69 *Supported Service Events for Cisco 5000 Series—Cisco ANA Version 3.7.1*

Event Name	ANA 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
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

Cisco 5000 Series—Supported Commands

Table 7-70 *Supported Commands for Cisco 5000 Series—Cisco ANA Version 3.7.1*

Command	ANA Version
Show REP Segment Information	3.7

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 ANA Version 3.7.1, see [Cisco Catalyst 6500 Series \(CatOS\) Switches](#)):

- [Cisco Catalyst 6500 Series \(CatOS\)—Supported Software Versions](#), page 7-65
- [Cisco Catalyst 6500 Series \(CatOS\)—Supported Topologies](#), page 7-65
- [Cisco Catalyst 6500 Series \(CatOS\)—Supported Modules](#), page 7-66
- [Cisco Catalyst 6500 Series \(CatOS\)—Supported Technologies](#), page 7-68
- [Cisco Catalyst 6500 Series \(CatOS\)—Supported Service Events](#), page 7-69

Cisco Catalyst 6500 Series (CatOS)—Supported Software Versions

Table 7-71 *Supported Software Versions for Cisco Catalyst 6500 Series (CatOS)—Cisco ANA Version 3.7.1*

Software Version	ANA Version
6.4(10)	3.6.3
7.6(1)	3.6.3
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

¹ANA recognizes all maintenance builds in this CatOS release train.

Cisco Catalyst 6500 Series (CatOS)—Supported Topologies

Table 7-72 *Supported Topologies for Cisco Catalyst 6500 Series (CatOS)—Cisco ANA Version 3.7.1*

Topology Type	Link Type	ANA 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 7-73 Supported Modules for Cisco Catalyst 6500 Series (CatOS)—Cisco ANA Version 3.7.1

Module Name	ANA 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
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 port 10/100/1000BaseT(RJ-45) module
CAT6K-WSX-6148-RJ45	3.6.0	48 port 10/100BaseTX(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)

Table 7-73 Supported Modules for Cisco Catalyst 6500 Series (CatOS)—Cisco ANA Version 3.7.1

Module Name	ANA Version	Module Description
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-S PA	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
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

Table 7-73 Supported Modules for Cisco Catalyst 6500 Series (CatOS)—Cisco ANA Version 3.7.1

Module Name	ANA Version	Module Description
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
WS-SVC-IDS2-BUN-K9	3.6.1	Cisco Catalyst 6500 Series Intrusion Detection System (IDS2) 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 ANA Version 3.7.1:

- [IP, page 7-90](#)
- [Ethernet, page 7-95](#)
- [Frame Relay, page 7-104](#)
- [PPP, page 7-105](#)
- [Hardware, page 7-118](#)
- [Serial, page 7-120](#)
- [CDP, page 7-125](#)

Cisco Catalyst 6500 Series (CatOS)—Supported Service Events

Table 7-74 *Supported Service Events for Cisco Catalyst 6500 Series (CatOS)—Cisco ANA Version 3.7.1*

Event Name	ANA 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
Module Unsupported	3.6.0	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 ANA Version 3.7.1, see [Cisco Catalyst 6500 Series \(IOS\) Switches](#)):

- [Cisco Catalyst 6500 Series \(IOS\)—Supported Software Versions, page 7-70](#)
- [Cisco Catalyst 6500 Series \(IOS\)—Supported Topologies, page 7-71](#)
- [Cisco Catalyst 6500 Series \(IOS\)—Supported Modules, page 7-71](#)
- [Cisco Catalyst 6500 Series \(IOS\)—Supported Technologies, page 7-78](#)
- [Cisco Catalyst 6500 Series \(IOS\)—Supported Service Events, page 7-79](#)

Cisco Catalyst 6500 Series (IOS)—Supported Software Versions

Table 7-75 *Supported Software Versions for Cisco Catalyst 6500 Series (IOS)—Cisco ANA Version 3.7.1*

Software Version	ANA Version
IOS 12.1	3.6.1
IOS 12.1(13)E6	3.6.2
IOS 12.1(20)E3	3.6.2
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

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 7-76 Supported Topologies for Cisco Catalyst 6500 Series (IOS)—Cisco ANA Version 3.7.1

Topology Type	Link Type	ANA Version
BGP	BGP	3.6.0
Ethernet	Ethernet	3.6.0
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 7-77 Supported Modules for Cisco Catalyst 6500 Series (IOS)—Cisco ANA Version 3.7.1

Module Name	ANA 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

Table 7-77 Supported Modules for Cisco Catalyst 6500 Series (IOS)—Cisco ANA Version 3.7.1

Module Name	ANA Version	Module Description
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
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;

Table 7-77 Supported Modules for Cisco Catalyst 6500 Series (IOS)—Cisco ANA Version 3.7.1

Module Name	ANA Version	Module Description
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
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

Table 7-77 Supported Modules for Cisco Catalyst 6500 Series (IOS)—Cisco ANA Version 3.7.1

Module Name	ANA Version	Module Description
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
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

Table 7-77 Supported Modules for Cisco Catalyst 6500 Series (IOS)—Cisco ANA Version 3.7.1

Module Name	ANA Version	Module Description
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
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

Table 7-77 Supported Modules for Cisco Catalyst 6500 Series (IOS)—Cisco ANA Version 3.7.1

Module Name	ANA Version	Module Description
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-FWM-1	3.6.0	Catalyst 6500 Firewall Module
WS-SVC-IDS2-BUN-K9	3.6.1	Cisco Catalyst 6500 Series Intrusion Detection System (IDS2) Service Module
WS-SVC-IDS2	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)

Table 7-77 Supported Modules for Cisco Catalyst 6500 Series (IOS)—Cisco ANA Version 3.7.1

Module Name	ANA Version	Module Description
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
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

Table 7-77 **Supported Modules for Cisco Catalyst 6500 Series (IOS)—Cisco ANA Version 3.7.1**

Module Name	ANA Version	Module Description
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).

Cisco Catalyst 6500 Series (IOS)—Supported Technologies

The following technologies are supported by the Cisco Catalyst 6500 Series (IOS) in Cisco ANA Version 3.7.1:

- [IP, page 7-90](#)
- [Routing Protocols, page 7-93](#)
- [Ethernet, page 7-95](#)
- [ATM, page 7-101](#)
- [HDLC, page 7-106](#)
- [SONET/SDH, page 7-107](#)
- [TDM/DSx, page 7-108](#)
- [MPLS, page 7-111](#)
- [MPLS-TE, page 7-113](#)
- [VPN \(VRF\), page 7-114](#)
- [PWE3, page 7-116](#)
- [Security, page 7-117](#)
- [Hardware, page 7-118](#)
- [Serial, page 7-120](#)
- [Additional Technologies, page 7-121](#)
- [LocalSwitching, page 7-122](#)
- [BFD, page 7-122](#)
- [Carrier Ethernet, page 7-123](#)
- [CDP, page 7-125](#)
- [Discovery Protocol, page 7-125](#)
- [Ethernet OAM, page 7-126](#)

Cisco Catalyst 6500 Series (IOS)—Supported Service Events

Table 7-78 *Supported Service Events for Cisco Catalyst 6500 Series (IOS)—Cisco ANA Version 3.7.1*

Event Name	ANA 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
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

Table 7-78 **Supported Service Events for Cisco Catalyst 6500 Series (IOS) – Cisco ANA Version 3.7.1 (continued)**

Event Name	ANA Version	Expedited
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
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

Table 7-78 **Supported Service Events for Cisco Catalyst 6500 Series (IOS)—Cisco ANA Version 3.7.1 (continued)**

Event Name	ANA Version	Expedited
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
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

Table 7-78 *Supported Service Events for Cisco Catalyst 6500 Series (IOS)—Cisco ANA Version 3.7.1 (continued)*

Event Name	ANA Version	Expedited
Tx utilization exceeded upper threshold	3.6.0	N
Tx utilization is below lower threshold	3.6.0	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 ANA Version 3.7.1, see [Cisco ME 6500 Series Ethernet Switches \(6524\)](#)):

- [Cisco ME 6500 Series \(6524\)—Supported Software Versions, page 7-82](#)
- [Cisco ME 6500 Series \(6524\)—Supported Topologies, page 7-83](#)
- [Cisco ME 6500 Series \(6524\)—Supported Modules, page 7-83](#)
- [Cisco ME 6500 Series \(6524\)—Supported Technologies, page 7-83](#)
- [Cisco ME 6500 Series \(6524\)—Supported Service Events, page 7-84](#)

Cisco ME 6500 Series (6524)—Supported Software Versions

Table 7-79 *Supported Software Versions for Cisco ME 6500 Series (6524)—Cisco ANA Version 3.7.1*

Software Version	ANA 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 7-80 Supported Topologies for Cisco ME 6500 Series (6524)—Cisco ANA Version 3.7.1

Topology Type	Link Type	ANA 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 7-81 Supported Modules for Cisco ME 6500 Series (6524)—Cisco ANA Version 3.7.1

Module Name	ANA 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 port 10/100/1000BaseT (RJ-45) module

Cisco ME 6500 Series (6524)—Supported Technologies

The following technologies are supported by the Cisco ME 6500 Series (6524) in Cisco ANA Version 3.7.1:

- [IP](#), page 7-90
- [Routing Protocols](#), page 7-93
- [Ethernet](#), page 7-95
- [MPLS](#), page 7-111
- [MPLS-TE](#), page 7-113
- [VPN \(VRF\)](#), page 7-114
- [PWE3](#), page 7-116
- [Security](#), page 7-117
- [Hardware](#), page 7-118
- [Serial](#), page 7-120
- [Additional Technologies](#), page 7-121

- [Carrier Ethernet](#), page 7-123
- [LLDP](#), page 7-124
- [CDP](#), page 7-125
- [Discovery Protocol](#), page 7-125
- [Ethernet OAM](#), page 7-126

Cisco ME 6500 Series (6524)—Supported Service Events

Table 7-82 *Supported Service Events for Cisco ME 6500 Series (6524)—Cisco ANA Version 3.7.1*

Event Name	ANA 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
Module Unsupported	3.6.0	N

Cisco ME 6500 Series (6524)—Supported Commands

Table 7-83 *Supported Commands for Cisco ME 6500 Series (6524)—Cisco ANA Version 3.7.1*

Command	ANA Version
Show REP Segment Information	3.7

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 ANA Version 3.7.1, see [Cisco Nexus 7000 Series Switches](#)):

- [Cisco Nexus 7000—Supported Software Versions, page 7-85](#)
- [Cisco Nexus 7000—Supported Topologies, page 7-85](#)
- [Cisco Nexus 7000—Supported Modules, page 7-86](#)
- [Cisco Nexus 7000—Supported Technologies, page 7-86](#)
- [Cisco Nexus 7000—Supported Service Events, page 7-87](#)
- [Cisco Nexus 7000—Additional Information, page 7-87](#)

Cisco Nexus 7000—Supported Software Versions

Table 7-84 *Supported Software Versions for Cisco Nexus 7000—Cisco ANA Version 3.7.1*

Software Version	ANA Version
NX-OS 4.2(2)	3.7.1
NX-OS 4.2(3)	3.7.1

Cisco Nexus 7000—Supported Topologies

Table 7-85 *Supported Topologies for Cisco Nexus 7000—Cisco ANA Version 3.7.1*

Topology Type	Link Type	ANA Version
Business	Business	3.7.1
Ethernet	Ethernet	3.7.1
Physical Layer	Physical Layer	3.7.1

Cisco Nexus 7000—Supported Modules

Table 7-86 Supported Modules for Cisco Nexus 7000—Cisco ANA Version 3.7.1

Module Name	ANA 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 (cable included)
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-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, 40G Fabric
N7K-M148GT-11	3.7.1	Nexus 7000 - 48 Port 10/100/1000, RJ-45, 40G Fabric
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 Short wavelength gigabit ethernet SFP.

Cisco Nexus 7000—Supported Technologies

The following technologies are supported by the Cisco Nexus 7000 in Cisco ANA Version 3.7.1:

- [IP, page 7-90](#)
- [Hardware, page 7-118](#)
- [Serial, page 7-120](#)

Cisco Nexus 7000—Supported Service Events

Table 7-87 Supported Service Events for Cisco Nexus 7000—Cisco ANA Version 3.7.1

Event Name	ANA 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

Cisco Nexus 7000—Additional Information

As a prerequisite for the Cisco Nexus 7000 VNE, you must configure any VDC completely. Be sure to specify the complete hostname (such as `myHostname#`) while giving the device credentials. Specifying only the # will affect ANA device modeling.

Cisco Service Control Engines

This section includes the following information about Cisco SCE switches (for information on the NE types supported in Cisco ANA Version 3.7.1, see [Cisco Service Control Engines](#)):

- [Cisco SCE—Supported Topologies, page 7-88](#)
- [Cisco SCE—Supported Technologies, page 7-88](#)
- [Cisco SCE—Supported Service Events, page 7-88](#)

Cisco SCE—Supported Topologies

Table 7-88 *Supported Topologies for Cisco SCE—Cisco ANA Version 3.7.1*

Topology Type	Link Type	ANA 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 ANA Version 3.7.1:

- [IP, page 7-90](#)
- [Ethernet, page 7-95](#)
- [Hardware, page 7-118](#)
- [Serial, page 7-120](#)

Cisco SCE—Supported Service Events

Table 7-89 *Supported Service Events for Cisco SCE—Cisco ANA Version 3.7.1*

Event Name	ANA 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 Switches

The following sections list the objects and attributes that are supported on Cisco switches in Cisco ANA Version 3.7.1 per technology:

- [IP, page 7-90](#)
- [Routing Protocols, page 7-93](#)
- [Ethernet, page 7-95](#)
- [ATM, page 7-101](#)
- [Frame Relay, page 7-104](#)
- [PPP, page 7-105](#)
- [HDLC, page 7-106](#)
- [SONET/SDH, page 7-107](#)
- [TDM/DSx, page 7-108](#)
- [MPLS, page 7-111](#)
- [MPLS-TE, page 7-113](#)
- [VPN \(VRF\), page 7-114](#)
- [PWE3, page 7-116](#)
- [Security, page 7-117](#)
- [Hardware, page 7-118](#)
- [Serial, page 7-120](#)
- [Additional Technologies, page 7-121](#)
- [LocalSwitching, page 7-122](#)
- [BFD, page 7-122](#)
- [Carrier Ethernet, page 7-123](#)
- [LLDP, page 7-124](#)
- [CDP, page 7-125](#)
- [Discovery Protocol, page 7-125](#)
- [Ethernet OAM, page 7-126](#)

For information about IMO changes in Cisco ANA 3.7.1, please see <http://developer.cisco.com/web/ana/integration>.

IP

Table 7-90 IP Attribute Support on Cisco Switches—Cisco ANA Version 3.7.1

Attribute	1900	2900	ME3400	3500	3550	3560	ME 3600X	3750	3750ME	ME 3800X	4000	4500	ACE 4700	4900	4924ME	5000	6500 CatOS	6500 IOS	6524ME	Nexus 7000	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
Subnetwork Mask		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
Interface Name	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
IP Interface State	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	
OSPF Interface Cost																		Y			
Broadcast Address											Y							Y			
MTU																					
Lookup Method																					
Address Resolution Type																					
ARP Timeout																					
Secured ARP																					
ICMP Mask Reply																					
IGMP Proxy																					
HSRP Groups							Y		Y	Y		Y ¹						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—IIRoutingEntity																					
Routing Table		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	
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—IIRoutingEntry																					
Destination IP Subnet		Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	

Table 7-90 IP Attribute Support on Cisco Switches—Cisco ANA Version 3.7.1 (continued)

Attribute	1900	2900	ME3400	3500	3550	3560	ME 3600X	3750	3750ME	ME 3800X	4000	4500	ACE 4700	4900	4924ME	5000	6500 CatOS	6500 IOS	6524ME	Nexus 7000	SCE
Next Hop IP Address		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	
Routing Protocol Type		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	
IMO Name—IARPEntity																					
ARP Table		Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y		Y	Y	Y	Y	Y	Y
IMO Name—IARPEntity																					
IP Address		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
Port		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
IMO Name—IIPPool																					
IP Address Pool Entries																					
Name																					
Index																					
IMO Name—IIPRangeBasedIIPoolEntry																					
Start IP Address																					
End IP Address																					
Unused Addresses																					
Used Addresses																					
Reserved Addresses																					
IMO Name—IIPSubnetBasedIIPoolEntry																					
IP Subnet																					
Unused Addresses																					
Used Addresses																					
Reserved Addresses																					
IMO Name—HSRPGGroupEntry																					
Group Number							Y		Y	Y		Y ²		Y ³				Y	Y		
Port Description							Y		Y	Y		Y ⁴		Y ⁵				Y	Y		
Priority							Y		Y	Y		Y ⁶		Y ⁷				Y	Y		
Coupled Router							Y		Y	Y		Y ⁸		Y ⁹				Y	Y		
State							Y		Y	Y		Y ¹⁰		Y ¹¹				Y	Y		
Tracking Interfaces							Y			Y											
Virtual IP Address							Y		Y	Y		Y ¹²		Y ¹³				Y	Y		

Table 7-90 IP Attribute Support on Cisco Switches—Cisco ANA Version 3.7.1 (continued)

Attribute	1900	2900	ME3400	3500	3550	3560	ME 3600X	3750	3750ME	ME 3800X	4000	4500	ACE 4700	4900	4924ME	5000	6500 CatOS	6500 IOS	6524ME	Nexus 7000	SCE
Virtual MAC Address							Y		Y	Y		Y ¹⁴		Y ¹⁵				Y	Y		
IMO Name—I TunnelGRE																					
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—I IPSLAResponderService																					
responderStatus																					
TWAMPResponderStatus																					
tcpConnect																					
udpEcho																					
IMO Name—I IPAddressPortPair																					
type																					
ipAddress																					
port																					

^{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}Validated with 12.2(52)SG only.

Routing Protocols

Table 7-91 Routing Protocols Attribute Support on Cisco Switches—Cisco ANA Version 3.7.1

Attribute	1900	2900	ME3400	3500	3550	3560	ME 3600X	3750	3750ME	ME 3800X	4000	4500	ACE 4700	4900	4924ME	5000	6500 CatOS	6500 IOS	6524ME	Nexus 7000	SCE
IMO Name—IBgpNeighborEntry																					
Remote Identifier						Y	Y		Y	Y		Y ¹		Y ²	Y			Y	Y		
Neighbor Type																					
Distributing Interfaces																					
Remote Address						Y	Y		Y	Y		Y ³		Y ⁴	Y			Y	Y		
Remote Autonomous System						Y	Y		Y	Y		Y ⁵		Y ⁶	Y			Y	Y		
Peer State						Y	Y		Y	Y		Y ⁷		Y ⁸	Y			Y	Y		
Peer AdminState									Y												
Hold Time						Y	Y		Y	Y		Y ⁹		Y ¹⁰	Y			Y	Y		
Keep Alive Time						Y	Y		Y	Y		Y ¹¹		Y ¹²	Y			Y	Y		
VrfName																					
Address family						Y															
IMO Name—IospfEntry																					
Area Identifier			Y				Y		Y	Y		Y ¹³		Y ¹⁴	Y			Y	Y		
IP Address			Y				Y		Y	Y		Y ¹⁵		Y ¹⁶	Y			Y	Y		
Type			Y				Y		Y	Y		Y ¹⁷		Y ¹⁸	Y			Y	Y		
Administrative Status			Y				Y		Y	Y		Y ¹⁹		Y ²⁰	Y			Y	Y		
Ospf Entry State			Y				Y		Y	Y		Y ²¹		Y ²²	Y			Y	Y		
IMO Name—IospfProcess																					
Process Id							Y			Y											
OSPF Version							Y			Y											
Router Id							Y			Y											
IMO Name—IospfNeighbor																					
Neighbor Id							Y			Y											
Outgoing Interface							Y			Y											
State							Y			Y											
Neighbor Interface Address							Y			Y											
Area Id							Y			Y											
IMO Name—IospfInterface																					
Area Id							Y			Y											
Network Type							Y			Y											
Cost							Y			Y											

Table 7-91 Routing Protocols Attribute Support on Cisco Switches—Cisco ANA Version 3.7.1 (continued)

Attribute	1900	2900	ME3400	3500	3550	3560	ME 3600X	3750	3750ME	ME 3800X	4000	4500	ACE 4700	4900	4924ME	5000	6500 CatOS	6500 IOS	6524ME	Nexus 7000	SCE
State							Y			Y											
Interface Address													Y	Y					Y	Y	
Type							Y			Y											
IF Priority							Y			Y											
DR Id							Y			Y											
BDR Id							Y			Y											
IMO Name—IISpfTimers																					
Schedule Delay							Y			Y											
Min Hold Time							Y			Y											
Max Wait Time							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, 11Supported for 4503E, 4507RE, 4507, and 4506E only.

12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22Validated with 12.2(52)SG only.

Ethernet

Table 7-92 Ethernet Attribute Support on Cisco Switches—Cisco ANA Version 3.7.1

Attribute	1900	2900	ME3400	3500	3550	3560	ME 3600X	3750	3750ME	ME 3800X	4000	4500	ACE 4700	4900	4924ME	5000	6500 CatOS	6500 IOS	6524ME	Nexus 7000	SCE
IM0 Name—ILinkAggregationGroup802dot3ad																					
dot3adAggMACAddress		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		
dot3adAggActorSystemID		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		
dot3adAggActorOperKey		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		
dot3adAggPartnerSystemPriority		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		
dot3adAggCollectorMaxDelay		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		
AggregationProtocolType		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		
ChannelAdminStatus		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		
IM0 Name—IEthernet																					
MAC Address	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			
IM0 Name—IVlanInterface																					
Mode			Y		Y	Y		Y	Y			Y ¹		Y	Y		Y	Y	Y		
Native VLAN Identification			Y		Y	Y		Y	Y			Y ²		Y	Y		Y	Y	Y		
Virtual LAN Table																					
IANA Type																			Y		
Containing CTPs																					

Table 7-92 Ethernet Attribute Support on Cisco Switches—Cisco ANA Version 3.7.1 (continued)

Attribute	1900	2900	ME3400	3500	3550	3560	ME 3600X	3750	3750ME	ME 3800X	4000	4500	ACE 4700	4900	4924ME	5000	6500 CatOS	6500 IOS	6524ME	Nexus 7000	SCE
Contained CTPs																					
vlanAdminType			Y						Y					Y			Y				
vlanencapType			Y						Y					Y			Y				
getAccess																					
Allowed Vlans									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		
Containing CTPs																					
Contained CTPs																					
IMO Name—IStpService																					
StpProtocol		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		
StpHelloTime		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		
StpInstanceInfoTable		Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y		Y	Y		Y	Y	Y		
Same as ISystemService																					
StpUplinkFastState		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		

Table 7-92 Ethernet Attribute Support on Cisco Switches—Cisco ANA Version 3.7.1 (continued)

Attribute	1900	2900	ME3400	3500	3550	3560	ME 3600X	3750	3750ME	ME 3800X	4000	4500	ACE 4700	4900	4924ME	5000	6500 CatOS	6500 IOS	6524ME	Nexus 7000	SCE
StpForwardDelay		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		
IMO Name—IMstService																					
MstProperties		Y						Y								Y					
Same as IStpService		Y						Y								Y					
IMO Name—IPvstpService																					
UpLinkFast		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		
IMO Name—IMstProperties																					
MstForceVersion		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		
MstExternalRootCost		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		
MstCfgIdName		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		
IMO Name—IStpInstanceInfo																					
Object Identification																					
StpBridgeId		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		
Designated Parent and Root Bridges		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		
IsRoot		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		
StpPortInfoTable		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		
Vlan Id																					
StpDesignatedBridge		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		
IMO Name—IMstInstanceInfo																					
MstVlanIds		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		

Table 7-92 Ethernet Attribute Support on Cisco Switches—Cisco ANA Version 3.7.1 (continued)

Attribute	1900	2900	ME3400	3500	3550	3560	ME 3600X	3750	3750ME	ME 3800X	4000	4500	ACE 4700	4900	4924ME	5000	6500 CatOS	6500 IOS	6524ME	Nexus 7000	SCE
IMO Name—IPvstpInstanceInfo																					
Protocol Type		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		
StpBridgeHelloTime		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		
StpProtocolSpecification		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		
StpForwardDelay		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		
IMO Name—IRstpInstanceInfo																					
StpForceVersion		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		
IMO Name—IStpPortInfo																					
StpPort		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			
StpPortState		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			
StpPortEdgePort		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			
StpPortRole		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			
StpDesignatedBridge		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			
StpPortBpduGuardState		Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y		Y	Y		Y	Y			
StpPortBpduFilterState		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			
IMO Name—IPvstpPortInfo																					
PvstpPortFastState		Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y		Y	Y		Y	Y			
IMO Name—IEthernetChannel																					
Group Number		Y ¹¹	Y	Y	Y ¹²	Y ¹³	Y	Y	Y	Y	Y	Y		Y	Y		Y	Y	Y		
Bandwidth		Y ¹⁴	Y	Y	Y	Y ¹⁵	Y	Y	Y	Y	Y	Y		Y	Y		Y	Y	Y		
Aggregation Protocol		Y ¹⁶	Y	Y	Y ¹⁷	Y ¹⁸	Y	Y	Y	Y	Y	Y		Y			Y	Y	Y		

Table 7-92 Ethernet Attribute Support on Cisco Switches—Cisco ANA Version 3.7.1 (continued)

Attribute	1900	2900	ME3400	3500	3550	3560	ME 3600X	3750	3750ME	ME 3800X	4000	4500	ACE 4700	4900	4924ME	5000	6500 CatOS	6500 IOS	6524ME	Nexus 7000	SCE
IANA Type		Y ¹⁹	Y	Y	Y ²⁰	Y ²¹	Y	Y	Y	Y	Y	Y		Y			Y	Y	Y		
Containing CTPs																					
Contained CTPs																					
Mac Address							Y		Y	Y											
Admin Status							Y		Y	Y							Y				
Oper Status							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	²²	Y	Y	Y		Y	Y		Y	Y		Y	Y	Y	Y	Y	Y		
OperatingMode	Y	Y	²³	Y	Y	Y		Y	Y		Y	Y		Y	Y	Y	Y	Y	Y		
DomainName		Y	²⁴	Y	Y	Y		Y	Y		Y	Y		Y	Y	Y	Y	Y	Y		
ConfigurationRevision	Y	Y	²⁵	Y	Y	Y		Y	Y		Y	Y		Y	Y	Y	Y	Y	Y		
isPruningEnabled	Y	Y	²⁶	Y	Y	Y		Y	Y		Y	Y		Y	Y	Y	Y	Y	Y		
isAuthenticationEnabled	Y	Y	²⁷	Y	Y	Y		Y	Y		Y	Y		Y	Y	Y	Y	Y	Y		
IMO Name—IREPService																					
version		Y ²⁸	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y		Y	Y	Y		Y	Y		
administrativeVlan		Y ²⁹	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y		Y	Y	Y		Y	Y		
notificationEnabled		Y ³⁰	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y		Y	Y	Y		Y	Y		
IMO Name—IREPSegmentInfo																					
segmentId		Y ³¹	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y		Y	Y	Y		Y	Y		
segmentComplete		Y ³²	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y		Y	Y	Y		Y	Y		
IMO Name—IREPPortInfo																					
portName		Y ³³	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y		Y	Y	Y		Y	Y		
portKey		Y ³⁴	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y		Y	Y	Y		Y	Y		
segmentId		Y ³⁵	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y		Y	Y	Y		Y	Y		
portType		Y ³⁶	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y		Y	Y	Y		Y	Y		
portRole		Y ³⁷	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y		Y	Y	Y		Y	Y		
operStatus		Y ³⁸	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y		Y	Y	Y		Y	Y		

Table 7-92 Ethernet Attribute Support on Cisco Switches—Cisco ANA Version 3.7.1 (continued)

Attribute	1900	2900	ME3400	3500	3550	3560	ME 3600X	3750	3750ME	ME 3800X	4000	4500	ACE 4700	4900	4924ME	5000	6500 CatOS	6500 IOS	6524ME	Nexus 7000	SCE
blockedVlans		Y ³⁹	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y		Y	Y	Y		Y	Y		
preemptTimer		Y ⁴⁰	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y		Y	Y	Y		Y	Y		
lslAgeoutTimer		Y ⁴¹	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y		Y	Y	Y		Y	Y		
remoteDeviceName		Y ⁴²	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y		Y	Y	Y		Y	Y		
remoteDeviceMac		Y ⁴³	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y		Y	Y	Y		Y	Y		
remotePortName		Y ⁴⁴	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y		Y	Y	Y		Y	Y		
IMO Name—IIBridgeLan																					
Id																					
IMO Name—IIBridgeEntry																					
IS Id																					
IBridge																					
BBridge																					

^{1, 2, 3, 4}SNMP is supported on ANA 3.6.0 and later.

^{5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21}Not Supported on IOS version 12.2(25)SEE2

^{22, 23, 24, 25, 26, 27, 28, 29}Supported on ME3400-E devices only.

^{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, 42}SNMP is supported on ANA 3.6.0 and later.

^{43, 44}Supported for 12.2(25)EWA14 only.

ATM

Table 7-93 *ATM Attribute Support on Cisco Switches—Cisco ANA Version 3.7.1*

Attribute	1900	2900	ME3400	3500	3550	3560	ME 3600X	3750	3750ME	ME 3800X	4000	4500	ACE 4700	4900	4924ME	5000	6500 CatOS	6500 IOS	6524ME	Nexus 7000	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			
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																					

Table 7-93 ATM Attribute Support on Cisco Switches—Cisco ANA Version 3.7.1 (continued)

Attribute	1900	2900	ME3400	3500	3550	3560	ME 3600X	3750	3750ME	ME 3800X	4000	4500	ACE 4700	4900	4924ME	5000	6500 CatOS	6500 IOS	6524ME	Nexus 7000	SCE
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			
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																					

Table 7-93 ATM Attribute Support on Cisco Switches—Cisco ANA Version 3.7.1 (continued)

Attribute	1900	2900	ME3400	3500	3550	3560	ME 3600X	3750	3750ME	ME 3800X	4000	4500	ACE 4700	4900	4924ME	5000	6500 CatOS	6500 IOS	6524ME	Nexus 7000	SCE
Same as IAtm																					
IMO Name—IAtmTrunkVc																					
Destination Description																					
Same as IAtmVc																					
IMO Name—IVcSwitchingEntity																					
Cross Connect Table																					
crossConnectTableSize																					
Logical Sons																					
IMO Name—IIMAGroup																					
AdminStatus																					
OperStatus																					
GroupNumber																					
ImaVersion																					
Speed																					
ConfiguredBandwidth																					
NumberOfLinks																					
NumberOfActiveLinks																					
MinimumNumberOfTxLinks																					
MinimumNumberOfRxLinks																					
ClockMode																					
FrameLength																					
interfaceName																					
groupStatus																					

Frame Relay

Table 7-94 Frame Relay Attribute Support on Cisco Switches—Cisco ANA Version 3.7.1

Attribute	1900	2900	ME3400	3500	3550	3560	ME 3600X	3750	3750ME	ME 3800X	4000	4500	ACE 4700	4900	4924ME	5000	6500 CatOS	6500 IOS	6524ME	Nexus 7000	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																					
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																					

Table 7-94 Frame Relay Attribute Support on Cisco Switches—Cisco ANA Version 3.7.1 (continued)

Attribute	1900	2900	ME3400	3500	3550	3560	ME 3600X	3750	3750ME	ME 3800X	4000	4500	ACE 4700	4900	4924ME	5000	6500 CatOS	6500 IOS	6524ME	Nexus 7000	SCE
Same as IFRVc																					
IMO Name—IEncapsulation																					
Virtual Connection Interface																	Y				
Binding Information																					

PPP

Table 7-95 PPP Attribute Support on Cisco Switches—Cisco ANA Version 3.7.1

Attribute	1900	2900	ME3400	3500	3550	3560	ME 3600X	3750	3750ME	ME 3800X	4000	4500	ACE 4700	4900	4924ME	5000	6500 CatOS	6500 IOS	6524ME	Nexus 7000	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																					

Table 7-95 PPP Attribute Support on Cisco Switches—Cisco ANA Version 3.7.1 (continued)

Attribute	1900	2900	ME3400	3500	3550	3560	ME 3600X	3750	3750ME	ME 3800X	4000	4500	ACE 4700	4900	4924ME	5000	6500 CatOS	6500 IOS	6524ME	Nexus 7000	SCE
LocalMRRU																					
RemoteMRRU																					
LoadThreshold																					
LCPSStatus																					
AdminStatus																					
OperStatus																					

HDLC

Table 7-96 HDLC Attribute Support on Cisco Switches—Cisco ANA Version 3.7.1

Attribute	1900	2900	ME3400	3500	3550	3560	ME 3600X	3750	3750ME	ME 3800X	4000	4500	ACE 4700	4900	4924ME	5000	6500 CatOS	6500 IOS	6524ME	Nexus 7000	SCE
IMO Name—lencapsulation (HDLC/PPP)																					
Virtual Connection																					
Binding Information																		Y			
Binding Status																		Y			
IANA Type																		Y			
Containing CTPs																					
Contained CTPs																					

SONET/SDH

Table 7-97 SONET/SDH Attribute Support on Cisco Switches—Cisco ANA Version 3.7.1

Attribute	1900	2900	ME3400	3500	3550	3560	ME 3600X	3750	3750ME	ME 3800X	4000	4500	ACE 4700	4900	4924ME	5000	6500 CatOS	6500 IOS	6524ME	Nexus 7000	SCE
IM0 Name—ISonetSdh																					
Specific Type																					
Loopback Type																		Y			
Scrambling Mode																		Y			
Same as IPhysicalLayer																					
TCAThresholdB1																					
TCAThresholdB2																					
TCAThresholdB3																					
clocking																					
IM0 Name—IDS1PdhChannelized																					
Au4Number																					
Au3Number																					
Sts1Number																					
Tug3Number																					
Tug2Number																					
VtNumber																					
C11Number																					
C12Number																					
Vt15Number																					
Vt2Number																					
T1Number																					
E1Number																					
PathType																					
Description																					
IM0 Name—ISonetSdhHop																					
Description																					
AppliqueType																					
PathType																					
IM0 Name—ISonetSts1																					
Sts1Number																					
IM0 Name—ISdhAu4																					
Au4Number																					

Table 7-97 SONET/SDH Attribute Support on Cisco Switches—Cisco ANA Version 3.7.1 (continued)

Attribute	1900	2900	ME3400	3500	3550	3560	ME 3600X	3750	3750ME	ME 3800X	4000	4500	ACE 4700	4900	4924ME	5000	6500 CatOS	6500 IOS	6524ME	Nexus 7000	SCE
IMO Name—ISdhAu3																					
Au3Number																					

TDM/DSx

Table 7-98 TDM/DSx Attribute Support on Cisco Switches—Cisco ANA Version 3.7.1

Attribute	1900	2900	ME3400	3500	3550	3560	ME 3600X	3750	3750ME	ME 3800X	4000	4500	ACE 4700	4900	4924ME	5000	6500 CatOS	6500 IOS	6524ME	Nexus 7000	SCE
IMO Name—IDS0Bundle																					
Bundled Time Slots																		Y			
Bundle Location																					
IANA Type																		Y			
Containing CTPs																					
Contained CTPs																					
AdminStatus																					
OperStatus																					
IMO Name—IDS1Pdh / IDS3Pdh																					
Framing Type																					
Cell Mapping Type																					
Loopback Type																		Y			
Scrambling Mode																		Y			
Same as IPPhysicalLayer																					
portDescription																					
internationalBit																					
nationalBits																					
framing																					
lineCode																					
cableLength																					
recoveredClockingId																					
clocking																					
loopback																					
alarmState																					

Table 7-98 TDM/DSx Attribute Support on Cisco Switches—Cisco ANA Version 3.7.1 (continued)

Attribute	1900	2900	ME3400	3500	3550	3560	ME 3600X	3750	3750ME	ME 3800X	4000	4500	ACE 4700	4900	4924ME	5000	6500 CatOS	6500 IOS	6524ME	Nexus 7000	SCE
IMO Name—IClockService																					
ActiveClockSource																					
NcsMode																					
HoldTimeout																					
UseStratum4																					
Mode																					
NcsPriorityList																					
PtpService																					
IMO Name—IClockSource																					
Priority																					
Source																					
Status																					
Type																					
IMO Name—IPtpService																					
Mode																					
ClockId																					
Domain																					
Priority1																					
Priority2																					
PtpEnabled																					
PtpInterfaceList																					
IMO Name—IPtpInterface																					
Version																					
AnnounceInterval																					
AnnounceTimeout																					
DestinationAddress																					
SourceAddress																					
DelayReq																					
MasterMode																					
SlaveMode																					
SyncInterval																					
SyncLimit																					
InterfaceXid																					

Table 7-98 TDM/DSx Attribute Support on Cisco Switches—Cisco ANA Version 3.7.1 (continued)

Attribute	1900	2900	ME3400	3500	3550	3560	ME 3600X	3750	3750ME	ME 3800X	4000	4500	ACE 4700	4900	4924ME	5000	6500 CatOS	6500 IOS	6524ME	Nexus 7000	SCE
IMO Name—IACRService																					
RecoveredClockSource																					
RecoveredClockMode																					
CemInterface																					
RecoveredClockList																					
IMO Name—IRecoveredClock																					
ClockId																					
RecoveredClockMode																					
Port																					
Cem																					
Status																					
FrequencyOffset																					
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 7-98 TDM/DSx Attribute Support on Cisco Switches—Cisco ANA Version 3.7.1 (continued)

Attribute	1900	2900	ME3400	3500	3550	3560	ME 3600X	3750	3750ME	ME 3800X	4000	4500	ACE 4700	4900	4924ME	5000	6500 CatOS	6500 IOS	6524ME	Nexus 7000	SCE
IMO Name—ISyncEInterface																					
selectionInput																					
ingressESMCMode																					
egressESMCMode																					
ingressQLMode																					
ingressQuality																					
egressQLMode																					
egressQuality																					
waitToRestore																					
holdOffTimer																					

MPLS

Table 7-99 MPLS Attribute Support on Cisco Switches—Cisco ANA Version 3.7.1

Attribute	1900	2900	ME3400	3500	3550	3560	ME 3600X	3750	3750ME	ME 3800X	4000	4500	ACE 4700	4900	4924ME	5000	6500 CatOS	6500 IOS	6524ME	Nexus 7000	SCE
IMO Name—IMpls																					
Distribution Protocol							Y		Y	Y								Y	Y		
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 7-99 MPLS Attribute Support on Cisco Switches—Cisco ANA Version 3.7.1 (continued)

Attribute	1900	2900	ME3400	3500	3550	3560	ME 3600X	3750	3750ME	ME 3800X	4000	4500	ACE 4700	4900	4924ME	5000	6500 CatOS	6500 IOS	6524ME	Nexus 7000	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		

MPLS-TE

Table 7-100 MPLS-TE Attribute Support on Cisco Switches—Cisco ANA Version 3.7.1

Attribute	1900	2900	ME3400	3500	3550	3560	ME 3600X	3750	3750ME	ME 3800X	4000	4500	ACE 4700	4900	4924ME	5000	6500 CatOS	6500 IOS	6524ME	Nexus 7000	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											
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		

Table 7-100 MPLS-TE Attribute Support on Cisco Switches—Cisco ANA Version 3.7.1 (continued)

Attribute	1900	2900	ME3400	3500	3550	3560	ME 3600X	3750	3750ME	ME 3800X	4000	4500	ACE 4700	4900	4924ME	5000	6500 CatOS	6500 IOS	6524ME	Nexus 7000	SCE
Measured Average Burst and Peak Bandwidth									Y									Y	Y		
LSP Identification									Y									Y	Y		
Name									Y									Y	Y		
FRRTunnelName							Y			Y											
FRRTunnelState							Y			Y											
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		

VPN (VRF)

Table 7-101 VPN (VRF) Attribute Support on Cisco Switches—Cisco ANA Version 3.7.1

Attribute	1900	2900	ME3400	3500	3550	3560	ME 3600X	3750	3750ME	ME 3800X	4000	4500	ACE 4700	4900	4924ME	5000	6500 CatOS	6500 IOS	6524ME	Nexus 7000	SCE
IMO Name—IVrf																					
Virtual Routing Table						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		
Name						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		

Table 7-101 VPN (VRF) Attribute Support on Cisco Switches—Cisco ANA Version 3.7.1 (continued)

Attribute	1900	2900	ME3400	3500	3550	3560	ME 3600X	3750	3750ME	ME 3800X	4000	4500	ACE 4700	4900	4924ME	5000	6500 CatOS	6500 IOS	6524ME	Nexus 7000	SCE
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		
Next Hop IP Address						Y	Y		Y	Y								Y	Y		
Type						Y	Y		Y	Y								Y	Y		
Routing Protocol Type						Y	Y		Y	Y								Y	Y		
Outgoing Interface Name						Y	Y		Y	Y								Y	Y		
IMO Name—IMpBgp																					
BGP Identifier						Y	Y		Y	Y		Y		Y	Y			Y	Y		
Local Autonomous System						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		
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 7-102 PWE3 Attribute Support on Cisco Switches—Cisco ANA Version 3.7.1

Attribute	1900	2900	ME3400	3500	3550	3560	ME 3600X	3750	3750ME	ME 3800X	4000	4500	ACE 4700	4900	4924ME	5000	6500 CatOS	6500 IOS	6524ME	Nexus 7000	SCE
IMO Name—IPTPLayer2MplsTunnel																					
Local and Remote Router Addresses							Y		Y	Y								Y	Y		
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			

Security

Table 7-103 Security Attribute Support on Cisco Switches—Cisco ANA Version 3.7.1

Attribute	1900	2900	ME3400	3500	3550	3560	ME 3600X	3750	3750ME	ME 3800X	4000	4500	ACE 4700	4900	4924ME	5000	6500 CatOS	6500 IOS	6524ME	Nexus 7000	SCE
IMO Name—IAccessList																					
Type			Y				Y		Y	Y		Y ¹		Y ²	Y			Y	Y		
Access List Entries			Y				Y		Y	Y		Y ³		Y ⁴	Y			Y	Y		
Name or Id			Y				Y		Y	Y		Y ⁵		Y ⁶	Y			Y	Y		
Index			Y				Y		Y	Y		Y ⁷		Y ⁸	Y			Y	Y		
IMO Name—IAccessListEntry																					
Entry Identification			Y				Y		Y	Y		Y ⁹		Y ¹⁰	Y			Y	Y		
Action Logic			Y				Y		Y	Y		Y ¹¹		Y ¹²	Y			Y	Y		
Source and Destination Address			Y				Y		Y	Y		Y ¹³		Y ¹⁴	Y			Y	Y		
Source and Destination Wildcard			Y				Y		Y	Y		Y ¹⁵		Y ¹⁶	Y			Y	Y		
Protocol Type			Y				Y		Y	Y		Y ¹⁷		Y ¹⁸	Y			Y	Y		
Source and Destination Port Ranges			Y				Y		Y	Y		Y ¹⁹		Y ²⁰	Y			Y	Y		
Source and Destination Port Action			Y				Y		Y	Y		Y ²¹		Y ²²	Y			Y	Y		
Protocol Specific Info			Y				Y		Y	Y		Y ²³		Y ²⁴	Y			Y	Y		
Differential Services Code Points			Y				Y		Y	Y		Y ²⁵		Y ²⁶	Y			Y	Y		
Type of Service			Y				Y		Y	Y		Y ²⁷		Y ²⁸	Y			Y	Y		
Precedence			Y				Y		Y	Y		Y ²⁹		Y ³⁰	Y			Y	Y		
Matches			Y				Y		Y	Y		Y ³¹		Y ³²	Y			Y	Y		

1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16Supported for 4503E, 4507RE, 4507, and 4506E only.

17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 31, 32Validated with 12.2(52)SG only.

Hardware

Table 7-104 Hardware Attribute Support on Cisco Switches—Cisco ANA Version 3.7.1

Attribute	1900	2900	ME3400	3500	3550	3560	ME 3600X	3750	3750ME	ME 3800X	4000	4500	ACE 4700	4900	4924ME	5000	6500 CatOS	6500 IOS	6524ME	Nexus 7000	SCE
IMO Name—IChassis																					
Description			Y ¹			Y	Y ²		Y	Y ³	Y	Y	Y	Y	Y		Y	Y	Y	Y	
Equipment Holder Type				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	
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
Module Description			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
Operational Status		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
Managed IP Address																					
Redundant Equipment																					
Configured Redundancy												Y								Y	
Redundancy Status				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	
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
Slots Number																					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
Communication State		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

Table 7-104 Hardware Attribute Support on Cisco Switches—Cisco ANA Version 3.7.1 (continued)

Attribute	1900	2900	ME3400	3500	3550	3560	ME 3600X	3750	3750ME	ME 3800X	4000	4500	ACE 4700	4900	4924ME	5000	6500 CatOS	6500 IOS	6524ME	Nexus 7000	SCE
Element Category		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
Device Name		Y	Y	Y	Y	Y	Y ⁴	Y	Y	Y ⁵	Y	Y	Y	Y	Y	Y	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
System Description	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
Software Version	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
Memory and CPU Usage		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	
Flash Device Size		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	
Processor DRAM		Y	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
Sys Location	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	
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		
Type		Y	Y		Y	Y						Y		Y	Y		Y	Y	Y		

Table 7-104 Hardware Attribute Support on Cisco Switches—Cisco ANA Version 3.7.1 (continued)

Attribute	1900	2900	ME3400	3500	3550	3560	ME 3600X	3750	3750ME	ME 3800X	4000	4500	ACE 4700	4900	4924ME	5000	6500 CatOS	6500 IOS	6524ME	Nexus 7000	SCE
MAC Address		Y	Y		Y	Y					Y	Y		Y	Y	Y	Y	Y	Y		
IP Interface		Y			Y	Y					Y	Y				Y		Y	Y		
Name		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		
Vlan Type			Y																		
IMO Name—IBridgeEntry																					
Destination MAC		Y	Y		Y	Y					Y	Y		Y	Y		Y	Y	Y		
Outgoing Interface			Y											Y	Y		Y	Y	Y		

¹Supported for 12.2(50)SE only.^{2,4}Supported only for version 12.2(50)SE^{3,5}Device Name is Mapped to Element Name in GUI

Serial

Table 7-105 Serial Attribute Support on Cisco Switches—Cisco ANA Version 3.7.1

Attribute	1900	2900	ME3400	3500	3550	3560	ME 3600X	3750	3750ME	ME 3800X	4000	4500	ACE 4700	4900	4924ME	5000	6500 CatOS	6500 IOS	6524ME	Nexus 7000	SCE
IMO Name—IPhysicalLayer																					
Media Type		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
Is Internal Port		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
Operational Status	Y	Y	Y	Y	Y	Y		Y	Y		Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y

Table 7-105 Serial Attribute Support on Cisco Switches—Cisco ANA Version 3.7.1 (continued)

Attribute	1900	2900	ME3400	3500	3550	3560	ME 3600X	3750	3750ME	ME 3800X	4000	4500	ACE 4700	4900	4924ME	5000	6500 CatOS	6500 IOS	6524ME	Nexus 7000	SCE
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
Location	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
Connector Description		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	
Connector Serial Num		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	
Status		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
Ipcore	Y																				

Additional Technologies

Table 7-106 Additional Technologies Attribute Support on Cisco Switches—Cisco ANA Version 3.7.1

Attribute	1900	2900	ME3400	3500	3550	3560	ME 3600X	3750	3750ME	ME 3800X	4000	4500	ACE 4700	4900	4924ME	5000	6500 CatOS	6500 IOS	6524ME	Nexus 7000	SCE
IMO Name—POS			Y		Y	Y			Y					Y	Y			Y	Y		
POS			Y		Y	Y			Y					Y	Y			Y	Y		

LocalSwitching

Table 7-107 LocalSwitching Attribute Support on Cisco Switches—Cisco ANA Version 3.7.1

Attribute	1900	2900	ME3400	3500	3550	3560	ME 3600X	3750	3750ME	ME 3800X	4000	4500	ACE 4700	4900	4924ME	5000	6500 CatOS	6500 IOS	6524ME	Nexus 7000	SCE
IMO Name—ILocalSwitchingEntity																					
LocalSwitchingTable									Y									Y			
PWSwitchingTable																					
IMO Name—ILocalSwitchingEntry																					
Local Switching Entry Key									Y									Y			
Local Switching Entry Status									Y									Y			
Segment 1									Y									Y			
Segment 1 Port Name									Y									Y			
Segment 1 Status									Y									Y			
Segment 2									Y									Y			
Segment 2 Port Name									Y									Y			
Segment 2 Status									Y									Y			

BFD

Table 7-108 BFD Attribute Support on Cisco Switches—Cisco ANA Version 3.7.1

Attribute	1900	2900	ME3400	3500	3550	3560	ME 3600X	3750	3750ME	ME 3800X	4000	4500	ACE 4700	4900	4924ME	5000	6500 CatOS	6500 IOS	6524ME	Nexus 7000	SCE
IMO Name—IBfdService																					
Status							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 7-109 Carrier Ethernet Attribute Support on Cisco Switches—Cisco ANA Version 3.7.1

Attribute	1900	2900	ME3400	3500	3550	3560	ME 3600X	3750	3750ME	ME 3800X	4000	4500	ACE 4700	4900	4924ME	5000	6500 CatOS	6500 IOS	6524ME	Nexus 7000	SCE
IMO Name—IVsi																					
vsiInstanceName																		Y	Y		
vpnId																		Y	Y		
discoveryMode																		Y	Y		
vsiMode																		Y	Y		
Operational state																		Y	Y		
Administrative state																		Y	Y		
IMO Name—IPseudowireProperties																					
isSplitHorizonEnabled																		Y			
isAutoDiscovered																		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			Y								Y ¹			
RewriteParams																		Y ²			
EncapsParams							Y			Y								Y ³			
AdminStatus							Y			Y								Y ⁴			
OperStatus							Y			Y								Y ⁵			
SplitHorizonGroup																		Y ⁶			
MatchCriteria							Y			Y								Y ⁷			
ConfiguredDescription																		Y			
GetServiceInstanceId							Y			Y								Y ⁸			
SetServiceInstanceId							Y			Y								Y ⁹			

1, 2, 3, 4, 5, 6, 7, 8, 9SNMP is used with versions greater than SRD.

LLDP

Table 7-110 LLDP Attribute Support on Cisco Switches—Cisco ANA Version 3.7.1

Attribute	1900	2900	ME3400	3500	3550	3560	ME 3600X	3750	3750ME	ME 3800X	4000	4500	ACE 4700	4900	4924ME	5000	6500 CatOS	6500 IOS	6524ME	Nexus 7000	SCE
IMo Name—ILLDPService																					
status		Y ¹	Y ²				Y	Y	Y ³	Y		Y ⁴		Y ⁵	Y				Y ⁶		
lldpAdvertisementsInterval		Y ⁷	Y ⁸				Y	Y	Y ⁹	Y		Y ¹⁰		Y ¹¹	Y				Y ¹²		
lldpHoldTime		Y ¹³	Y ¹⁴				Y	Y	Y ¹⁵	Y		Y ¹⁶		Y ¹⁷	Y				Y ¹⁸		
lldpReinitialisationDelay		Y ¹⁹	Y ²⁰				Y	Y	Y ²¹	Y		Y ²²		Y ²³	Y				Y ²⁴		
localChassisID		Y ²⁵	Y ²⁶				Y	Y	Y ²⁷	Y		Y ²⁸		Y ²⁹	Y				Y ³⁰		
localSystemName		Y ³¹	Y ³²				Y	Y	Y ³³	Y		Y ³⁴		Y ³⁵	Y				Y ³⁶		
IMo Name—ILLDPNeighbor																					
localPortName		Y ³⁷	Y ³⁸				Y	Y	Y ³⁹	Y		Y ⁴⁰		Y ⁴¹	Y				Y ⁴²		
remotePortDesc		Y ⁴³	Y ⁴⁴				Y	Y	Y ⁴⁵	Y		Y ⁴⁶		Y ⁴⁷	Y				Y ⁴⁸		
remoteChassisId		Y ⁴⁹	Y ⁵⁰				Y	Y	Y ⁵¹	Y		Y ⁵²		Y ⁵³	Y				Y ⁵⁴		
remoteManagementIP		Y ⁵⁵	Y ⁵⁶				Y	Y	Y ⁵⁷	Y		Y ⁵⁸		Y ⁵⁹	Y				Y ⁶⁰		
localPortId		Y ⁶¹	Y ⁶²				Y	Y	Y ⁶³	Y		Y ⁶⁴		Y ⁶⁵	Y				Y ⁶⁶		
remotePortId		Y ⁶⁷	Y ⁶⁸				Y	Y	Y ⁶⁹	Y		Y ⁷⁰		Y ⁷¹	Y				Y ⁷²		
remoteDeviceId		Y ⁷³	Y ⁷⁴				Y	Y	Y ⁷⁵	Y		Y ⁷⁶		Y ⁷⁷	Y				Y ⁷⁸		

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 7-111 CDP Attribute Support on Cisco Switches—Cisco ANA Version 3.7.1

Attribute	1900	2900	ME3400	3500	3550	3560	ME 3600X	3750	3750ME	ME 3800X	4000	4500	ACE 4700	4900	4924ME	5000	6500 CatOS	6500 IOS	6524ME	Nexus 7000	SCE
IM0 Name—ICdpService																					
cdpHoldtime		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		
cdpDeviceId		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		
cdpVersion		Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y		Y	Y	Y	Y	Y	Y		
IM0 Name—ICdpNeighbor																					
remoteDeviceId	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		
remoteIPAddress	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		

Discovery Protocol

Table 7-112 Discovery Protocol Attribute Support on Cisco Switches—Cisco ANA Version 3.7.1

Attribute	1900	2900	ME3400	3500	3550	3560	ME 3600X	3750	3750ME	ME 3800X	4000	4500	ACE 4700	4900	4924ME	5000	6500 CatOS	6500 IOS	6524ME	Nexus 7000	SCE
IM0 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 7-113 Ethernet OAM Attribute Support on Cisco Switches—Cisco ANA Version 3.7.1

Attribute	1900	2900	ME3400	3500	3550	3560	ME 3600X	3750	3750ME	ME 3800X	4000	4500	ACE 4700	4900	4924ME	5000	6500 CatOS	6500 IOS	6524ME	Nexus 7000	SCE
IMO Name—ICfmService																					
cacheSize			Y					Y										Y	Y		
maximumCacheSize			Y					Y										Y	Y		
holdTime			Y					Y										Y	Y		
version			Y					Y										Y	Y		
maintenanceIntermediatePointsTable			Y					Y										Y	Y		
maintenanceDomain			Y					Y										Y	Y		
IMO Name—IMaintenanceDomain																					
name			Y					Y										Y	Y		
level			Y					Y										Y	Y		
Id			Y					Y										Y	Y		
maintenanceAssociation			Y					Y										Y	Y		
IMO Name—IMaintenanceEndPoint																					
macAddress			Y					Y										Y	Y		
Interface			Y					Y										Y	Y		
continuityCheckStatus			Y					Y										Y	Y		
direction			Y					Y										Y	Y		
IMO Name—IMaintenanceAssociation																					
name			Y					Y										Y	Y		
associationType			Y					Y										Y	Y		
maximalMeps			Y					Y										Y	Y		
continuityCheckInterval			Y					Y										Y	Y		
continuityCheckEnable			Y					Y										Y	Y		
crossCheckEnable			Y					Y										Y	Y		
direction			Y					Y										Y	Y		
bridge			Y					Y										Y	Y		
maintenanceEndPoints			Y					Y										Y			
cfmRemoteMaintenanceEndPoints			Y					Y										Y	Y		
IMO Name—IMaintenanceIntermediatePoint																					
level			Y					Y										Y	Y		
cfmInterface			Y					Y										Y	Y		

Table 7-113 Ethernet OAM Attribute Support on Cisco Switches—Cisco ANA Version 3.7.1 (continued)

Attribute	1900	2900	ME3400	3500	3550	3560	ME 3600X	3750	3750ME	ME 3800X	4000	4500	ACE 4700	4900	4924ME	5000	6500 CatOS	6500 IOS	6524ME	Nexus 7000	SCE
isAutocreated			Y						Y									Y	Y		
Vlans			Y						Y									Y	Y		
macAddress			Y						Y									Y	Y		
IMO Name—IRemoteMaintenanceEndPoint																					
mepId			Y						Y									Y	Y		
macAddress			Y						Y									Y	Y		
level			Y						Y									Y	Y		
maintenanceEndPointStatus			Y						Y									Y	Y		
maintenanceEndPointOid			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			
remoteLoopback			Y				Y		Y	Y								Y			

Table 7-113 Ethernet OAM Attribute Support on Cisco Switches—Cisco ANA Version 3.7.1 (continued)

Attribute	1900	2900	ME3400	3500	3550	3560	ME 3600X	3750	3750ME	ME 3800X	4000	4500	ACE 4700	4900	4924ME	5000	6500 CatOS	6500 IOS	6524ME	Nexus 7000	SCE
IMO Name—IUNIProperties																					
UNIId			Y						Y									Y			
isServiceMultiplexing			Y						Y									Y			
isBundlingEnabled			Y						Y									Y			
bundlingType			Y						Y									Y			
IMO Name—IEthernetLMI																					
isGlobalEnabled			Y ¹						Y ²												
mode			Y ³						Y ⁴												
ELMIInterfaces			Y						Y									Y			
deviceEVCs			Y						Y									Y			
IMO Name—IDeviceEVC																					
EVCName			Y						Y									Y			
EVCStatus			Y						Y									Y			
EVCType			Y						Y									Y			
cfmMaName			Y						Y									Y			
configuredRemoteUNICount			Y						Y									Y			
activeRemoteUNICount			Y						Y									Y			
UNIInterfaces			Y						Y									Y			
IMO Name—IUNIInterfaces																					
UNIStatus			Y						Y									Y			
UNIId			Y						Y									Y			
interfaceName			Y						Y									Y			
vlanList			Y						Y									Y			
lmiLinkStatus			Y						Y									Y			
IMO Name—IELMIInterfaces																					
interfaceName			Y						Y									Y			
T391			Y						Y									Y			
T392			Y						Y									Y			
N391			Y						Y									Y			
N393			Y						Y									Y			

1, 2, 3, 4Supported from IOS version 12.2(35)SE onwards



CHAPTER 8

Support Information for Generic Devices

This chapter contains support information for Virtual Network Elements (VNEs) that manage Generic devices in Cisco ANA Version 3.7.1. For more information about the objects and attributes described in this chapter, see Part 2: Technology Support and Information Model Objects.

This chapter contains the following topics:

- [Understanding the Generic VNE, page 8-1](#)
- [Supported Technologies on Generic Devices, page 8-5](#)

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.

- [Physical Inventory Model, page 8-2](#)
- [Logical Inventory Model, page 8-2](#)
- [Generic VNE—Supported Traps, page 8-3](#)
- [Generic VNE—Supported Events, page 8-4](#)
- [Generic VNE Limitations, page 8-4](#)
- [Generic VNE—Supported Technologies, page 8-4](#)
- [Generic VNE—Supported Service Events, page 8-4](#)

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 8-1 on page 8-2](#) describes which MIB tables are used to model the physical inventory components that are supported by the generic VNE.

Table 8-1 *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		ifOperStatus and ifAdminStatus
Port status	ifTable	ifSpeed
Port speed	ifTable	ifPhysAddress (Ethernet ports)
MAC address	ifTable	



Note

Certain general properties on the managed element, such as system description, are modeled using the system MIB.

Logical Inventory Model

[Table 8-2 on page 8-2](#) describes which MIB tables are used to model the logical inventory components that are supported by the generic VNE.

Table 8-2 *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

Table 8-2 MIBs Used for Logical Inventory Model of Generic VNE—Cisco ANA 3.7 (continued)

Logical Component	MIB Table	Columns/Tables Used For Modeling
Bridging table	dot1dTpFdbTable	—
Default bridge	dot1dBridge	- dot1dBaseBridgeAddress - dot1dBaseType

Generic VNE—Supported Traps

The generic VNE can parse the standard MIB2 traps listed in [Table 8-3 on page 8-3](#).

Table 8-3 Supported Traps for Generic VNE—Cisco ANA 3.7.1

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 Cisco ANA receives an mplsTunnelDown trap from a device modeled with the generic VNE, Cisco ANA 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 Cisco ANA can attach a correlation flow.

Generic VNE—Supported Events

The generic VNE supports the service events listed in [Table 8-4 on page 8-4](#).

Table 8-4 *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 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 ANA Version 3.7.1:

- [IP, page 8-5](#)
- [Ethernet, page 8-8](#)
- [Hardware, page 8-13](#)
- [Serial, page 8-16](#)

Generic VNE—Supported Service Events

Table 8-5 *Supported Service Events for Generic VNE—Cisco ANA Version 3.7.1*

Event Name	ANA Version	Expedited
Device Unreachable	3.6.0	N
Discarded packet rate exceeded upper threshold	3.6.0	N
Dropped packet rate exceeded upper threshold	3.6.0	N
Port Down	3.6.0	N

Supported Technologies on Generic Devices

The following sections list the objects and attributes that are supported on Generic devices in Cisco ANA Version 3.7.1 per technology:

- [IP, page 8-5](#)
- [Ethernet, page 8-8](#)
- [Hardware, page 8-13](#)
- [Serial, page 8-16](#)

For information about IMO changes in Cisco ANA 3.7.1, please see <http://developer.cisco.com/web/ana/integration>.

IP

Table 8-6 IP Attribute Support on Generic Devices—Cisco ANA Version 3.7.1

Attribute	Generic
IMO Name—IPIInterface	
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	

Table 8-6 *IP Attribute Support on Generic Devices—Cisco ANA Version 3.7.1 (continued)*

Attribute	Generic
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—IARPEntity	
IP Address	Y
MAC Address	Y
Port	Y
Entry Type	Y
IMO Name—IIPPool	
IP Address Pool Entries	
Name	
Index	
IMO Name—IIPRangeBasedIIPPoolEntry	
Start IP Address	
End IP Address	
Unused Addresses	
Used Addresses	
Reserved Addresses	
IMO Name—IIPSubnetBasedIIPPoolEntry	
IP Subnet	
Unused Addresses	

Table 8-6 *IP Attribute Support on Generic Devices—Cisco ANA Version 3.7.1 (continued)*

Attribute	Generic
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—IIPSLAResponderService	
responderStatus	
TWAMPResponderStatus	
tcpConnect	
udpEcho	
IMO Name—IIPAddressPortPair	
type	
ipAddress	
port	

Ethernet

Table 8-7 Ethernet Attribute Support on Generic Devices—Cisco ANA Version 3.7.1

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 8-7 Ethernet Attribute Support on Generic Devices—Cisco ANA Version 3.7.1 (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 8-7 Ethernet Attribute Support on Generic Devices—Cisco ANA Version 3.7.1 (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 8-7 Ethernet Attribute Support on Generic Devices—Cisco ANA Version 3.7.1 (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 8-7 Ethernet Attribute Support on Generic Devices—Cisco ANA Version 3.7.1 (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—IRESservice	
version	
administrativeVlan	
notificationEnabled	
IMO Name—IRESsegmentInfo	
segmentId	
segmentComplete	
IMO Name—IRESportInfo	
portName	
portKey	
segmentId	
portType	
portRole	
operStatus	
blockedVlans	
preemptTimer	
lslAgeoutTimer	
remoteDeviceName	

Table 8-7 Ethernet Attribute Support on Generic Devices—Cisco ANA Version 3.7.1 (continued)

Attribute	Generic
remoteDeviceMac	
remotePortName	
IMO Name—IBridgeLan	
Id	
IMO Name—IIBridgeEntry	
IS Id	
IBridge	
BBridge	

Hardware

Table 8-8 Hardware Attribute Support on Generic Devices—Cisco ANA Version 3.7.1

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 8-8 Hardware Attribute Support on Generic Devices—Cisco ANA Version 3.7.1 (continued)

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 8-8 Hardware Attribute Support on Generic Devices—Cisco ANA Version 3.7.1 (continued)

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 8-9 Serial Attribute Support on Generic Devices—Cisco ANA Version 3.7.1

Attribute	Generic
IMO Name—IPhysicalLayer	
Media Type	
Clocking Source	
Maximum Speed	Y
Is Internal Port	
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	
Containing CTPs	
Contained CTPs	
Port Alias	
Location	
Sending Alarms	
Connector Description	
Part ID	
Connector Serial Num	
Product	
Status	
Managed	



PART 2

Technology Support and Information Model Objects



CHAPTER 9

Technology Support Introduction

Part 2—Technology Support and Information Model Objects outlines the level of functionality that Cisco ANA provides for each technology it supports. This chapter covers the following topics:

- [Supported Technologies, page 9-1](#)
- [Networking-Related IMOs, page 9-4](#)
- [Scheme Values, page 9-6](#)
- [Polling Interval Values, page 9-6](#)



Note

Part 2 describes *general* Cisco ANA capabilities for each technology covered. The specific level of support provided for a particular technology on an individual Cisco ANA Virtual Network Element (VNEs) can vary. For details on technology support on individual VNEs, see Part 1—Cisco VNEs.

Supported Technologies

[Table 9-1](#) lists the technologies supported in this version of the product.

Cisco ANA provides different levels of support for each technology. The fact that a specific technology is listed in [Table 9-1](#) does not imply that every aspect of every relevant standard is represented and supported. For details on the level of support provided for each technology, see the description for that technology in the chapter listed in the “Chapter Reference” column.

In addition to supporting specific technologies, Cisco ANA:

- Relies on several abstract modeling components used throughout product. For details, see [Chapter 37, “Common Components.”](#)
- Uses common approaches to discovering and modeling network topologies. For details, see [Chapter 38, “Cisco ANA VNE Topology.”](#)

Table 9-1 **Supported Technologies**

Technology Family	Technology Group	Technology	Chapter Reference
Network (Layer 3)	IP	IP (including IPv6)	Chapter 10, “Internet Protocol”
		Address Resolution Protocol (ARP)	
		Hot Standby Router Protocol (HSRP)	
		Generic Routing Encapsulation (GRE)	
		Carrier Grade NAT	
		IP SLA Responder	
	Routing Protocols	Border Gateway Protocol (BGP), Multiprotocol extensions (MP-BGP), external BGP (eBGP)	Chapter 11, “Routing Protocols”
		Open Shortest Path First (OSPF) and OSPFv3	
		Intermediate System to Intermediate System (IS-IS)	
	VPN and VRF	Virtual Routing and Forwarding (VRF)	Chapter 12, “VPN and VRF”
		VRF-Lite (Multi-VRF)	
		VPN	
		6VPE	
	BFD	Bidirectional Forwarding Detection	Chapter 13, “Bidirectional Forwarding Detection”
	SBC	Session Border Controller	Chapter 14, “Session Border Controller”
Hybrid Network/ Data Link (Layers 3 and 2)	MPLS	Multiprotocol Label Switching (MPLS)	Chapter 15, “Multiprotocol Label Switching”
		Label Distribution Protocol (LDP)	
	MPLS TE	Multiprotocol Label Switching Traffic Engineering (MPLS TE)	Chapter 16, “Multiprotocol Label Switching Traffic Engineering”
		MPLS TE Fast Reroute (MPLS TE FRR)	
	Pseudowire	Pseudowire Emulation Edge to Edge (PWE3)	Chapter 17, “Pseudowire”
		TDM Pseudowire	
		Multi-segment Pseudowire	
		ATM over Pseudowire (ATM PW)	
		PW-to-TE Tunnel Mapping	
	Clocking	IE1588	Chapter 32, “Clocking”
		SyncE	
		ACR	

Table 9-1 **Supported Technologies (continued)**

Technology Family	Technology Group	Technology	Chapter Reference
Data Link/MAC (Layer 2)	Ethernet	Ethernet (IEEE 802.3)	Chapter 18, “Ethernet (IEEE 802.3)”
		VLAN (IEEE 802.1Q)	
		QinQ (IEEE 802.1ad)	
		LAG (IEEE 802.3ad)	
		Ethernet Channel	
		STP (IEEE 802.1D)	
		RSTP (IEEE 802.1w)	
		PvSTP	
		MST (IEEE 802.1s)	
		SVI	
		VTP	
		REP	
		VPLS and VSI	
		H-VPLS	
		PBB	
		EFP	
	Ethernet OAM	CFM (Cisco and Draft 8.1)	Chapter 19, “Ethernet OAM”
		Link OAM	
		Ethernet LMI	
	ATM	ATM	Chapter 20, “Asynchronous Transfer Mode”
		IMA	
		ATM Cross-Connect	
		IP over ATM (MPoA 1483R)	
		Ethernet over ATM (MPoA 1483B)	
	Frame Relay	Frame Relay	Chapter 21, “Frame Relay”
	ISDN	Integrated Services Digital Network (ISDN)	Chapter 22, “Integrated Services Digital Network”
	PPP	Point To Point Protocol (PPP)	Chapter 23, “Point-to-Point Protocol”
		POS	
		PPPoA, PPPoE, PPPoFR	
		Multilink PPP	
	HDLC	High-Level Data Link Control (HDLC)	Chapter 24, “High-Level Data Link Control”
	L2TP	Layer 2 Tunnel Protocol (L2TP)	Chapter 25, “Layer 2 Tunnel Protocol”

Table 9-1 **Supported Technologies (continued)**

Technology Family	Technology Group	Technology	Chapter Reference
Data Link/MAC (Layer 2) (cont.)	Discovery Protocols	CDP, LLDP	Chapter 26, “Discovery Protocols”
	LLDP	Link Layer Discovery Protocol	
	Local Switching	Local Switching	Chapter 27, “Local Switching”
Physical Layer (Layer 1)	xDSL	Digital Subscriber Line (xDSL)	Chapter 28, “Digital Subscriber Line”
	IPoDWDM	Internet Protocol over Dense Wave Division Multiplexing (IPoDWDM)	Chapter 30, “Internet Protocol Over Dense Wave Division Multiplexing”
	SONET/SDH	SONET/SDH	Chapter 29, “SONET/SDH”
	TDM/DSx	TDM	Chapter 31, “TDM/DSx”
		DSx	
		T3/E3	
		Channelized T3, OC3, DS3 interface	
	Serial	Serial	Chapter 33, “Serial”
Other	Security	Access Control Lists (ACLs)	Chapter 34, “Access Control Lists”
	Hardware	Physical Containment	Chapter 35, “Physical Components”
		Logical Containment	Chapter 36, “Logical Components”
	Common	Common Components	Chapter 37, “Common Components”
		Local Switching	

Networking-Related IMOs

Networking-related Information Model Objects (IMOs) represent the networking aspects of a network element (NE). The two major categories of IMOs are termination points and forwarding components.

For information about IMO changes in Cisco ANA 3.7, please see <http://developer.cisco.com/web/ana/integration>.

Termination Points

Termination points represent the endpoints of a connection. A termination point may represent a physical endpoint (for example, a port connector) or a connection endpoint (such as an ATM layer of a port). A connection endpoint can also be called a network interface.

Termination points are related by containment. The following attributes express those containment relationships:

- Contained Connection Termination Point—Points to all upper-layer termination points bound to this termination point.
- Containing Termination Points—Points to all lower-layer termination points to which this termination point is bound.

The relation between termination points may represent one of the following:

- Type of hardware. For example:

A SONET/SDH port with a fiber-optic connector is represented by two IMOs:

- Port Connector IMO—Represents the fiber-optic connector.
- SonetSdh IMO—Represents the SONET/SDH port.

The Port Connector IMO contains the SonetSdh IMO. This containment relationship is represented as follows:

- The Port Connector IMO points to the SonetSdh IMO with the Contained Connection Termination Point attribute.
- The SonetSdh IMO points to the Port Connector IMO with the Containing Termination Point attribute.

- Configuration. For example:

An Ethernet port configured with an IP address (and, optionally, other network-layer attributes) is represented by two IMOs:

- Ethernet Interface IMO—Represents the Ethernet layer of the port.
- IP Interface IMO—Represents the network-layer aspect, including the IP address configured on the port.

The Ethernet Interface IMO contains the IP Interface IMO. This containment relationship is represented as follows:

- The Ethernet Interface IMO points to the IP Interface IMO with the Contained Connection Termination Point attribute.
- The IP Interface IMO points to the Ethernet Interface IMO with the Containing Termination Point attribute.

- State. For example:

An active PPP connection running on top of ATM VC is represented by two IMOs:

- Atm Vc IMO—Represents the ATM VC.
- Vc Based Encapsulation IMO—Represents the PPPoA encapsulation.

The Atm Vc IMO contains the Vc Based Encapsulation IMO. This containment relationship is represented as follows:

- The Atm Vc IMO points to the IP Vc Based Encapsulation IMO with the Contained Connection Termination Point attribute.
- The Vc Based Encapsulation IMO points to the Atm Vc IMO with the Containing Termination Point attribute.

**Note**

The relationship between termination points may be restricted to specific termination point types, based on how the technology is implemented. For example, a physical layer IMO may not contain an IP Interface IMO, which represents the network layer interface.

Forwarding Components

Forwarding components represent components that perform some type of forwarding function between termination points. Among other things, forwarding components can represent routing, bridging, and switching components in the NE.

Each forwarding component has a logical association with the termination points for which it does the forwarding. This relationship is expressed by the logical associations attribute of the forwarding component IMO. An example of such a relationship would be the logical association between an IVcSwitchingEntity IMO representing the ATM/FR switching fabric and the IAtm/IFrameRelay IMOs representing the relevant ATM/FR ports.

**Note**

The support level of each network technology can be varied. The support level is reflected in its related IMOs with their attributes, network topology, and fault and alarm correlation, as described in each of this Guide's technology chapters and in the Common Components chapter.

The polling intervals for the relationship between the termination points, as well as between them and the various forwarding components, are more complex than can be uniformly expressed, so they are marked as Not Applicable (N/A) in their corresponding Polling Interval columns. This applies to Containing Termination Points, Contained Connection Termination Points, and Logical Sons attributes of an IMO.

Scheme Values

The Scheme column of each IMO table can have the following values:

- IPCore
- Product
- Any
- N/A—This value is populated as part of the creation of the IMO, not by polling the device.

Polling Interval Values

The Polling Interval column of each IMO table can have the following values:

- Status
- Configuration
- System
- Topology Layer 1 (Topology L1)
- Topology Layer 2 (Topology L2)
- N/A—Not every property has a polling interval. Some properties are created from the results of multiple queries, and there is no specific polling for them.
- For more information about polling intervals, see the [Cisco Active Network Abstraction 3.7.1 Administrator Guide](#)



CHAPTER 10

Internet Protocol

This chapter describes the level of support that Cisco ANA provides for IP, as follows:

- [Technology Description, page 10-1](#)
- [Information Model Objects \(IMOs\), page 10-4](#)
- [Network Topology, page 10-13](#)
- [Service Alarms, page 10-14](#)

Technology Description

This section provides the following IP technology descriptions:

- [IP](#)
- [ARP](#)
- [HSRP](#)
- [GRE](#)
- [Carrier-Grade NAT \(CGN\)](#)
- [IPv6](#)
- [IP SLA Responder Service](#)

Please see Part 1: Cisco VNEs in this guide for information about which devices support the various technologies.

IP

IP is a network layer (Layer 3) protocol that contains addressing information and some control information that enables packets to be routed. IP is documented in RFC 791 and is the primary network layer protocol in the Internet protocol suite. Along with TCP, IP represents the heart of the Internet protocols. IP has two primary responsibilities: providing connectionless, best-effort delivery of datagrams through an internetwork; and providing fragmentation and reassembly of datagrams to support data links with different maximum transmission unit (MTU) sizes.

ARP

Address Resolution Protocol (ARP) is a protocol for mapping an IP address to a physical machine address (a MAC address) that is recognized in the local network. For example, in IP version 4 (IPv4), the most common level of IP in use today, an address is 32 bits long. In an Ethernet LAN, however, addresses for attached devices are 48 bits long. A table, usually called the ARP cache, is used to maintain a correlation between each MAC address and its corresponding IP address. ARP provides the protocol rules for making this correlation and providing address conversion in both directions.

HSRP

Hot Standby Router Protocol (HSRP) is a routing protocol that provides automatic router backup by allowing host computers on the Internet to use multiple routers that act as a single virtual router, maintaining connectivity even if the first hop router fails, because other routers are on hot standby and ready to go. The protocol is fully compatible with Novell's Internetwork Packet Exchange (IPX), AppleTalk, and Banyan VINES, and (in some configurations) with Xerox Network Systems (XNS) and DECnet.

Developed by Cisco and specified in RFC 2281, HSRP ensures that only a single router (called the active router) is forwarding packets on behalf of the virtual router at any given time. A standby router is chosen to be ready to become the active router, in the event that the current active router fails. HSRP defines a mechanism used to determine active and standby routers by referring to their IP addresses. Once these are determined, the failure of an active router will not cause any significant interruption of connectivity.

On any given LAN, there may be multiple, possibly overlapping, hot standby groups, each with a single MAC address and IP address. The IP address should belong to the primary subnet, but must be different from any actual or virtual addresses allocated to any routers or hosts on the network.

GRE

Generic Routing Encapsulation (GRE) is a tunneling protocol, originated by Cisco Systems and standardized in RFC 2784. It was designed to encapsulate a wide variety of network layer packets inside IP tunneling packets. The original packet is the payload for the final packet. The protocol is used on the Internet to secure VPNs.

Carrier-Grade NAT (CGN)

Carrier-Grade NAT is large-scale NAT, capable of providing private-IPv4-to-public-IPv4 translation in the order of millions of translations. Carrier-Grade NAT can support several hundred thousand subscribers with the bandwidth throughput of at least 10Gb/s full-duplex. With IPv4 addresses reaching depletion, Carrier-Grade NAT is vital in providing private IPv4 connectivity to the public IPv4 internet.

IPv6

IP version 6 (also known as IPv6, specified in RFC 2373, "IP Version 6 Addressing Architecture") is the successor to IPv4. The changes from IPv4 to IPv6 fall primarily into these categories:

- **Expanded Addressing Capabilities**—IPv6 increases the IP address size from 32 bits to 128 bits, supporting more levels of addressing hierarchy, a much greater number of addressable nodes, and simpler auto-configuration of addresses. It improves scalability of multicast routing by adding a scope field to multicast addresses. It also defines a new type of “anycast” address, used to send a packet to any one of a group of nodes.
- **Header Format Simplification**— Some IPv4 header fields have been dropped or made optional, to reduce the common-case processing cost of packet handling and to limit the bandwidth cost of the IPv6 header.
- **Improved Support for Extensions and Options**—Changes in the way IP header options are encoded allows for more efficient forwarding, less stringent limits on the length of options, and greater flexibility for introducing new options in the future.
- **Flow Labeling Capability**—This new capability enables the labeling of packets belonging to particular traffic flows for which the sender requests special handling, such as non default quality of service or real-time service.

Currently, Cisco ANA support for IPv6 has the following limitations:

- ANA does not support native IPv6 devices; this implies use of dual stack on all devices.
- ANA implementation of IPv6 is limited to discovery and display of IPv6-enabled interfaces and IPv6-enabled VPNs.
- Fault management of IPv6-enabled interfaces and VPN is limited to parsing and displaying the events reported for those interfaces and VPNs. ANA does not correlate or otherwise process these events.
- None of the routing protocols are supported for IPv6-enabled interfaces. To get topology links among IPv6-enabled interfaces, Cisco Discovery Protocol (CDP) must be enabled.

Provider Backbone Bridge (PBB)

Provider backbone bridges (PBBs), specified by IEEE 802.1ah-2008, provide a way to increase the number of service provider supported Layer 2 service instances beyond the number supported by QinQ and VPLS. PBB adds a backbone VLAN tag and backbone destination and source MAC addresses to encapsulate customer Ethernet frames and create a MAC tunnel across core switches.

Cisco ANA models the IB type of Backbone edge bridges which includes both I-type and B-type components.

IP SLA Responder Service

Cisco IOS Service Level Agreements (SLAs) software allows you to analyze IP service levels for IP applications and services by using active traffic monitoring to measure network performance. The IP SLA responder is a component embedded in the destination Cisco device that allows the system to anticipate and respond to IP SLAs request packets. The responder provides accurate measurements without requiring dedicated probes. The responder uses the Cisco IOS IP SLAs Control Protocol to provide a mechanism through which it can be notified on which port it should listen and respond.

Two-Way Active Measurement Protocol (TWAMP) defines a standard for measuring round-trip network performance between any two devices that support the protocol.

Information Model Objects (IMOs)

This section describes the following IMOs:

- [IP Interface \(IIPInterface\)](#)
- [IP Multiplexer Entry \(IIPMuxEntry\)](#)
- [IP Interface Address \(IIPInterfaceAddress\)](#)
- [IP Subnetwork \(IPSubnet\)](#)
- [Routing Entity \(IRoutingEntity\)](#)
- [Routing Entry \(IRoutingEntry\)](#)
- [ARP Entity \(IARPEntity\)](#)
- [ARP Entry \(IARPEntity\)](#)
- [IP Address Pool \(IIPPool\)](#)
- [IP Range-Based Address Pool Entry \(IIPRangeBasedIPPoolEntry\)](#)
- [IP Subnet-Based Address Pool Entry \(IIPSubnetBasedIPPoolEntry\)](#)
- [Hot Standby Router Protocol \(HSRP\) Group Entry \(IHSRPGroupEntry\)](#)
- [Generic Routing Encapsulation \(GRE\) Tunnel Interface \(ITunnelGRE\)](#)
- [Bridge ILan \(IBridgeILan\)](#)
- [IB Bridge Entry \(IIBBridgeEntry\)](#)
- [IP SLA Responder Service \(IIPSLAResponderService\)](#)
- [IP SLA IP Address Port Pair \(IIPSLAIPAddressPortPair\)](#)
- [CGN Service \(ICgnService\)](#)
- [CGN Statistics Entry \(ICgnStatsEntry\)](#)
- [CGN Service Address Pool \(ICgnServiceAddressPool\)](#)
- [CGN Service Location \(ICgnServiceLocation\)](#)

IP Interface

The network layer [IP Interface](#) IMO represents the IP-level functionality of an interface configuration in a network element. Its Containing Termination Points attribute is its primary binding to a data link layer interface object. It is accessed primarily by a [Routing Entity](#).

Table 10-1 *IP Interface (IIPInterface)*

Attribute Name	Attribute Description	Scheme	Polling Interval
IP Address	IP addresses (including IPv6)	Product	Configuration
Subnetwork Mask	IP subnetwork masks (including IPv6)	Product	Configuration
IP Interface Addresses Array	Array of all IP Interface Addresses (including IPv6)	Product	Configuration
Interface Name	Interface name	Product	Configuration
Interface Description	Interface description	Product	Configuration
IP Interface State	IP interface state (<i>Unknown, Up, Down</i>)	Product	Configuration

Table 10-1 *IP Interface (IIPInterface) (continued)*

Attribute Name	Attribute Description	Scheme	Polling Interval
OSPF Interface Cost	$2 \times 10^9 / \langle \text{interface speed in BPS} \rangle$	Any	Configuration
Broadcast Address	The broadcast address of the subnetwork	Any	Configuration
MTU	Maximum transmit units	Any	Configuration
Lookup Method	Lookup method (<i>Route Table First, Host Table First</i>)	Any	Configuration
Address Resolution Type	Address resolution type	Any	Configuration
ARP Timeout	ARP table entry aging timeout	Any	Configuration
Secured ARP	Secured ARP settings (<i>Enable, Disable</i>)	Any	Configuration
ICMP Mask Reply	Control message mask reply	Any	Configuration
IGMP Proxy	Group management proxy	Any	Configuration
HSRP Groups	Arrays of Hot Standby Router Protocol (HSRP) Group Entry (valid only for Cisco routers that implement HSRP)	Any	Configuration
IP Multiplexing Table	Array of IP Multiplexing Entries	Any	Configuration
IANA Type	Internet Assigned Numbers Authority (IANA) type of the sublayer	N/A	N/A
Containing Termination Points	Underlying termination points (connection or physical)	Any	N/A
Contained Connection Termination Points	Bound connection termination points	Any	N/A

IP Multiplexer Entry

The [IP Multiplexer Entry](#) IMO represents an entry in the IP Multiplexing Table of an [IP Interface](#) object. It is used when an [IP Interface](#) is bound to multiple virtual connection-based data link layer interfaces (such as [ATM Interface](#) and [Frame Relay Interface](#)) in order to map a destination IP subnet to a specific virtual connection.

Table 10-2 *IP Multiplexer Entry (IIPMuxEntry)*

Attribute Name	Attribute Description	Scheme	Polling Interval
Termination Point	Virtual data link layer encapsulation	Any	Configuration
Destination IP Subnet	Destination IP subnet	Any	Configuration

IP Interface Address

The [IP Interface Address](#) IMO represents one of several possible IP addresses and their subnetwork masks that can be assigned to an [IP Interface](#) using an [IP Subnetwork](#) IMO. It indicates whether it is the primary or a secondary address.

Table 10-3 *IP Interface Address (IIPInterfaceAddress)*

Attribute Name	Attribute Description	Scheme	Polling Interval
Type	IP address type (for IPv4: <i>Primary, Secondary</i> ; for IPv6, <i>IPv6 Link-local, IPv6 Unicast, IPv6 Anycast, IPv6 Multicast</i>)	Any	Configuration
IP Subnet	IP subnetwork (supports IPv6)	Any	Configuration

IP Subnetwork

The [IP Subnetwork](#) type (it is not an IMO) describes either an IP Subnetwork Address (with the host part zeroed) or, alternatively, a host IP address along with the IP subnetwork mask.

Table 10-4 *IP Subnetwork (IPSubnet)*

Attribute Name	Attribute Description	Scheme	Polling Interval
IP Address	IP address (supports IPv6)	Any	Configuration
Subnetwork Mask	IP subnetwork mask (supports IPv6)	Any	Configuration

Address Family

The [Address Family](#) IMO represents the VRF route targets associated with IPv4 and IPv6 address family configurations.

Table 10-5 *Address Family (IAddressFamily)*

Attribute Name	Attribute Description	Scheme	Polling Interval
Address family type	Address family type (<i>IPv4 address family, IPv6 address family</i>)	Any	Configuration
Export route targets	List of export route targets	Any	Configuration
Import route targets	List of import route targets	Any	Configuration

Routing Entity

The [Routing Entity](#) IMO represents the routing and address resolution protocol-independent forwarding component of an IP router. It is bound by its Logical Sons attribute to all the network-layer [IP Interface](#) IMOs among which this Routing Entity is routing IP packets.

Table 10-6 **Routing Entity (IRoutingEntity)**

Attribute Name	Attribute Description	Scheme	Polling Interval
Routing Table	Array of Equivalent (Shared Destination) Routing Entries	Product	Configuration
ARP Entity	Address resolution entity (ARP Entity)	Product	Configuration
Routing Table Changes	Routing table changes count	Any	Configuration
Name	Routing entity name	Any	Configuration
Logical Sons	Array of all IP Interfaces which IP packets are being routed between, by this Routing Entity	Any	N/A

Routing Entry

The [Routing Entry](#) IMO describes a routing table's entries. Each routing table entry is an array of entries sharing a single [IP Subnetwork](#) destination. Based on their protocol type, some of a device's routing table entries which are not relevant to the Cisco ANA Information Model may be omitted from this table structure.

Table 10-7 **Routing Entry (IRoutingEntry)**

Attribute Name	Attribute Description	Scheme	Polling Interval
Destination IP Subnet	Final destination IP subnet	Product	Configuration
Next Hop IP Address	Next hop IP address	Product	Configuration
Type	Routing entry type (<i>Null, Other, Invalid, Direct, Indirect, Static</i>)	Product	Configuration
Routing Protocol Type	Routing protocol type (<i>Null, Other, Local, Network Managed, ICMP, EGP, GGP, Hello, RIP, IS-IS, ES-IS, Cisco IGRP, BBN SPF IGP, OSPF, BGP, EIGRP</i>)	Product	Configuration
Outgoing Interface Name	Outgoing IP interface name	Product	Configuration
Prefix Length	The number of bits set in the subnet mask (the shorthand way of expressing the subnet mask).	Product	Configuration

ARP Entity

The [ARP Entity](#) IMO describes a domain-wide IP address to MAC Address Resolution Protocol (ARP) entity.

Table 10-8 *ARP Entity (IARPEntity)*

Attribute Name	Attribute Description	Scheme	Polling Interval
ARP Table	Array of ARP Entries	Product	Configuration

ARP Entry

The [ARP Entry](#) IMO describes a domain-wide IP address to MAC Address Resolution Protocol (ARP) table entry.

Table 10-9 *ARP Entry (IARPEntity)*

Attribute Name	Attribute Description	Scheme	Polling Interval
IP Address	IP address	Product	Configuration
MAC Address	MAC address	Product	Configuration
Port	Data link layer (MAC) interface	Product	Configuration
Entry Type	ARP entry type (<i>Null, Other, Invalid, Dynamic, Static</i>)	Product	Configuration

IP Address Pool

The [IP Address Pool](#) IMO, with its associated [IP Range-Based Address Pool Entry](#) and [IP Subnet-Based Address Pool Entry](#) IMOs, describes an IP address pool of a gateway or router device. Protocols such as Dynamic Host Configuration Protocol (DHCP) and IP Control Protocol (IPCP) use these pools to distribute IP assignments to local and remote parties.

Table 10-10 *IP Address Pool (IIPPool)*

Attribute Name	Attribute Description	Scheme	Polling Interval
IP Address Pool Entries	Array of IP Range Based Address Pool Entries or IP Subnet Based Address Pool Entries	Any	Configuration
Name	IP addresses pool name	Any	Configuration
Index	IP addresses pool index	Any	Configuration

IP Range-Based Address Pool Entry

See the description for [IP Address Pool](#).

Table 10-11 IP Range-Based Address Pool Entry (*IIPRangeBasedIPPoolEntry*)

Attribute Name	Attribute Description	Scheme	Polling Interval
Start IP Address	Start IP address of the IP address pool	Any	Configuration
End IP Address	End IP address of the IP address pool	Any	Configuration
Unused Addresses	Unused addresses count	Any	Configuration
Used Addresses	Used addresses count	Any	Configuration
Reserved Addresses	Reserved addresses count	Any	Configuration

IP Subnet-Based Address Pool Entry

See the description for [IP Address Pool](#).

Table 10-12 IP Subnet-Based Address Pool Entry (*IIPSubnetBasedIPPoolEntry*)

Attribute Name	Attribute Description	Scheme	Polling Interval
IP Subnet	IP Subnetwork of the IP address pool	Any	Configuration
Unused Addresses	Unused addresses count	Any	Configuration
Used Addresses	Used addresses count	Any	Configuration
Reserved Addresses	Reserved addresses count	Any	Configuration

Hot Standby Router Protocol (HSRP) Group Entry

The [Hot Standby Router Protocol \(HSRP\) Group Entry](#) IMO represents both the configuration and the result of running HSRP within a group of routers connected to the same segment of an Ethernet network. HSRP provides backup for router failures by presenting the group of routers to the LAN as a single virtual router with a single set of IP and MAC addresses.

Table 10-13 Hot Standby Router Protocol (HSRP) Group Entry (*IHSRPGroupEntry*)

Attribute Name	Attribute Description	Scheme	Polling Interval
Group Number	Group number	Product	Configuration
Port Description	Port description	Product	Configuration
Priority	Priority from 0 (<i>Lowest</i>) to 255 (<i>Highest</i>) used for active router selection	Product	Configuration
Coupled Router	Coupled active or standby router IP address (as the grouping is implemented using only two routers)	Product	Configuration
State	Protocol state (<i>Disabled, Initial, Learn, Listen, Speak, Standby, Active</i>)	Product	Configuration
Virtual IP Address	Virtual IP address used by this group	Product	Configuration
Virtual MAC Address	Virtual MAC address used by this group	Product	Configuration

Generic Routing Encapsulation (GRE) Tunnel Interface

The network-layer [Generic Routing Encapsulation \(GRE\) Tunnel Interface](#) IMO represents a GRE tunnel interface configuration in a network element. It is accessed primarily by an [IP Interface](#) bound by its Contained Connection Termination Points attribute.

Table 10-14 **Generic Routing Encapsulation (GRE) Tunnel Interface (ITunnelGRE)**

Attribute Name	Attribute Description	Scheme	Polling Interval
Name	Tunnel name	Product	Configuration
Tunnel Destination and Source	Tunnel destination and source IP addresses	Product	Configuration
IP Address	Primary IP address	Product	Configuration
IP Interface State	IP interface state (<i>Unknown, Up, Down</i>)	Any	Configuration
IANA Type	Internet Assigned Numbers Authority (IANA) type of the sublayer	N/A	N/A
Containing Connection Termination Points	Underlying termination points (connection or physical)	Any	N/A
Contained Connection Termination Points	Bound connection termination points	Any	N/A
Keep Alive State	Indicates whether the GRE keep alive is <i>set</i> or <i>not set</i>	Any	N/A
Keep Alive Time	The interval at which GRE will try to send keepalive packets	Any	N/A
Keep Alive Retry	Number of times the GRE will try to send keepalive packets without a response before bringing down the interface or tunnel protocol	Any	N/A

Bridge ILan

This IMO encapsulates the bridge mapping associations between the backbone edge bridges and the BridgeILan tunnel.

Table 10-15 **Bridge ILan (IBridgeILan)**

Attribute Name	Attribute Description	Scheme	Polling Interval
IBBridgeMapping	The object which associates the I-SID, I type Backbone Edge Bridge and B type Backbone Edge Bridge with the BridgeILan tunnel.	IPCore	Configuration
ID	On 7600 devices, this is the ID of the created MAC tunnel. On ASR 9000 devices, the ID is composed from the Bridge group and Bridge domain on the B-Bridge component.	IPCore	Configuration

IIBridgeEntry

This IMO encapsulates the MAC-in-MAC tunnel properties, including I-SID and XID of the I-Bridge Component and the XID of the B-Bridge component.

Table 10-16 IB Bridge Entry (*IIBBridgeEntry*)

Attribute Name	Attribute Description	Scheme	Polling Interval
B Type Bridge	The B type Backbone Edge Bridge ID.	IPCore	Configuration
I Type Bridge	The I type Backbone Edge Bridge ID.	IPCore	Configuration
I-SID	The 24 bit Service Instance ID.	IPCore	Configuration

IP SLA Responder Service

The [IP SLA Responder Service](#) IMO represents the IMO interface for the IP SLA Responder that allows the system to anticipate and respond to IP SLAs request packets. Cisco IP SLA allows monitoring of network performance between Cisco routers or from a Cisco router to a remote IP device. This object supports UDP_ECHO and TCP_CONNECT operation types. The UDP_ECHO operation measures end-to-end response time or connectivity between a Cisco router and IP devices. The TCP_CONNECT operation tests the connection to specific destination ports on a remote server.

Table 10-17 IP SLA Responder Service (*IIPSLAResponderService*)

Attribute Name	Attribute Description	Scheme	Polling Interval
Responder Status	Status of the IP SLA Responder (<i>Up, Down</i>).	Product	Configuration
TWAMP Responder Status	Status of the IP SLA TWAMP responder (<i>Up, Down</i>).	Product	Configuration
TCP Connect	Destination IP address and port number used for the TCP connect operation, as in IP SLA Address Port Pair .	Product	Configuration
UDP Echo	Destination IP address and port number used for the UDP echo operation.	Product	Configuration

IP SLA Address Port Pair

The [IP SLA Address Port Pair](#) IMO represents the pair consisting of IP address and port for the TCP Connect and UDP Echo data in [IP SLA Responder Service](#). The IP Address can be IPv4 or IPv6.

Table 10-18 IP SLA IP Address Port Pair (*IIPSLAIPAddressPortPair*)

Attribute Name	Attribute Description	Scheme	Polling Interval
IP Address	The IP address in the pair. The IP address can be IPv4 or IPv6.	Product	Configuration
Port	The port in the pair.	Product	Configuration

CGN Service

The [CGN Service](#) object models the Carrier Grade NAT service, including its name, statistics, address pools, associated service infra interface and service app interface and locations.

Table 10-19 *CGN Service (IcgnService)*

Attribute Name	Attribute Description	Scheme	Polling Interval
CGN Name	The service name configured for the CGN service.	ipcore	configuration
Statistics	A set of statistics relating to the CGN service. See CGN Statistics Entry .	ipcore	configuration
Address Pools	The private to public address pool mapping that is managed by the CGN service.	ipcore	configuration
Locations	The preferred locations where the CGN service is configured.	ipcore	configuration
Service Interfaces	The service interfaces associated with the CGN service (service infra and service app). The service infra interface represents the control connection to the card running the CGN service. The service app interfaces are used for delivering packets to and from the card running the CGN service.	ipcore	configuration

CGN Statistics Entry

The [CGN Statistics Entry](#) object models all the statistics for a given Carrier Grade NAT service as a name value pair.

The supported statistics are:

- Translations create rate
- Translations delete rate
- Inside to outside forward rate
- Outside to inside forward rate
- Inside to outside drops port limit exceeded
- Inside to outside drops system limit reached
- Inside to outside drops resource depletion

Table 10-20 *CGN Statistics Entry (ICgnStatsEntry)*

Attribute Name	Attribute Description	Scheme	Polling Interval
Statistics Name	The name of the statistic for the CGN service.	ipcore	configuration
Statistics Value	The value of the statistic for the CGN service.	ipcore	configuration

CGN Service Address Pool

The [CGN Service Address Pool](#) object models the address pool configured for a given Carrier Grade NAT service, including its address family, address pool, inside VRFs and outside VRFs.

Table 10-21 *CGN Service Address Pool (ICgnServiceAddressPool)*

Attribute Name	Attribute Description	Scheme	Polling Interval
Outside VRF	The outside VRF associated with this address pool. The outside VRF is used for packet flow from the public network to the private network.	ipcore	configuration
Address Pool	The range of IP addresses that is managed by the outside VRF.	ipcore	configuration
Inside VRF	The inside VRF associated with this address pool. The inside VRF is used for packet flow from the private network to the public network.	ipcore	configuration
Address Family	The address family type that is translated by the inside VRF, either IPv4 or IPv6.	ipcore	configuration

CGN Service Location

The [CGN Service Location](#) object models the service location configured for a given Carrier Grade NAT service.

Table 10-22 *CGN Service Location (ICgnServiceLocation)*

Attribute Name	Attribute Description	Scheme	Polling Interval
Instance Name	The preferred active location of the CGN service.	ipcore	configuration
Location	Hyperlink to the physical inventory of the preferred active location of the CGN service.	ipcore	configuration
Infra Interface	The interface that represents the control connection to the card running the CGN service,	ipcore	configuration
Location Type	The configured location type, active or standby.	ipcore	configuration
Redundancy Status	The operational state of the redundancy.	ipcore	configuration

CGN IP Interface

The [CGN IP Interface](#) object extends the [IP Interface](#) object as a differentiator for a CGN IP interface. See [IP Interface](#) for a description of the attributes associated with this object.

Network Topology

Discovery of the IP network layer is unsupported. However, IP addresses and subnets are used in signature and test of the underlying topology discovery (for example, MPLS, PPP, HDLC, BFD, GRE) when searching for the local IP address in any one-hop-away remote side's routing table. In particular, the local and remote IP addresses of [IP Interface](#) found under the same subnet are compared.

For more information, see [Chapter 15, “Multiprotocol Label Switching,”](#) [Chapter 23, “Point-to-Point Protocol,”](#) and [Chapter 24, “High-Level Data Link Control.”](#)

Service Alarms

The following alarms are supported for this technology:

- [All IP Interfaces Down, page 41-4](#)
- [GRE Tunnel Down, page 41-33](#)
- [HSRP Group Status Changed, page 41-34](#)
- [Carrier Grade NAT Translations Create Rate, page 41-16](#)
- [Carrier Grade NAT Translations Delete Rate, page 41-17](#)
- [Carrier Grade NAT Inside-to-Outside Forward Rate, page 41-18](#)
- [Carrier Grade NAT Outside-to-Inside Forward Rate, page 41-18](#)
- [Carrier Grade NAT Inside-to-Outside Drops Port Limit Exceeded, page 41-19](#)
- [Carrier Grade NAT Inside-to-Outside Drops System Limit Reached, page 41-20](#)
- [Carrier Grade NAT Inside-to-Outside Drops Resource Depletion, page 41-21](#)



CHAPTER 11

Routing Protocols

This chapter describes the level of support that Cisco ANA provides for routing protocols, as follows:

- [Technology Description, page 11-1](#)
- [Information Model Objects \(IMOs\), page 11-3](#)
- [Vendor-Specific Inventory and IMOs, page 11-7](#)
- [Network Topology, page 11-7](#)
- [Service Alarms, page 11-7](#)

Technology Description

This section provides the following IP technology descriptions:

- [BGP](#)
- [MP-BGP](#)
- [OSPF](#)
- [IS-IS](#)

Please see Part 1: Cisco VNEs in this guide for information about which devices support the various technologies.

BGP

The Border Gateway Protocol (BGP) routes traffic between autonomous systems. An autonomous system is a network or group of networks under common administration and with common routing policies. BGP exchanges routing information for the Internet and is the protocol used between ISPs. Customer networks, such as universities and corporations, usually employ an Interior Gateway Protocol (IGP), such as RIP or OSPF, to exchange routing information within their networks. Customers connect to ISPs, and ISPs use BGP to exchange customer and ISP routes. When BGP is used between autonomous systems, the protocol is referred to as external BGP (eBGP). If a service provider is using BGP to exchange routes within an autonomous system, the protocol is referred to as interior BGP (iBGP).

BGP is a very robust and scalable routing protocol, as evidenced by the fact that it is the routing protocol employed on the Internet. To achieve scalability at this level, BGP uses many route parameters, called attributes, to define routing policies and maintain a stable routing environment. BGP neighbors exchange full routing information when the TCP connection between neighbors is first established. When changes

to the routing table are detected, the BGP routers send to their neighbors only those routes that have changed. BGP routers do not send periodic routing updates, and BGP routing updates advertise only the optimal path to a destination network.

MP-BGP

Multiprotocol BGP (MP-BGP) adds capabilities to BGP to enable multicast routing policy throughout the Internet and to connect multicast topologies within and between BGP autonomous systems. That is, MP-BGP is an enhanced BGP that carries IP multicast routes. BGP carries two sets of routes, one set for unicast routing and one set for multicast routing. The routes associated with multicast routing are used by the Protocol Independent Multicast (PIM) to build data distribution trees.

eBGP/iBGP

As noted previously, BGP is an inter-autonomous system routing protocol. When BGP is used between autonomous systems (AS), the protocol is referred to as external BGP (eBGP). If a service provider is using BGP to exchange routes within an AS, then the protocol is referred to as interior BGP (iBGP).

OSPF

Open Shortest Path First (OSPF) is a routing protocol developed for IP networks by the IGP working group of the Internet Engineering Task Force (IETF). It was derived from several research efforts, including a version of OSI's IS-IS routing protocol.

OSPF has two primary characteristics:

- It is an open protocol. Its specification is in the public domain (RFC 1247).
- It is based on the Shortest Path First (SPF) algorithm, sometimes known as the Dijkstra algorithm.

OSPF is a link-state routing protocol that calls for the sending of link-state advertisements (LSAs) to all other routers within the same hierarchical area. Information on attached interfaces, metrics used, and other variables are included in OSPF LSAs. As OSPF routers accumulate link-state information, they use the SPF algorithm to calculate the shortest path to each node.

In addition to OSPF versions 1 and 2, Cisco ANA 3.7.1 supports OSPF version 3 which includes IPv6 feature implementation support.

IS-IS

Intermediate System to Intermediate System (IS-IS) is an OSI link-state hierarchical routing protocol that floods the network with link-state information to build a complete, consistent picture of a network topology. IS-IS distinguishes between Level 1 and Level 2 ISs. Level 1 ISs communicate with other Level 1 ISs in the same area. Level 2 ISs route between Level 1 areas and form an intradomain routing backbone.

Information Model Objects (IMOs)

This section describes the following IMOs:

- [BGP Neighbor Entry \(IBgpNeighbourEntry\)](#)
- [OSPF Process \(IOspfProcess\)](#)
- [OSPF Neighbor \(IOspfNeighbor\)](#)
- [OSPF Interface \(IOspfInterface\)](#)
- [SPF Timers \(ISpfTimers\)](#)
- [ISIS Process \(IISISProcess\)](#)
- [ISIS Metric \(IISISMetric\)](#)
- [ISIS Interface \(IISISInterface\)](#)
- [ISIS Neighbor \(IISISNeighbor\)](#)

BGP Neighbor Entry

The [BGP Neighbor Entry](#) IMO represents both the configuration and the outcome of running the Border Gateway Protocol (BGP) within a group of participating routers in a BGP neighborhood. It contains information about the connection with a remote BGP peer. It is the entry of the BGP Neighbors Table attribute of the [Multi Protocol BGP Entity](#) object (see [VPN and VRF](#)), representing the BGP routing service concept in the IMO.

Table 11-1 *BGP Neighbor Entry (IBgpNeighbourEntry)*

Attribute Name	Attribute Description	Scheme	Polling Interval
Remote Identifier	Identifier of the remote peer (<i>IP Address</i>)	Any	Configuration
Neighbor Type	Neighbor type (<i>Null, Client, Non Client</i>)	Any	Configuration
Distributing Interface	Distributing IP interface	Any	Configuration
Remote Address	Remote peer IP address	Any	Configuration
Remote Autonomous System	Remote peer autonomous system	Any	Configuration
Status	Status (<i>Null, Idle, Connect, Active, Open Sent, Open Confirm, Established</i>)	Any	Configuration
Hold Time	Established hold time in seconds	Any	Configuration
Keep Alive Time	Established keepalive time in seconds	Any	Configuration
Peer Autonomous System (AS)	The AS to which the peer belongs.	Any	Configuration

OSPF Process

The [OSPF Process](#) IMO contains identifying information for the OSPF process and the router on which it is configured.

Table 11-2 *OSPF Process (IOspfProcess)*

Attribute Name	Attribute Description	Scheme	Polling Interval
Process ID	Unique process identifier.	Any	Configuration
OSPF Version	The OSPF version (v1, v2 or v3)	Any	Configuration
Router ID	The IP address of the OSPF process router.	Any	Configuration

OSPF Neighbor

The [OSPF Neighbor](#) IMO contains information about the OSPF neighboring router.

Table 11-3 *OSPF Neighbor (IOspfNeighbor)*

Attribute Name	Attribute Description	Scheme	Polling Interval
Neighbor ID	IP Address that represents the OSPF Router ID of the neighboring router. The Neighbor ID is learned when Hello packets are received from the neighbor, or is configured if this is a virtual adjacency.	Any	Configuration
Outgoing Interface	Identifier of the OSPF Interface through which the neighbor is known.	Any	Configuration
Neighbor State	The state of a conversation being held with a neighboring router (<i>down, attempt, init, 1-way, 2-way, exstart, exchange, loading, removed and full.</i>)	Any	Configuration
Neighbor Interface Address	IP Address of the neighbor's OSPF interface.	Any	Configuration
Area ID	The ID of the network segment to which the neighbor belongs.	Any	Configuration

OSPF Interface

The [OSPF Interface](#) IMO represents the connection between the OSPF router and the attached network.

Table 11-4 *OSPF Interface (IOspfInterface)*

Attribute Name	Attribute Description	Scheme	Polling Interval
Area ID	The Area ID of the area to which the attached network belongs. All routing protocol packets originating from the interface are labelled with this Area ID.	Any	Configuration
Network Type	The OSPF interface type (point-to-point, broadcast, NBMA, or virtual link.)	Any	Configuration
Cost	The cost of sending a data packet on the interface, expressed in the link state metric.	Any	Configuration
State	The functional level of an interface (down, loopback, waiting, point-to-point, DR other, backup, DR). State determines whether or not full adjacencies are allowed to form over the interface.	Any	Configuration
Interface Address	The IP address of the interface used by the OSPF process.	Any	Configuration
Interface Name	The name of the interface used by the OSPF process.	Any	Configuration
Network Type	The type of network to which the OSPF interface belongs.	Any	Configuration
IF Priority	An 8-bit unsigned integer representing the priority of the router. When two routers attached to a network both attempt to become designated router, the one with the highest router priority takes precedence. A router whose router priority is set to 0 is ineligible to become the designated router on the attached network.	Any	Configuration
DR ID	The router ID of the designated router that advertises link state for the network.	Any	Configuration
BDR ID	The router ID of the backup designated router that becomes the designated router upon failure of the current designated router.	Any	Configuration

SPF Timers

The [SPF Timers](#) IMO contains parameters that control OSPF shortest path first (SPF) throttling.

Table 11-5 *SPF Timers (ISpfTimers)*

Attribute Name	Attribute Description	Scheme	Polling Interval
Schedule Delay	Initial delay to schedule an SFP calculation after a change, in milliseconds.	Product	Configuration
Min Hold Time	Minimum hold time between two consecutive SPF calculations, in milliseconds.	Product	Configuration
Max Wait Time	Maximum wait time between two consecutive SPF calculations, in milliseconds.	Product	Configuration

IS-IS Process

The [IS-IS Process](#) IMO contains identifying information for the IS-IS process and the router on which it is configured.

The tag (process ID) can be used to identify multiple IS-IS processes by providing a meaningful name for a routing process. This name must be unique among all IP router processes for a given router. If the tag is not specified, the process is referenced with a null tag.

Table 11-6 *ISIS Process (IISISProcess)*

Attribute Name	Attribute Description	Scheme	Polling Interval
ISIS Interface	The interfaces running the IS-IS protocol.	IPCore	Configuration
ISIS Metric	Metric used for the redistributed route.	IPCore	Configuration
ISIS Neighbor	The routers with which this router has IS-IS adjacencies.	IPCore	Configuration
Manual Area Address	The ID of the IS-IS area to which the router belongs.	IPCore	Configuration
IS Type	The type of the IS (<i>Level 1, Level 2 or Level 1 and 2</i>).	IPCore	Configuration
System ID	The system ID of the router.	IPCore	Configuration
Process ID	The area tag of the IS-IS instance. When there are multiple IS-IS areas, the area tag is used to identify the IS-IS instance.	IPCore	Configuration

ISIS Metric

The [ISIS Metric](#) IMO represents the metric used for the redistributed route. This is a number in the range 0-63 if the router is configured with the metric-style narrow command or a number in the range 0 - 16777215 if the router is configured with the metric-style transition or metric-style wide command. Default value is 10.

Table 11-7 *ISIS Metric (IISISMetric)*

Attribute Name	Attribute Description	Scheme	Polling Interval
IS Type	Level at which the Intermediate System is running (<i>Level 1, Level 2 or Level 1 and 2</i>).	IPCore	Configuration
Metric Style	The type of metric (<i>Narrow, Transient, Wide</i>).	IPCore	Configuration
Metric Value	The value of the metric.	IPCore	Configuration
Address Family	The IP address type (<i>IPv4, IPv6</i>).	IPCore	Configuration

ISIS Interface

The [ISIS Interface](#) IMO represents the interfaces on which the IS-IS is configured.

Table 11-8 *ISIS Interface (IISISInterface)*

Attribute Name	Attribute Description	Scheme	Polling Interval
Interface Name	The interface name of the neighbor.	IPCore	Configuration
Interface OID	The interface on which the IS-IS is configured.	IPCore	Configuration

ISIS Neighbor

The [ISIS Neighbor](#) IMO represents the routers with which this router has IS-IS adjacencies.

Table 11-9 *ISIS Neighbor (IISISNeighbor)*

Attribute Name	Attribute Description	Scheme	Polling Interval
IS Type	The IS type of the neighbor (<i>Level 1, Level 2 or Level 1 and 2</i>).	IPCore	Configuration
System ID	The identifier for the neighbor system.	IPCore	Configuration
Admin State	The state of the neighbor (<i>up, down</i>).	IPCore	Configuration
Hold Time	Holding time, in seconds, for this adjacency. The value is based on received IS-to-IS Hello (IIH) PDUs and the elapsed time since receipt.	IPCore	Configuration
SNPA	Subnetwork point of attachment (SNPA) for the neighbor.	IPCore	Configuration
Interface Name	The interface name of the neighbor.	IPCore	Configuration
IP Address	The IP address of the neighbor.	IPCore	Configuration
Address Family	The IP address type (IPv4, IPv6).	IPCore	Configuration

Vendor-Specific Inventory and IMOs

There are no vendor-specific inventory or IMOs for this technology.

Network Topology

Please see [Chapter 38, “Cisco ANA VNE Topology”](#).

Service Alarms

The following alarms are supported for this technology:

- [BGP Neighbor Loss, page 41-9](#)
- [BGP Process Down, page 41-10](#)
- [BGP Link Down, page 41-7](#)



CHAPTER 12

VPN and VRF

This chapter describes the level of support that Cisco ANA provides for Virtual Private Networks (VPN) and Virtual Routing and Forwarding (VRF), as follows:

- [Technology Description, page 12-1](#)
- [Information Model Objects \(IMOs\), page 12-2](#)
- [Vendor-Specific Inventory and IMOs, page 12-4](#)
- [Network Topology, page 12-4](#)
- [Service Alarms, page 12-5](#)

Technology Description

This section provides the following VPN and VRF technology descriptions:

- [VRF](#)
- [VRF-Lite \(Multi-VRF\)](#)
- [6VPE](#)

Please see Part 1: Cisco VNEs in this guide for information about which devices support the various technologies.

VRF

Virtual Routing and Forwarding (VRF) is an IP technology that allows multiple instances of a routing table to coexist on the same router at the same time. Because the routing instances are independent, the same or overlapping IP addresses can be used without conflict. “VRF” is also used to refer to a routing table instance that can exist in one or multiple instances per each VPN on a Provider Edge (PE) router.

VRF-Lite (Multi-VRF)

VRF-Lite is an application based on VRF that extends the concept of VRF to the Customer Edge (CE) router on the customer’s premises. It supports multiple, overlapping, independent routing and forwarding tables per customer.

Any routing protocol supported by normal VRF can be used in a VRF-Lite CE implementation. The CE supports traffic separation between customer networks. As there is no MPLS functionality on the CE, no label exchange happens between the CE and PE.

6VPE

IPv6 on VPN to Provider Edge (6VPE, RFC 2547) permits IPv6 domains to communicate with each other over an IPv4 core network, without explicit tunnel setup, requiring only one IPv4 address per IPv6 domain. 6VPE operates much like a normal IPv4 MPLS VPN provider edge, but with the addition of IPv6 support within VRF. It lets service providers support IPv6 over operational IPv4 MPLS backbones without requiring dual-stacking within the MPLS core, representing a large cost savings over core re-engineering. Only PE equipment must be dual-stack, to support awareness of both IPv4 and IPv6 access devices. 6VPE provides logically separate routing table entries for VPN member devices.

Information Model Objects (IMOs)

This section describes the following IMOs:

- [Virtual Routing Forwarding \(VRF\) Entity \(IVrf\)](#)
- [Virtual Routing Entry \(IVrfEntry\)](#)
- [Multi Protocol BGP Entity \(IMpBgp\)](#)
- [Equivalent Cross Virtual Routing Entry \(ICrossVrf\)](#)
- [Cross Virtual Routing Entry \(ICrossVrfRoutingEntry\)](#)

Virtual Routing Forwarding (VRF) Entity

The [Virtual Routing Forwarding \(VRF\) Entity](#) object describes the routing and address resolution protocols' independent forwarding component of a MPLS-BGP based VPN router. It is bound by its Logical Sons attribute to all the Network layer [IP Interface](#) objects among which it is routing IP packets.

Table 12-1 *Virtual Routing Forwarding (VRF) Entity (IVrf)*

Attribute Name	Attribute Description	Scheme	Polling Interval
Virtual Routing Table	Array of Equivalent Routing Entries	IPCore	Configuration
Exported Route Targets	Array of route target identifiers	IPCore	Configuration
Imported Route Targets	Array of route target identifiers	IPCore	Configuration
Address Families	List of the address families (IPv4, IPv6, or both)	IPCore	Configuration
Route Distinguisher	Route distinguisher	IPCore	Configuration
ARP Entity	Address Resolution Entity (ARP Entity) (see Internet Protocol)	IPCore	Configuration
Name	VRF name	IPCore	Configuration
Logical Sons	Array of all IP Interfaces among which this Virtual Routing Forwarding (VRF) Entity is routing IP packets	IPCore	N/A
Description	Description of the VRF	IPCore	Configuration

Table 12-1 *Virtual Routing Forwarding (VRF) Entity (IVrf) (continued)*

Attribute Name	Attribute Description	Scheme	Polling Interval
Import Route-map	Name of the VRF import route map used to import IP prefixes into the VRF.	IPCore	Configuration
Export Route-map	Name of the VRF export route map used to export IP prefixes from the VRF.	IPCore	Configuration

Virtual Routing Entry

The [Virtual Routing Entry](#) object describes a routing table's entries.

Table 12-2 *Virtual Routing Entry (IVrfEntry)*

Attribute Name	Attribute Description	Scheme	Polling Interval
Next Hop BGP Address	Next hop BGP IP address	IPCore	Configuration
Incoming and Outgoing Inner Label	Incoming and outgoing inner MPLS label	IPCore	Configuration
Outer Label	Outer MPLS label	IPCore	Configuration
Destination IP Subnet	Final destination IP subnet	IPCore	Configuration
Next Hop IP Address	Next hop IP address	IPCore	Configuration
Type	Route entry type (<i>Null, Other, Invalid, Direct, Indirect, Static</i>)	IPCore	Configuration
Routing Protocol Type	Routing protocol type (<i>Null, Other, Local, Network Managed, ICMP, EGP, GGP, Hello, RIP, IS-IS, ES-IS, Cisco IGRP, BBN SPF IGP, OSPF, BGP, EIGRP</i>)	IPCore	Configuration
Outgoing Interface Name	Outgoing IP interface name	IPCore	Configuration

Multi Protocol BGP Entity

The [Multi Protocol BGP Entity](#) object describes the BGP component of a MPLS-BGP based VPN router. It is bound by its Logical Sons attribute to all [Virtual Routing Forwarding \(VRF\) Entity](#) objects among which it is routing IP packets.

Table 12-3 *Multi Protocol BGP Entity (IMpBgp)*

Attribute Name	Attribute Description	Scheme	Polling Interval
BGP Identifier	Border Gateway Protocol (BGP) identifier	IPCore	Configuration
Local Autonomous System	Local peer autonomous system	IPCore	Configuration
Cross Virtual Routing Table	Array of Equivalent Cross Virtual Routing Entry	IPCore	Configuration
BGP Neighbors	Array of BGP neighbor entries (see Routing Protocols)	IPCore	Configuration
Logical Sons	Array of all Virtual Routing Forwarding (VRF) Entity objects among which this Multi Protocol BGP Entity is routing IP packets	IPCore	N/A

Equivalent Cross Virtual Routing Entry

The [Equivalent Cross Virtual Routing Entry](#) and [Cross Virtual Routing Entry](#) objects describe the first dimension of a cross virtual routing table, as an array of [Cross Virtual Routing Entry](#) objects sharing a single [Virtual Routing Forwarding \(VRF\) Entity](#) destination.

Table 12-4 *Equivalent Cross Virtual Routing Entry (ICrossVrf)*

Attribute Name	Attribute Description	Scheme	Polling Interval
Virtual Routing Entries	Array of Cross Virtual Routing Entry objects sharing a single destination	IPCore	Configuration
Virtual Routing Entity Name	Virtual Routing Entity (VRF) name	IPCore	Configuration

Cross Virtual Routing Entry

Table 12-5 *Cross Virtual Routing Entry (ICrossVrfRoutingEntry)*

Attribute Name	Attribute Description	Scheme	Polling Interval
Outgoing Virtual Routing Entity Identifier	Outgoing virtual routing entity Object Identifier (OID)	IPCore	Configuration
Incoming and Outgoing Virtual Routing Tags	Incoming and outgoing virtual routing tags	IPCore	Configuration
Destination IP Subnet	Final destination IP subnet	IPCore	Configuration
Next Hop IP Address	Next hop IP address	IPCore	Configuration
Type	Route entry type (<i>Null, Other, Invalid, Direct, Indirect, Static</i>)	IPCore	Configuration
Routing Protocol Type	Routing protocol type (<i>Null, Other, Local, Network Managed, ICMP, EGP, GGP, Hello, RIP, IS-IS, ES-IS, Cisco IGRP, BBN SPF IGP, OSPF, BGP, EIGRP</i>)	IPCore	Configuration
Outgoing Interface Name	Outgoing IP interface name	IPCore	Configuration

Vendor-Specific Inventory and IMOs

There are no vendor-specific inventory or IMOs for this technology.

Network Topology

Cisco ANA discovers MPLS-BGP-based VPN network topology by searching for the existence of the local [Virtual Routing Forwarding \(VRF\) Entity](#)'s imported route targets in any remote side's VRF entity exported route targets.

Please see [Chapter 38, "Cisco ANA VNE Topology"](#).

Service Alarms

There are no faults or alarms associated with this technology.



CHAPTER 13

Bidirectional Forwarding Detection

This chapter describes the level of support that Cisco ANA provides for Bidirectional Forwarding Detection (BFD), as follows:

- [Technology Description, page 13-1](#)
- [Information Model Objects \(IMOs\), page 13-2](#)
- [Vendor-Specific Inventory and IMOs, page 13-2](#)
- [Network Topology, page 13-2](#)
- [Service Alarms, page 13-3](#)

Technology Description

Please see Part 1: Cisco VNEs in this guide for information about which devices support the various technologies.

BFD

BFD provides rapid failure detection between forwarding engines while maintaining low overhead. It also provides a single, standardized method of link, device, or protocol failure detection at any protocol layer and over any media.

BFD can be used with the following protocols:

- OSPF
- BGP
- MPLS TE
- IPv4 (static)
- IPv6 (static)
- IS-IS

Information Model Objects (IMOs)

This section includes the following IMOs:

- [BFD Service](#)
- [BFD Session](#)

BFD Service

The [BFD Service](#) IMO contains a list of [BFD Session](#) objects.

Table 13-1 *BFD Service (IBfdService)*

Attribute Name	Attribute Description	Scheme	Polling Interval
Sessions	Returns a set of IBfdSession objects	Any	Configuration

BFD Session

The BFD Session IMO describes a single BFD session entry.

Table 13-2 *BFD Session (IBfdSession)*

Attribute Name	Attribute Description	Scheme	Polling Interval
Source IP	Source IP address of the session	Product	Configuration
Destination IP	Destination IP address of the session	Product	Configuration
Interval	The value of the requested interval	Product	Configuration
Multiplier	The value of the multiplier	Product	Configuration
Protocol	The routing protocol, such as OSPF, BGP or Static	Product	Configuration
State	The state of the session (<i>Up, Down, Init, Fail</i>)	Product	Configuration
Interface	OID of the physical interface	Product	Configuration
Process	Process ID of the session	Product	Configuration

Vendor-Specific Inventory and IMOs

There are no vendor-specific inventory or IMOs for this technology.

Network Topology

Cisco ANA discovers BFD topology by comparing the session parameters of potential BFD neighbors. In particular, it compares the source IP address and the destination IP address on both sides.

Service Alarms

The following alarms are supported for this technology:

- [BFD Connectivity Down, page 41-6](#)
- [BFD Neighbor Loss, page 41-6](#)

The BFD Connectivity Down alarm is cleared by the BFD Connectivity Up alarm. The BFD Neighbor Loss alarm is cleared by the BFD Neighbor Found alarm.



CHAPTER 14

Session Border Controller

This chapter describes the level of support that Cisco ANA provides for Session Border Controller (SBC), as follows:

- [Technology Description, page 14-1](#)
- [Information Model Objects \(IMOs\), page 14-2](#)
- [Vendor-Specific Inventory and IMOs](#)
- [Network Topology, page 14-20](#)
- [Service Alarms, page 14-20](#)

Technology Description

Please see Part 1: Cisco VNEs in this guide for information about which devices support the various technologies.

SBC

Session Border Control (SBC) is an IP multimedia security and operational enhancement function for session-oriented IP services, based on SIP/H.323/H.248 signaling. It enables direct IP-to-IP interconnect between multiple administrative domains for session-based services, providing protocol interworking, security, admission control, and management. It enables direct IP-to-IP peering between service providers, and between service providers and their business and residential customers.

The most common SBC deployment is Voice over IP (VoIP) peering between service providers. Up until now, this kind of peering was done by converting IP to public switched telephone network (PSTN) and using existing PSTN peering infrastructure, but the SBC approach has experienced phenomenal growth because it saves up to 75 percent in capital expenses.

Other important SBC services include:

- **Security**—Includes topology and address hiding, theft of service prevention, protocol normalization, and Denial of Service (DoS) protection.
- **Quality of Service (QoS) demarcation**—Allows inter-service-provider service level agreements.
- **Network Address Translation (NAT) traversal**—Required in service-provider-to-enterprise scenarios.
- **Billing**—Provides enhanced current accounting records with session information such as QoS, codecs used, and so on.

SBC controls the signaling and media traffic generated during the setup, conduct, and teardown of interactive media communications. Each of its terms, in this context, has a special meaning:

- **Session**—In VoIP, a *session* is the same as a call. Each call consists of exchanges of control signals, and one or more media streams and associated data. This data can include audio, video, and other data, as well as call statistics, QoS data, and information needed for control signaling. It is this session that the SBC controls.
- **Border**—The demarcation point between one part of a network and another. One example is the firewall separating a corporate LAN from the rest of the Internet. Other example are the filtering routers, security servers, and other network elements that can separate one department within a large corporation from others in the same corporation. The SBC controls the flow of session data across these borders.
- **Controller**—The administrative functions that the SBC performs on the session data streams as they cross the borders between parts of the network. In addition to basic control functions, an SBC can provide metrics, access security, and data conversion services.

**Note**

Cisco ANA currently provides SBC support on ASR 1000 routers only.

Information Model Objects (IMOs)

This section describes the following IMOs:

- [SBC Service \(ISbcService\)](#)
- [Service Border Element \(ISBE\)](#)
- [Data Border Element \(IDBE\)](#)
- [DBE Media Interface \(IDbeMediaInterface\)](#)
- [SBC Account \(ISbcAccount\)](#)
- [SBE AAA Interface \(ISbeAaaInterface\)](#)
- [SBE Billing Properties \(ISbeBillingProperties\)](#)
- [SBE Billing Instance Properties \(ISbeBillingInstanceProperties\)](#)
- [SBE RADIUS Client Properties \(ISbeRadiusClientProperty\)](#)
- [SBE RADIUS Server Properties \(ISbeRadiusServerProperties\)](#)
- [SBC Adjacency Endpoint \(ISbcAdjacencyEnd\)](#)
- [SBC Adjacency Group \(ISbcAdjacencyGroup\)](#)
- [SBC SIP Adjacency Endpoint \(ISbcSipAdjacencyEnd\)](#)
- [SBC SIP Adjacency Endpoint Authorization Realm \(ISbcSipAdjacencyEndAuthRealm\)](#)
- [SBE Configured BlackList \(ISbeConfiguredBlackList\)](#)
- [SBE Configured BlackList Entry \(ISbeConfiguredBlackListEntry\)](#)
- [SBE Current BlackList Listing \(ISbeCurrentBlacklisting\)](#)
- [SBE Codec List \(ISbeCodecList\)](#)
- [SBE Code List Entry \(ISbeCodecListEntry\)](#)
- [SBE Media Gateway \(ISbeMediaGateway\)](#)

- DBE Media Gateway Controller (IDbeMGC)
- SBC H248 Control Interface (ISbcH248ControlInterface)
- SBE Global Hunting Trigger List (ISbeGlobalHuntingTriggerList)
- SBE CAC Policy Set (ISbeCacPolicySet)
- SBE CAC Policy Table (ISbeCacPolicyTable)
- SBE CAC Rule Entry (ISbeCacRuleEntry)
- SBE Call Policy Set (ISbeCallPolicySet)
- SBE Call Policy Table (ISbeCallPolicyTable)
- SBE Call Policy Entry (ISbeCallRuleEntry)
- SBE Policy Set (ISbePolicySet)
- SBE Policy Table (ISbePolicyTable)
- SBE Rule Entry (ISbeRuleEntry)
- SBE SDP Match Table (ISbeSdpMatchTable)
- SBE SDP Policy Table (ISbeSdpPolicyTable)
- SBE QOS Profile (ISbeQosProfile)
- SBE SIP Header Profile (ISbeSipHeaderProfile)
- SBE SIP Header Profile Entry (ISbeSipHeaderProfileEntry)
- SBE SIP Header Profile Header (ISbeSipHeaderProfileHeader)
- SBE SIP Method Profile (ISbeSipMethodProfile)
- SBE SIP Method Profile Method (ISbeSipMethodProfileMethod)
- SBE SIP Option Profile (ISbeSipOptionProfile)
- SBE SIP Parameter Profile (ISbeSipParameterProfile)
- SBE SIP Profile (ISbeSipProfile)
- SBE SIP Timer Properties (ISbeSipTimerProperties)

SBC Service

The **SBC Service** object represents the SBC service function running on the physical network element (usually a router service card).

Table 14-1 **SBC Service (ISbcService)**

Attribute Name	Attribute Description	Scheme	Polling Interval
SBC Mode	The mode of the configured SBC service (<i>UM, DM, UM-HA</i>)	IPCore	Configuration
Release Version	The SBC release version (for example, Release 3.0.00)	IPCore	Configuration
Application Version	The SBC application version	IPCore	Configuration
HA Status	The redundancy (high availability) status of the configured SBC service (<i>primary, standby</i>)	IPCore	Configuration

Service Border Element

The [Service Border Element](#) object represents the SBE (also known as the signaling proxy) that controls access to the network core by VoIP signaling messages. The SBE does this by acting as a Session Initiation Protocol (SIP) back-to-back user agent (B2BUA) or H.323 gateway, handling all call processing through one of these protocols. There can be only one signaling agent per service card, and the SBE will typically control one or more media gateways.

Table 14-2 *Service Border Element (ISBE)*

Attribute Name	Attribute Description	Scheme	Polling Interval
Call Redirect Limit	Maximum number of redirections performed before the call fails (2 is default, range is 0-100)	IPCore	Configuration
Onhold Timeout	Time the SBE will wait after receiving a media timeout notification from the Data Border Element before tearing down an on-hold call.	IPCore	Configuration

Data Border Element

The [Data Border Element](#) object represents the DBE (also known as a media control proxy) that controls access to media packets on the network by acting as an RTP proxy.

Table 14-3 *Data Border Element (IDBE)*

Attribute Name	Attribute Description	Scheme	Polling Interval
DBE Location ID	The unique location ID configured on each vDBE within a UM DBE service.	IPCore	Configuration
DBE Type	The type of DBE (<i>DBE</i> , <i>vDBE</i>)	IPCore	Configuration

DBE Media Interface

The [DBE Media Interface](#) object represents either the pool of IPv4 network addresses that can be used by the DBE as local media addresses, or an interface defined on the DBE that is used for RTP packets.

Table 14-4 *DBE Media Interface (IDbeMediaInterface)*

Attribute Name	Attribute Description	Scheme	Polling Interval
Address Range	The defined range of addresses in the pool.	IPCore	Status
VRF Name	The VRF to which this interface is assigned.	IPCore	Status
Managed By	The unit managing this media interface, DBE or Media Gateway Controller.	IPCore	Status
Port Range Upper	The upper port range for the interface.	IPCore	Status
Port Range Lower	The lower port range for the interface.	IPCore	Status
Service Class	The class of service (CoS) affinity for the port range. The set of CoS is consistent with those used for QoS packet marking, and consists of voice and video.	IPCore	Status
Status	Status of the interface (<i>active</i> , <i>inactive</i>).	IPCore	Status

Table 14-4 DBE Media Interface (*IDbeMediaInterface*) (continued)

Attribute Name	Attribute Description	Scheme	Polling Interval
NAT Mode	The configured traversal mode for network address and port translation (<i>twice-napt, twice-nat</i>).	IPCore	Status
Termination	The ID of the interface termination point.	IPCore	Status

SBC Account

The [SBC Account](#) object represents the service relationship with the remote organization on the SBE, with which the SBC interacts.

Table 14-5 SBC Account (*ISbcAccount*)

Attribute Name	Attribute Description	Scheme	Polling Interval
Name	The SBC account name.	IPCore	Configuration
Adjacency List	User-defined signaling adjacencies which connect the SBC to devices within the remote-side organization.	IPCore	Configuration

SBE AAA Interface

The [SBE AAA Interface](#) object represents the SBE interface used to supply authentication, authorization, and accounting (AAA) subscriber services to the SBC.

Table 14-6 SBE AAA Interface (*ISbeAaaInterface*)

Attribute Name	Attribute Description	Scheme	Polling Interval
Network ID	The arbitrary SBE interface identifier (from 0-99999).	IPCore	Status
VRF	The VRF to which this SBE interface is assigned.	IPCore	Status
AAA Address	IP address of the AAA interface.	IPCore	Configuration
instanceName	Name of this AAA interface.	IPCore	Configuration

SBE Billing Properties

The [SBE Billing Properties](#) object represents all billing properties for an [SBC Account](#).

Table 14-7 *SBE Billing Properties (ISbeBillingProperties)*

Attribute Name	Attribute Description	Scheme	Polling Interval
Check Time	The local time of day (up to 23:59) at which to run the long-duration record check for 24-hour billing reporting.	IPCore	Configuration
Administrative Status	Administrative status (<i>Unknown, Up, Down</i>)	IPCore	Configuration
Operational Status	Operational status (<i>Unknown, Up, Down</i>)	IPCore	Configuration
instanceName	Name of this billing instance.	IPCore	Configuration
Local Billing Address	The IP address of the local SBE billing address. This can be different from the AAA local address. It is the address stored in bill records.	IPCore	Configuration

SBE Billing Instance Properties

The [SBE Billing Instance Properties](#) object represents a single SBE billing record.

Table 14-8 *SBE Billing Instance Properties (ISbeBillingInstanceProperties)*

Attribute Name	Attribute Description	Scheme	Polling Interval
Instance Number	ID number of the billing instance.	IPCore	Configuration
Billing Method	The billing method.	IPCore	Configuration
Local Billing Address	The IP address of the local SBE billing address. This can be different from the AAA local address. It is the address stored in bill records.	IPCore	Configuration
Check Time	The local time of day (up to 23:59) at which to run the long-duration record check for 24-hour billing reporting.	IPCore	Configuration
Batch Size	Batch size.	IPCore	Configuration
Batch Time	Batch time.	IPCore	Configuration
Deactivation Mode	Description of how this billing instance is to be deactivated (for example, <i>normal</i>).	IPCore	Configuration
RADIUS Client	The name of the configured RADIUS accounting client for this billing instance.	IPCore	Configuration
Active Calls	The number of currently active calls logged against the billing instance.	IPCore	Configuration
Operational Status	Operational status (<i>Unknown, Up, Down</i>)	IPCore	Configuration
Transport Status	Transport status	IPCore	Configuration
Administrative Status	Administrative status (<i>Unknown, Up, Down</i>)	IPCore	Configuration

SBE RADIUS Client Properties

The [SBE RADIUS Client Properties](#) object stores the properties associated with the RADIUS client which the SBE uses to access AAA services.

Table 14-9 *SBE RADIUS Client Properties (ISbeRadiusClientProperty)*

Attribute Name	Attribute Description	Scheme	Polling Interval
Name	Name of the RADIUS accounting client.	IPCore	Configuration
SBE Retry Interval	Interval at which the SBE resends accounting requests to the RADIUS server.	IPCore	Configuration
Client Type	The type of RADIUS client (<i>accounting, authentication</i>).	IPCore	Configuration
SBE Concurrent Request Limit	Total number of concurrent client requests configured.	IPCore	Configuration
SBE Retry Limit	Total number of retries for a single accounting request.	IPCore	Configuration

SBE RADIUS Server Properties

The [SBE RADIUS Server Properties](#) object stores properties associated with the RADIUS server as viewed by the AAA client.

Table 14-10 *SBE RADIUS Server Properties (ISbeRadiusServerProperties)*

Attribute Name	Attribute Description	Scheme	Polling Interval
Server Priority	The priority of the accounting server. The priority determines which of the configured servers is selected as the default server and where all requests are sent. A RADIUS client contacts the RADIUS servers sequentially, in order of priority, to establish an active RADIUS session. Each RADIUS client sends call detail records to the currently active RADIUS server. The priority must be in the range 1-10 (highest to lowest priority).	IPCore	Configuration
Server Key	The RADIUS accounting server authentication key or shared secret.	IPCore	Configuration
Port Number	The port number on which the server connects to the RADIUS server.	IPCore	Configuration
RADIUS Mode	The RADIUS mode (<i>remote, local</i>).	IPCore	Configuration
Remote Access Point	The IP address of the remote RADIUS server.	IPCore	Configuration

SBC Adjacency Endpoint

The [SBC SIP Adjacency Endpoint](#) object represents a signaling relationship between a local and a remote call agent. There is one adjacency defined per call agent. The adjacency defines protocol-specific parameters as well as admission control and routing policy. The SBC adjacency includes SIP and H.323 adjacencies (R4 supports SIP adjacencies only).

Table 14-11 *SBC Adjacency Endpoint (ISbcAdjacencyEnd)*

Attribute Name	Attribute Description	Scheme	Polling Interval
Description	Description of this adjacency.	IPCore	Configuration
Subnet Restriction	The configured IP address prefix restricting the set of remote signaling peers that can be contacted over this adjacency.	IPCore	Configuration
Media Passthrough	Permit media traffic to bypass the DBE (<i>true, false</i>).	IPCore	Configuration
Hunting Trigger Disabled	Enables or disables the hunting trigger on this adjacency.	IPCore	Configuration
Hunting Triggers	The list of hunting triggers associated with this adjacency.	IPCore	Configuration
VRF	The VRF with which this adjacency is associated.	IPCore	Configuration
Local Signaling Address	The logical IP address of this adjacency.	IPCore	Configuration
Remote Signaling Address	The signaling peer.	IPCore	Configuration
Local Signaling Port	The port used by this adjacency.	IPCore	Configuration
Remote Signaling Port	The port of the signaling peer.	IPCore	Configuration
Operational Status	Operational status of the adjacency (<i>attach, detach</i>).	IPCore	Configuration
SBC Account	The SBC Account associated with this adjacency.	IPCore	Configuration
Instance Name	The name of this adjacency.	IPCore	Configuration
Transport Protocol	The Layer 4 protocol this adjacency uses.	IPCore	Configuration

SBC Adjacency Group

The [SBC Adjacency Group](#) object represents a list of adjacencies. Adjacency groups permit operators to enable and disable features on a group basis instead of per adjacency.

Table 14-12 *SBC Adjacency Group (ISbcAdjacencyGroup)*

Attribute Name	Attribute Description	Scheme	Polling Interval
Name	The name of the adjacency group.	IPCore	Configuration
Adjacency List	The list of adjacencies in the named group.	IPCore	Configuration

SBC SIP Adjacency Endpoint

The [SBC SIP Adjacency Endpoint](#) object represents the same relationship as [SBC Adjacency Endpoint](#) but for a SIP adjacency only.

Table 14-13 *SBC SIP Adjacency Endpoint (ISbcSipAdjacencyEnd)*

Attribute Name	Attribute Description	Scheme	Polling Interval
Preferred Transport	The preferred transport to use. If the preferred transport is not available, another supported transport will be used.	IPCore	Configuration
Registration Target Address	The IP address of the SIP register server.	IPCore	Configuration
Registration Target Port	The port number of the SIP register server.	IPCore	Configuration

SBC SIP Adjacency Endpoint Authorization Realm

The [SBC SIP Adjacency Endpoint Authorization Realm](#) object represents a set of authentication credentials for a specified domain and adjacency.

Table 14-14 *SBC SIP Adjacency Endpoint Authorization Realm (ISbcSipAdjacencyEndAuthRealm)*

Attribute Name	Attribute Description	Scheme	Polling Interval
Domain	The name of the domain for which the authentication credentials are valid.	IPCore	Status
Username	The username that identifies the SBC in the specified domain.	IPCore	Status
Password	The password used to authenticate the username in the specified domain.	IPCore	Status

SBE Configured BlackList

The [SBE Configured BlackList](#) object represents a source to which one or more instances of [SBE Configured BlackList Entry](#) applies. The source can be broad or narrow, depending on the defined combination of IP address, port, VPN, and port type.

Table 14-15 *SBE Configured BlackList (ISbeConfiguredBlackList)*

Attribute Name	Attribute Description	Scheme	Polling Interval
Black List Type	The type of source to which this blacklist applies.	IPCore	Configuration
Instance Name	The name of this source.	IPCore	Configuration

SBE Configured BlackList Entry

The [SBE Configured BlackList Entry](#) object represents a set of specific blacklisting actions that are taken when events of a specified type are received from sources defined in one or more instances of [SBE Configured BlackList](#).

Table 14-16 *SBE Configured BlackList Entry (ISbeConfiguredBlackListEntry)*

Attribute Name	Attribute Description	Scheme	Polling Interval
Event Type	The type of event to which this limit applies.	IPCore	Configuration
Trigger Size	The number of events from the specified source that are allowed before blacklisting is triggered and all packets from the source are blocked.	IPCore	Configuration
Trigger Period	The period of time during which events will be considered as candidates for blacklisting triggers.	IPCore	Configuration
Blacklisting Period	The length of time during which packets from the source are blocked after the configured limits are exceeded.	IPCore	Configuration
Default Blacklisting Period	Identifies whether the specified blacklisting period is the default.	IPCore	Configuration
Default Trigger Size	Identifies whether the specified trigger size is the default.	IPCore	Configuration
Default Trigger Period	Identifies whether the specified trigger period is the default.	IPCore	Configuration

SBE Current BlackList Listing

The [SBE Current BlackList Listing](#) object represents a set of limits currently in effect against one or more blacklisted sources defined in one or more instances of [SBE Configured BlackList](#).

Table 14-17 *SBE Current BlackList Listing (ISbeCurrentBlacklisting)*

Attribute Name	Attribute Description	Scheme	Polling Interval
Source Address	The IP address of a blacklisted source.	IPCore	Configuration
All Source Addresses	Indicates whether Source Address applies to only one or to all sources. If <i>true</i> , ignore the value in Source Address.	IPCore	Configuration
Source Port Type	The port type of the blacklisted sources.	IPCore	Configuration
Source Port Number	The port number of the blacklisted sources.	IPCore	Configuration
Time Remaining	The time remaining until the blacklist will be removed (<i>hh:mm:ss</i>).	IPCore	Configuration
Event Type	The type of blacklisted event.	IPCore	Configuration
Blacklist Type	The type of source to which this blacklist applies.	IPCore	Configuration

SBE Codec List

The [SBE Codec List](#) object defines a list of allowed codecs (a whitelist) that can be applied via a Call Admission Control (CAC) policy.

Table 14-18 *SBE Codec List (ISbeCodecList)*

Attribute Name	Attribute Description	Scheme	Polling Interval
Name	The name of the list of allowed codecs.	IPCore	Configuration

SBE Codec List Entry

The [SBE Codec List Entry](#) object represents an entry in the [SBE Codec List](#).

Table 14-19 *SBE Code List Entry (ISbeCodecListEntry)*

Attribute Name	Attribute Description	Scheme	Polling Interval
minPacketizationPeriod	The minimum packetization period.	IPCore	Configuration
codecName	The name of the allowed codec to which the minimum packetization period applies.	IPCore	Configuration

SBE Media Gateway

The [SBE Media Gateway](#) object represents properties for the SBC/SBE side of the H.248 interface.

Table 14-20 *SBE Media Gateway (ISbeMediaGateway)*

Attribute Name	Attribute Description	Scheme	Polling Interval
codecList	Comma-separated list of codecs supported on the H.248 link.	IPCore	Configuration
ipAddress	IP address	IPCore	Configuration

DBE Media Gateway Controller

The [DBE Media Gateway Controller](#) object represents properties for the DBE side of the H.248 interface.

Table 14-21 *DBE Media Gateway Controller (IDbeMGC)*

Attribute Name	Attribute Description	Scheme	Polling Interval
remoteIP	The remote IP address.	IPCore	Configuration
remotePort	The remote port number.	IPCore	Configuration
transport	The transport protocol used.	IPCore	Configuration
Index	Identifies the index number of the DBE Media Gateway Controller.	IPCore	Configuration

SBC H248 Control Interface

The [SBC H248 Control Interface](#) object represents the H.248 interface used for signaling between the SBE and DBE in distributed mode, and between an SBE and a transcoding media gateway.

Table 14-22 *SBC H248 Control Interface (ISbcH248ControllInterface)*

Attribute Name	Attribute Description	Scheme	Polling Interval
ipAddress	IP address of the remote Media Gateway for an SBE, and the associated Media Gateway Controller for a DBE.	IPCore	Configuration
transport	The transport protocol used.	IPCore	Configuration
port	The port number.	IPCore	Configuration
Association	The media gateway associated with this H.248 control interface.	IPCore	Configuration

SBE Global Hunting Trigger List

The [SBE Global Hunting Trigger List](#) object represents a list of hunting triggers defined globally for SBCs. Hunting triggers enable SBCs to hunt for other route or destination adjacencies when normal routes fail.

Table 14-23 *SBE Global Hunting Trigger List (ISbeGlobalHuntingTriggerList)*

Attribute Name	Attribute Description	Scheme	Polling Interval
huntingMode	SIP hunting triggers.	IPCore	Status
huntingTriggers	The list of hunting triggers.	IPCore	Status

SBE CAC Policy Set

The [SBE CAC Policy Set](#) object represents a set of SBE Call Admission Control (CAC) policy rules. These rules permit application-level policy control over how VoIP call admission requests are processed.

Table 14-24 *SBE CAC Policy Set (ISbeCacPolicySet)*

Attribute Name	Attribute Description	Scheme	Polling Interval
firstScope	First call table scope of this policy set.	IPCore	Configuration
firstTable	The first CAC table used by this policy set.	IPCore	Configuration
Description	Description of the policy set.	IPCore	Configuration
Status	Status of the policy set (<i>active</i> , <i>inactive</i>).	IPCore	Configuration

SBE CAC Policy Table

The [SBE CAC Policy Table](#) object represents a table containing instances of [SBE CAC Rule Entry](#).

Table 14-25 *SBE CAC Policy Table (ISbeCacPolicyTable)*

Attribute Name	Attribute Description	Scheme	Polling Interval
instanceName	Name of the table	IPCore	Configuration
instanceDescription	Description of the table	IPCore	Configuration
matchType	List of event types to match on	IPCore	Configuration

SBE CAC Rule Entry

The [SBE CAC Rule Entry](#) object represents an entry in a [SBE CAC Policy Table](#).

Table 14-26 *SBE CAC Rule Entry (ISbeCacRuleEntry)*

Attribute Name	Attribute Description	Scheme	Polling Interval
scope	The scope of the entry.	IPCore	Configuration
nextPolicyTable	The next CAC policy table to be evaluated in the chain.	IPCore	Configuration

SBE Call Policy Set

The [SBE Call Policy Set](#) object represents a set of SBE call policy rules. These rules permit application-level policy control over how in-call VoIP signaling and media are processed.

Table 14-27 *SBE Call Policy Set (ISbeCallPolicySet)*

Attribute Name	Attribute Description	Scheme	Polling Interval
isActive	Indicates if the policy set is <i>active</i> or <i>inactive</i> .	IPCore	Configuration
policySetNumber	The ID number of the policy set.	IPCore	Configuration
name	The name of the policy set.	IPCore	Configuration
description	The description of the policy set.	IPCore	Configuration
firstCallTable	The first call table used by this policy set.	IPCore	Configuration

SBE Call Policy Table

The [SBE Call Policy Table](#) object represents a table containing instances of [SBE Call Policy Entry](#).

Table 14-28 *SBE Call Policy Table (ISbeCallPolicyTable)*

Attribute Name	Attribute Description	Scheme	Polling Interval
instanceName	Name of the call policy table.	IPCore	Configuration
instanceDescription	Description of the call policy table.	IPCore	Configuration
matchType	The type of call events to match on.	IPCore	Configuration

SBE Call Policy Entry

The [SBE Call Policy Entry](#) object represents an entry in a [SBE CAC Policy Table](#).

Table 14-29 *SBE Call Policy Entry (ISbeCallRuleEntry)*

Attribute Name	Attribute Description	Scheme	Polling Interval
entryNumber	ID number of the Call policy entry.	IPCore	Configuration
action	Action to be taken on a match.	IPCore	Configuration
matchValue	The event to match on.	IPCore	Configuration
entryCategory	The policy entry category.	IPCore	Configuration

SBE Policy Set

The [SBE Policy Set](#) object represents a group of policies that can be active on the SBC at any one time.

Table 14-30 *SBE Policy Set (ISbePolicySet)*

Attribute Name	Attribute Description	Scheme	Polling Interval
isActive	Indicates whether the policy set is active or inactive.	IPCore	Configuration
policySetNumber	ID number of the SBE policy set.	IPCore	Configuration
name	Name of the SBE policy set.	IPCore	Configuration
description	Description of the SBE policy set.	IPCore	Configuration

SBE Policy Table

The [SBE Policy Table](#) object represents a table of instances of [SBE Rule Entry](#). It is an abstract class that contains attributes common to both call policy and CAC policy rules.

Table 14-31 *SBE Policy Table (ISbePolicyTable)*

Attribute Name	Attribute Description	Scheme	Polling Interval
matchType	The criteria used to select an SBE Rule Entry from the table.	IPCore	Configuration
name	The name of the SBE policy table.	IPCore	Configuration
description	Description of the SBE policy table.	IPCore	Configuration

SBE Rule Entry

The [SBE Rule Entry](#) object represents an entry in [SBE Policy Table](#). It is abstract class that contains attributes common to both Call and CAC policy rules.

Table 14-32 *SBE Rule Entry (ISbeRuleEntry)*

Attribute Name	Attribute Description	Scheme	Polling Interval
entryNumber	The entry's ID number in the SBE Policy Table .	IPCore	Configuration
action	The action to be performed if the entry's matchValue matches the matchType in the SBE Policy Table .	IPCore	Configuration
matchValue	The value to be matched against the matchType in the SBE Policy Table .	IPCore	Configuration
entryCategory	The category of the entry in the number analysis table.	IPCore	Configuration
instanceName	The name of this entry.	IPCore	Configuration
dstAdjacency	The destination adjacency of this entry.	IPCore	Configuration
matchAdjacency	The adjacency to which this entry relates.	IPCore	Configuration
SbeAccount	The account to which this entry relates.	IPCore	Configuration
MatchAdjacencyGroup	The adjacency group to which this entry relates.	IPCore	Configuration

SBE SDP Match Table

The [SBE SDP Match Table](#) object represents a table of strings used in event and policy matching.

Table 14-33 *SBE SDP Match Table (ISbeSdpMatchTable)*

Attribute Name	Attribute Description	Scheme	Polling Interval
tableType	The type of table.	IPCore	Status
matchStrings	The list of strings to match on.	IPCore	Status

SBE SDP Policy Table

The [SBE SDP Policy Table](#) object represents a table of the SBE/SBC policies.

Table 14-34 *SBE SDP Policy Table (ISbeSdpPolicyTable)*

Attribute Name	Attribute Description	Scheme	Polling Interval
name	Name of the policy table	IPCore	Status

SBE QOS Profile

The [SBE QOS Profile](#) object represents a defined quality-of-service profile used by CAC policies. These policies are used exclusively for marking packets.

Table 14-35 *SBE QOS Profile (ISbeQosProfile)*

Attribute Name	Attribute Description	Scheme	Polling Interval
classOfService	The type of call to which this QoS profile will be applied (for example, <i>voice</i> , <i>video</i> , <i>fax</i> , <i>signaling</i>).	IPCore	Configuration
markingType	The type of marking: DSCP or IP precedence.	IPCore	Configuration
dscp	DSCP value.	IPCore	Configuration
ipPrecedence	IP precedence value.	IPCore	Configuration
tos	Terms of Service (ToS) value.	IPCore	Configuration

SBE SIP Header Profile

The [SBE SIP Header Profile](#) object represents an instance of a SIP header profile, used to control which SIP message requests are accepted (whitelist) or rejected (blacklist) on the SBE.

Table 14-36 *SBE SIP Header Profile (ISbeSipHeaderProfile)*

Attribute Name	Attribute Description	Scheme	Polling Interval
instanceName	Name of the SIP header profile.	IPCore	Configuration
isInUse	Flag indicating whether the profile is in use.	IPCore	Configuration
profileType	The profile type (<i>blacklist</i> ; profiles are whitelists by default).	IPCore	Configuration
description	Description of the profile.	IPCore	Configuration

SBE SIP Header Profile Entry

The [SBE SIP Header Profile Entry](#) object represents an entry in the [SBE SIP Header Profile](#).

Table 14-37 *SBE SIP Header Profile Entry (ISbeSipHeaderProfileEntry)*

Attribute Name	Attribute Description	Scheme	Polling Interval
entryNr	ID number of the entry	IPCore	Configuration
action	The action to be taken when there is a match on the value and conditions	IPCore	Configuration
value	Value in the SIP message to be matched on	IPCore	Configuration
conditions	Condition in the SIP message to be matched on	IPCore	Configuration
parameterProfile	Parameter profile	IPCore	Configuration

SBE SIP Header Profile Header

The [SBE SIP Header Profile Header](#) object is an abstract class representing a header on the [SBE SIP Header Profile](#).

Table 14-38 *SBE SIP Header Profile Header (ISbeSipHeaderProfileHeader)*

Attribute Name	Attribute Description	Scheme	Polling Interval
name	Name of the SBE SIP Header Profile	IPCore	Configuration

SBE SIP Method Profile

The [SBE SIP Method Profile](#) object specifies how methods for the corresponding [SBE SIP Header Profile](#) will be applied.

Table 14-39 *SBE SIP Method Profile (ISbeSipMethodProfile)*

Attribute Name	Attribute Description	Scheme	Polling Interval
isPassthrough	If <i>true</i> , permits message bodies to be passed through for non vital messages accepted by the profile. If <i>false</i> , strips the message body out of any non vital SIP messages matched by the profile.	IPCore	Configuration

SBE SIP Method Profile Method

The [SBE SIP Method Profile](#) object stores the method strings that form the whitelist or blacklist [SBE SIP Header Profile](#).

Table 14-40 *SBE SIP Method Profile Method (ISbeSipMethodProfileMethod)*

Attribute Name	Attribute Description	Scheme	Polling Interval
instanceName	Name of the method.	IPCore	Configuration
action	The action to be performed by the method strings.	IPCore	Configuration
mapStatusCode	The map status code.	IPCore	Configuration
headerProfile	The corresponding SBE SIP Header Profile for this method.	IPCore	Configuration
parameterProfile	The corresponding SBE SIP Parameter Profile for this method.	IPCore	Configuration

SBE SIP Option Profile

The [SBE SIP Option Profile](#) object stores the option strings that form a SIP Option profile whitelist or blacklist.

Table 14-41 *SBE SIP Option Profile (ISbeSipOptionProfile)*

Attribute Name	Attribute Description	Scheme	Polling Interval
options	The option strings that form the whitelist or blacklist.	IPCore	Configuration

SBE SIP Parameter Profile

The [SBE SIP Parameter Profile](#) object stores the parameters that form a SIP parameter profile whitelist or blacklist.

Table 14-42 *SBE SIP Parameter Profile (ISbeSipParameterProfile)*

Attribute Name	Attribute Description	Scheme	Polling Interval
parameters	The parameter strings that form the whitelist or blacklist.	IPCore	Configuration

SBE SIP Profile

The [SBE SIP Profile](#) is an abstract class representing SIP Header, Option, and Method profiles.

Table 14-43 *SBE SIP Profile (ISbeSipProfile)*

Attribute Name	Attribute Description	Scheme	Polling Interval
instanceName	Name of the profile.	IPCore	Configuration
isInUse	Flag indicating whether it is in use.	IPCore	Configuration
profileType	The profile type.	IPCore	Configuration
description	Profile description.	IPCore	Configuration

SBE SIP Timer Properties

The [SBE SIP Timer Properties](#) object represents a SIP Timer. Users can configure SIP timers to permit performance tuning of network elements participating in SBC traffic.

Table 14-44 *SBE SIP Timer Properties (ISbeSipTimerProperties)*

Attribute Name	Attribute Description	Scheme	Polling Interval
tcpConnectTimeout	Time (in milliseconds) the SBC waits for a SIP TCP connection to a remote peer to complete before failing the connection. The default is 1000.	IPCore	Configuration
tcpIdleTimeout	Minimum time (in milliseconds) a TCP socket must remain open while not processing traffic. If the socket remains idle after that time, it can be closed. The default is two seconds.	IPCore	Configuration
tlsIdleTimeout	Transport Layer Security (TLS) idle timeout.	IPCore	Configuration
inviteTimeout	Time (in milliseconds) the SBC waits for a final response to an outbound SIP INVITE request. The default is 180 seconds. If no response is received during that time, an internal Request Timeout response is generated and returned to the caller.	IPCore	Configuration
udpFirstRetransmitInterval	Time (in milliseconds) the SBC waits for a UDP response or ACK before sending the first retransmission of the relevant signal. If the SBC keeps getting no responses, it doubles subsequent retransmission intervals each time until it reaches the udp-max-retransmit-interval duration. It will cease retransmitting the request and timeout the signal if 64 times this duration passes without the receipt of a response or ACK. The default first UDP retransmission interval is 500 milliseconds.	IPCore	Configuration
udpMaxRetransmitInterval	Maximum interval (in milliseconds) after which SBC will retransmit. The default interval is four seconds.	IPCore	Configuration
tcpConnectTimeout	Time interval (in milliseconds) over which SBC will retain negative UDP responses to INVITE requests. All subsequent retransmitted responses received within this interval will be answered with a negative ACK. Thereafter, any further retransmitted responses are ignored. The default UDP response linger period is 32 seconds.	IPCore	Configuration

Vendor-Specific Inventory and IMOs

There are no vendor-specific inventory or IMOs for this technology.

Network Topology

Cisco ANA does not support discovery of Network layer topology.

Service Alarms

There are no service alarms specific to this technology.



CHAPTER 15

Multiprotocol Label Switching

This chapter describes the level of support that Cisco ANA provides for MPLS, as follows:

- [Technology Description, page 15-1](#)
- [Information Model Objects \(IMOs\), page 15-2](#)
- [Vendor-Specific Inventory and IMOs](#)
- [Network Topology, page 15-6](#)
- [Service Alarms, page 15-6](#)

Technology Description

This section provides the following MPLS technology descriptions:

- [MPLS](#)
- [LDP](#)

Please see Part 1: Cisco VNEs in this guide for information about which devices support the various technologies.

MPLS

MPLS was originally presented as a way of improving the forwarding speed of routers. It is now emerging as a crucial standard technology that offers new capabilities for large-scale IP networks. Traffic engineering (TE), the ability of network operators to dictate the path that traffic takes through the network, and VPN support, are examples of two key applications where MPLS is superior to any currently available IP technology. It integrates Layer 2 information about network links (bandwidth, latency, utilization) into Layer 3 (IP) within a particular autonomous system, or ISP, in order to simplify and improve IP packet exchange. It also gives network operators a great deal of flexibility in how they divert and route traffic around link failures, congestion, and bottlenecks.

When packets enter an MPLS-based network, label edge routers (LERs) give them a label identifier. These labels not only contain information based on the routing table entries (for example, destination, bandwidth, delay, and other metrics), but also refer to the IP header field (source IP address), Layer 4 socket number information, and differentiated service. Once this classification is complete and mapped, different packets are assigned to corresponding label switched paths (LSPs), where label switch routers (LSRs) place outgoing labels on the packets.

LDP

Label Distribution Protocol (LDP) enables neighboring provider or provider-edge routers acting as LSRs in an MPLS-aware network to exchange label prefix binding information, which is required for forwarding traffic. The LSRs discover potential peers in the network with which they can establish LDP sessions in order to negotiate and exchange the labels (addresses) to be used for forwarding packets.

LDP supports two types of peer discovery:

- Basic discovery—Used to discover directly connected LDP LSRs. An LSR sends hello messages to the “all routers on this subnet” multicast address, on interfaces for which LDP has been configured.
- Extended discovery—Used between indirectly connected LDP LSRs. An LSR sends targeted hello messages to specific IP addresses. Targeted sessions must be configured since the routers are not physically connected and broadcasting would not reach the peers. The IP addresses of both peers are required for extended discovery.

Information Model Objects (IMOs)

This section describes the following IMOs:

- [MPLS Interface \(IMpls\)](#)
- [Label Switching Entity \(ILse\)](#)
- [Equivalent Label Switching Entry \(ILSEEntries\)](#)
- [MPLS Entry \(IMplsEntry\)](#)
- [MPLS Aggregate Entry \(IMplsAggregateEntry\)](#)
- [LDP Service \(ILdpService\)](#)
- [LDP Peer \(ILdpPeer\)](#)
- [LDP Peer Discovery Source \(ILdpPeerDiscoverySource\)](#)

MPLS Interface

The network/data link layer [MPLS Interface](#) object represents an MPLS configuration in a router interface. It is bound by its Containing Termination Points attribute to a data link layer interface object, and is accessed primarily by the Network layer [IP Interface](#) bound by its Contained Connection Termination Points attribute. It is also accessed by the [Label Switching Entity](#).

Table 15-1 MPLS Interface (IMpls)

Attribute Name	Attribute Description	Scheme	Polling Interval
Distribution Protocol	Distribution protocol (<i>Null, LDP, TDP, RSVP, TDP and LDP</i>)	IPCore	Configuration
Outer and Inner Labels	Outer and inner labels for Path Tracer	IPCore	Configuration
Traffic Engineering Properties	Traffic engineering properties (MPLS TE Properties)	IPCore	Configuration
Resource Reservation Properties	Resource Reservation Protocol properties	IPCore	Configuration

Table 15-1 *MPLS Interface (IMpls) (continued)*

Attribute Name	Attribute Description	Scheme	Polling Interval
IANA Type	Internet Assigned Numbers Authority (IANA) type of the sublayer	N/A	N/A
Containing Termination Points	Underlying termination points (connection or physical)	IPCore	N/A
Contained Connection Termination Points	Bound connection termination points	IPCore	N/A

Label Switching Entity

The [Label Switching Entity](#) object describes the protocol-independent forwarding component of an LSR. It is bound by its Logical Sons attribute to all the network or data link layer [MPLS Interface](#) objects among which this [Label Switching Entity](#) is switching IP packets.

Table 15-2 *Label Switching Entity (ILse)*

Attribute Name	Attribute Description	Scheme	Polling Interval
MPLS Table	Array of Equivalent Label Switching Entries between MPLS interfaces	IPCore	Configuration
MPLS Aggregate Table	Array of Equivalent Label Switching Entries from MPLS interfaces into VRF tables	IPCore	Configuration
MPLS Tunnel Segments	Array of switched MPLS TE tunnel segments (GUI usage) (see Multiprotocol Label Switching Traffic Engineering)	IPCore	Configuration
LDP Service	LDP Service which holds the LDP Peers	IPCore	Configuration
Logical Sons	Array of all MPLS Interfaces among which this Label Switching Entity is switching IP packets	IPCore	N/A

Equivalent Label Switching Entry

The [Equivalent Label Switching Entry](#), [MPLS Entry](#), and [MPLS Aggregate Entry](#) objects describe an MPLS Label Switching table's entries. Each is an array of [MPLS Entries](#) or [MPLS Aggregate Entries](#) sharing a single ingress label.

Table 15-3 *Equivalent Label Switching Entry (ILSEEntries)*

Attribute Name	Attribute Description	Scheme	Polling Interval
Label Switching Entries	Array of either MPLS Entries or MPLS Aggregate Entries (sharing a single ingress label)	IPCore	Configuration

MPLS Entry

Table 15-4 *MPLS Entry (IMplsEntry)*

Attribute Name	Attribute Description	Scheme	Polling Interval
Incoming Label	Incoming label	IPCore	Configuration
Outgoing Interface and Label	Outgoing interface and label	IPCore	Configuration
Switching Action	Switching action (<i>Null, Pop, Swap, Aggregate, Untagged, Pop, Act</i>)	IPCore	Configuration
Next Hop IP Address	Next hop IP address	IPCore	Configuration
Destination Mask	IP subnet mask of the destination	IPCore	Configuration
Destination Address	Destination IP address	IPCore	Configuration

MPLS Aggregate Entry

Table 15-5 *MPLS Aggregate Entry (IMplsAggregateEntry)*

Attribute Name	Attribute Description	Scheme	Polling Interval
Virtual Routing Entity	Virtual Routing and Forwarding (VRF) entity	IPCore	Configuration
Incoming Label	Incoming label	IPCore	Configuration
Outgoing Interface and Label	Outgoing interface and label	IPCore	Configuration
Switching Action	Switching action (<i>Null, Pop, Swap, Aggregate, Untagged, Pop, Act</i>)	IPCore	Configuration
Next Hop IP Address	Next hop IP address	IPCore	Configuration

LDP Service

The [LDP Service](#) object, which is used in MPLS network environments, describes the main attributes of the LDP service. It is accessed only by the [Label Switching Entity](#)'s LDP Service attribute.

Table 15-6 *LDP Service (ILdpService)*

Attribute Name	Attribute Description	Scheme	Polling Interval
Local Identification	Local LDP identifier	IPCore	Configuration
Status	Service status (<i>Unknown, Running, Down</i>)	IPCore	Configuration
LDP Peers	Array of LDP Peers	IPCore	Configuration

LDP Peer

The [LDP Peer](#) object describes a remote LDP entity that currently has an LDP session with the Local [LDP Service](#). The LDP Peer is bound to the LDP Service by the latter's LDP Peer attribute.

Table 15-7 *LDP Peer (ILdpPeer)*

Attribute Name	Attribute Description	Scheme	Polling Interval
Peer Identification	Peer LDP identifier	IPCore	Configuration
Transport Addresses	Peer transport IP addresses	IPCore	Configuration
Distribution Method	Label distribution method (<i>Unknown, Downstream, Downstream On Demand</i>)	IPCore	Configuration
Protocol Type	Peer protocol type (<i>Unknown, LDP, TDP</i>)	IPCore	Configuration
Path Vector Limit	Path vector limit for loop detection	IPCore	Configuration
Session Status	LDP session status type (<i>Transient, Initialized, Open Received, Open Sent, Operational</i>)	IPCore	Configuration
Protocol Version	LDP session protocol version	IPCore	Configuration
Hold Time	Hold time for maintaining the session without receiving traffic or keepalive	IPCore	Configuration
Hello Time Interval	Time interval at which hello (<i>Keep Alive</i>) packets should be sent	IPCore	Configuration
Peer Discovery Sources	Array of LDP Peer Discovery Sources	IPCore	Configuration

LDP Peer Discovery Source

The [LDP Peer Discovery Source](#) object describes the discovery source of the LDP Peer. Identification of the Peer is done using broadcast on [MPLS Interfaces](#) and a hello message exchanged between LSRs.

Table 15-8 *LDP Peer Discovery Source (ILdpPeerDiscoverySource)*

Attribute Name	Attribute Description	Scheme	Polling Interval
Interface Name	MPLS interface name on which the peer was discovered	IPCore	Configuration
Source Addresses	Source IP addresses from which the hello message was sent	IPCore	Configuration
Type	Discovery type (<i>Link, Targeted</i>)	IPCore	Configuration

Vendor-Specific Inventory and IMOs

There are no vendor-specific inventory or IMOs for this technology.

Network Topology

Cisco ANA 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.

Service Alarms

The following alarms are supported for this technology:

- [Broken LSP Discovered, page 41-11](#)
- [MPLS Black Hole Found, page 41-47](#)
- [MPLS Interface Removed, page 41-48](#)
- [LDP Neighbor Loss, page 41-41](#)



CHAPTER 16

Multiprotocol Label Switching Traffic Engineering

This chapter describes the level of support that Cisco ANA provides for Multiprotocol Label Switching Traffic Engineering (MPLS TE), as follows:

- [Technology Description, page 16-1](#)
- [Information Model Objects \(IMOs\), page 16-2](#)
- [Vendor-Specific Inventory and IMOs](#)
- [Network Topology, page 16-4](#)
- [Service Alarms, page 16-5](#)

Technology Description

This section provides the following MPLS TE technology descriptions:

- [MPLS TE](#)
- [MPLS TE FRR](#)

Please see Part 1: Cisco VNEs in this guide for information about which devices support the various technologies.

MPLS TE

MPLS TE software enables an MPLS backbone to replicate and expand upon the traffic engineering capabilities of Layer 2 ATM and Frame Relay networks. MPLS TE is in wide use on service-provider backbone networks where extreme levels of efficient resource usage and failure recovery are essential.

MPLS TE lets network operators route traffic using *constraint-based routing*. In this type of routing, the path for traffic flow is the shortest path that meets the resource requirements (or constraints) of the traffic flow. These constraints can include bandwidth requirements, media requirements, priority versus other flows, and so on. MPLS TE gracefully recovers from link or node failures that change the topology of the backbone by adapting to the new set of constraints.

MPLS TE is founded on the MPLS integration of Layer 2 and Layer 3 technologies. By making traditional Layer 2 features available to Layer 3, MPLS enables traffic engineering. Providers can offer in a one-tier network what could be achieved otherwise only by overlaying a Layer 3 network on a Layer 2 network.

MPLS TE tunnel paths are calculated at the tunnel head based on a fit between required and available resources (constraint-based routing). The IGP automatically routes the traffic into these tunnels. Typically, a packet crossing the MPLS traffic engineering backbone travels on a single tunnel that connects the ingress point to the egress point.

MPLS TE FRR

MPLS TE FRR protects the functionality of MPLS networks by permitting fast rerouting of traffic to a backup LSP whenever a link or node along an LSP fails.

Information Model Objects (IMOs)

This section describes the following IMOs:

- [MPLS TE Tunnel Interface \(IMplsTETunnel\)](#)
- [MPLS TE Properties \(IMplsTEProperties\)](#)
- [MPLS TE Allocation Entry \(IMplsTEPropertiesAllocationEntry\)](#)
- [MPLS TE Tunnel Segment \(IMplsTESegment\)](#)

MPLS TE Tunnel Interface

The network/data link layer [MPLS TE Tunnel Interface](#) object is bound by its Containing Termination Points attribute to a data link layer interface object. It is accessed primarily by the Network layer [IP Interface](#) object bound by its Contained Connection Termination Points attribute. It is also accessed by the [Label Switching Entity](#).

Table 16-1 MPLS TE Tunnel Interface (IMplsTETunnel)

Attribute Name	Attribute Description	Scheme	Polling Interval
Destination Address	Destination IP address	IPCore	Configuration
Outgoing Interface and Label	Outgoing interface and label	IPCore	Configuration
LSP Identification	Label Switching Path (LSP) identifier	IPCore	Configuration
Requested Bandwidth	Requested bandwidth	IPCore	Configuration
Measured Average, Burst and Peak Bandwidth	Measured average, burst, and peak bandwidth	IPCore	Configuration
Setup and Hold Priority	Setup and hold priority of the tunnel	IPCore	Configuration
Affinity Bits and Mask	Required traffic engineering affinity bits and mask attributes of the tunnel's links	IPCore	Configuration
Automatic Route Announcement Status	Automatic route announcement status (<i>Enable, Disable</i>)	IPCore	Configuration
Optimization Lock Down Status	Label switching path optimization lock down status (<i>Enable, Disable</i>)	IPCore	Configuration
Path Option	Label switching path option (<i>Explicit, Dynamic</i>)	IPCore	Configuration
Name	Interface name	IPCore	Configuration

Table 16-1 *MPLS TE Tunnel Interface (IMplsTETunnel) (continued)*

Attribute Name	Attribute Description	Scheme	Polling Interval
Description	Interface description	IPCore	Configuration
Administrative Status	Administrative status (<i>Unknown, Up, Down</i>)	IPCore	Status
Operational Status	Operational status (<i>Unknown, Up, Down</i>)	IPCore	Status
IsFRREnabled	Indicates whether Fast Reroute is enabled on this tunnel (<i>true, false</i>)	IPCore	Configuration
IANA Type	Internet Assigned Numbers Authority (IANA) type of the sublayer	N/A	N/A
Containing Termination Points	Underlying termination points (MPLS Interface)	IPCore	N/A
Contained Connection Termination Points	Bound connection termination points (IP Interface or MPLS Interface)	IPCore	N/A

MPLS TE Properties

The [MPLS TE Properties](#) object and its [MPLS TE Allocation Entry](#) objects describe the traffic engineering properties of an [MPLS Interface](#) object, to which they bound are by the [MPLS Interface](#) object's Traffic Engineering Properties attribute.

Table 16-2 *MPLS TE Properties (IMplsTEProperties)*

Attribute Name	Attribute Description	Scheme	Polling Interval
Administrative Weight	Administrative weight	IPCore	Configuration
Attributes Identifier	Attributes list identifier	IPCore	Configuration
signaling Protocol	signaling protocol (<i>None, RSVP, CR-LDP, Other</i>)	IPCore	Configuration
Available, Physical and Reserveable Bandwidth	Available, physical, and reserveable bandwidth	IPCore	Configuration
Reserved Bandwidth	Array of instances of MPLS TE Allocation Entry	IPCore	Configuration

MPLS TE Allocation Entry

Table 16-3 *MPLS TE Allocation Entry (IMplsTEPropertiesAllocationEntry)*

Attribute Name	Attribute Description	Scheme	Polling Interval
Priority Level	Allocation priority level (<i>0-7</i>)	IPCore	Configuration
Allocated and Cumulative Bandwidth	Allocated and cumulative bandwidth at, and up to, this priority level	IPCore	Configuration

MPLS TE Tunnel Segment

The [MPLS TE Tunnel Segment](#) object describes the properties of a single segment of an MPLS TE Tunnel. Cisco ANA uses this object to help users visualize MPLS TE Tunnels networks, and it affects the VNE logic implementation. Tunnel segments are aggregated in the MPLS TE Tunnel Segments table of the Label Switching Entity.

Table 16-4 *MPLS TE Tunnel Segment (IMplsTESegment)*

Attribute Name	Attribute Description	Scheme	Polling Interval
Segment Type	Segment type (<i>Head, Intermediate, Tail</i>).	IPCore	Configuration
Measured Average, Burst and Peak Bandwidth	Measured average, burst, and peak bandwidth.	IPCore	Configuration
LSP Identification	Label Switching Path (LSP) identifier.	IPCore	Configuration
Name	Segment name.	IPCore	Configuration
FRRTunnelName	Name of the Fast Reroute backup TE tunnel for the given MPLS TE tunnel segment.	IPCore	Configuration
FRRTunnelState	Indicates the status of the Fast Reroute backup tunnel: <i>ready</i> when the primary tunnel is in working condition; <i>active</i> when there is a failure in the primary tunnel and the backup is in use; <i>not configured</i> if the primary has no designated backup tunnel.	IPCore	Configuration
AverageBandwidth	The current bandwidth used to automatically allocate the tunnel's bandwidth.	IPCore	Configuration
In Interface	Incoming interface (if not a head segment).	IPCore	Configuration
In Label	Incoming label (if not a head segment).	IPCore	Configuration
Out Interface	Outgoing interface (if not a tail segment).	IPCore	Configuration
Out Label	Outgoing label (if not a tail segment).	IPCore	Configuration
Source Address	Source IP address of the tunnel.	IPCore	Configuration
Destination Address	Destination IP address of the tunnel.	IPCore	Configuration

Vendor-Specific Inventory and IMOs

There are no vendor-specific inventory or IMOs for this technology.

Network Topology

Cisco ANA does not support discovery of MPLS TE Network layer topology.

Service Alarms

The following alarms are supported for this technology:

- [MPLS TE Tunnel Down, page 41-49](#)
- [MPLS TE FRR State Changed, page 41-49](#)



CHAPTER 17

Pseudowire

This chapter describes the level of support that Cisco ANA provides for Pseudowire, as follows:

- [Technology Description, page 17-1](#)
- [Information Model Objects \(IMOs\), page 17-2](#)
- [Vendor-Specific Inventory and IMOs](#)
- [Network Topology, page 17-3](#)
- [Service Alarms, page 17-3](#)

Technology Description

This section provides the following Pseudowire technology descriptions:

- [PWE3](#)
- [TDM PW](#)
- [ATM PW](#)
- [PW-to-TE Tunnel Mapping](#)
- [Multi-Segment PW](#)
- [PTP Layer 2 MPLS Tunnel Interface](#)

Please see Part 1: Cisco VNEs in this guide for information about which devices support the various technologies.

PWE3

PWE3 provides methods for carrying networking services (such as ATM, Ethernet, TDM, and SONET/SDH) over a packet-switched network (PSN) as outlined in RFC 3985. It is a point-to-point connection between pairs of PE routers. It emulates services like Ethernet over an underlying core MPLS network through encapsulation into a common MPLS format, thus allowing carriers to converge their services with an MPLS network.

TDM PW

TDM Pseudowire is a widely used method for carrying Time Division Multiplexed E1, T1, E3, or T3 circuits across PSNs. It enables:

- Enterprises to run voice, video, and legacy data over the PSN
- Service providers to provide revenue-generating legacy voice and data services over the PSN
- Data carriers to offer PSN-based leased and private lines

ATM PW

ATM Pseudowire (RFC 4816) is a transparent cell transport service that allows migration of ATM services to a PSN without having to provision the ATM subscriber or CE devices. ATM CEs view the ATM transparent cell transport service as if they were directly connected via a TDM leased line. This service is used as an internal function in an ATM service provider's network as a way to connect existing ATM switches via a higher-speed PSN, or to provide ATM backhaul services for remote access to existing ATM networks.

PW-to-TE Tunnel Mapping

PW-to-TE Tunnel Mapping (RFC 5602) permits operation of pseudowire services across MPLS PSNs by mapping pseudowires to MPLS TE tunnels.

Multi-Segment PW

A Multi-Segment Pseudowire (MS-PW) is a statically or dynamically configured set of two or more contiguous PW segments that behave and function as a single point-to-point PW. MS-PW thus extends PW across more than one packet switched network (PSN) domain, multiple provider domains, and different PSN types.

Information Model Objects (IMOs)

This section describes the following IMO:

- [PTP Layer 2 MPLS Tunnel Interface \(IPTPLayer2MplsTunnel\)](#)

PTP Layer 2 MPLS Tunnel Interface

The network/data link layer [PTP Layer 2 MPLS Tunnel Interface](#) object is bound by its Containing Termination Points attribute to a data link layer interface object. It is accessed primarily by [Label Switching Entity](#).

For multi-segment PW, at the VNE layer, ANA maintains stitching between two [IPTPLayer2MplsTunnel](#) (PW endpoints), as [Local Switching Entry](#) under [Local Switching Entity](#).

Table 17-1 **PTP Layer 2 MPLS Tunnel Interface (IPTPLayer2MplsTunnel)**

Attribute Name	Attribute Description	Scheme	Polling Interval
Local and Remote Router Addresses	Local and remote router IP addresses	IPCore	Configuration
Local and Remote Virtual Connection Labels	Local and remote virtual connection labels	IPCore	Configuration
Tunnel Identification	Tunnel identifier	IPCore	Configuration
Tunnel Status	Tunnel status (<i>Unknown, Up, Down</i>)	IPCore	Configuration
Local and Remote Tunnel Interface	Local and remote tunnel interface Object Identifier	IPCore	Configuration
IANA Type	Internet Assigned Numbers Authority (IANA) type of the sublayer	N/A	N/A
Containing Termination Points	Underlying termination points (connection or physical)	IPCore	N/A
Contained Connection Termination Points	Bound connection termination points (Tunnel Container)	IPCore	N/A
Pseudowire Type	The MPLS pseudowire type (for example, <i>Ethernet</i> , <i>SAToP</i> , and so on)	IPCore	Configuration
Preferred Path Tunnel	The Object Identifier of the preferred path	IPCore	Configuration
Local MTU	The local MTU	IPCore	Configuration
Remote MTU	The remote MTU	IPCore	Configuration
Peer Status	Status of the signaling peer	IPCore	Configuration
Signaling Protocol	The signaling protocol	IPCore	Configuration
VFI Name	The name of the VFI	IPCore	Configuration

Vendor-Specific Inventory and IMOs

There are no vendor-specific inventory or IMOs for this technology.

Network Topology

Cisco ANA 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.

Service Alarms

The following alarm is supported for this technology:

- [Layer 2 Tunnel Down](#), page 41-40



CHAPTER 18

Ethernet (IEEE 802.3)

This chapter describes the level of support that Cisco ANA provides for Ethernet, as follows:

- [Technology Description, page 18-1](#)
- [Information Model Objects \(IMOs\), page 18-5](#)
- [Vendor-Specific Inventory and IMOs, page 18-19](#)
- [Network Topology, page 18-21](#)
- [Service Alarms, page 18-22](#)

Technology Description

This section provides the following Ethernet technology descriptions:

- [Ethernet \(IEEE 802.3\)](#)
- [VLAN \(IEEE 802.1Q\)](#)
- [QinQ \(IEEE802.1ad\)](#)
- [LAG](#)
- [EtherChannel](#)
- [STP](#)
- [SVI](#)
- [VTP](#)
- [VPLS](#)
- [H-VPLS](#)
- [REP](#)

Please see Part 1: Cisco VNEs in this guide for information about which devices support the various technologies.

Ethernet (IEEE 802.3)

Ethernet refers to the family of LAN products covered by the IEEE 802.3 standard that defines the carrier sense multiple access collision detect (CSMA/CD) protocol. Four data rates are currently defined for operation over optical fiber and twisted-pair cables: 10Base-T Ethernet (10 Mb/s), Fast Ethernet (100 Mb/s), Gigabit Ethernet (1000 Mb/s) and 10-Gigabit Ethernet (10 Gb/s).

The IEEE 802.3 standard provides MAC (Layer 2) addressing, duplexing, differential services, and flow control attributes, and various physical (Layer 1) definitions, with media, clocking, and speed attributes. It also provides a [LAG](#) (similar to [EtherChannel](#)) definition for providing both higher link capacity and availability.

VLAN (IEEE 802.1Q)

A virtual LAN (VLAN), is a logical group of hosts that communicate as if they were attached to the same network broadcast domain, even though they do not share the same physical location or network switch. Although much like a physical LAN, VLAN hosts can be grouped together even if they are not located on the same network switch. Because a VLAN is a logical entity, its creation and reconfiguration is done through software, rather than by physically locating devices.

IEEE 802.1Q, or VLAN Tagging, is an IEEE standard allowing multiple bridged networks to transparently share the same physical network link without leakage. IEEE 802.1Q (and its shortened form, dot1q) is used to refer to the encapsulation protocol used to implement this mechanism over Ethernet networks.

QinQ (IEEE802.1ad)

QinQ (IEEE802.1) tagging (also known as dot1q tunneling) is a technology that allows the nesting of an additional VLAN tag on a packet, in addition to an existing one. According to the standard, either VLAN tag is an 802.1Q header.

QinQ allows service providers to use a single VLAN to support customers who have multiple VLANs. The core service-provider network carries 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 and without affecting the traffic of other customers.

LAG

A Link Aggregation Group (LAG) is a group of two or more network links bundled together to appear as a single link based on the IEEE 802.3ad standard. For instance, bundling two 100-Mb/s network interfaces into a single link creates one 200-Mb/s link. A LAG may include two or more network cards and two or more cables, but the software sees the link as one logical link.

A LAG provides capacity increase, load balancing, and higher link availability, which prevents the failure of any single component link leading to a disruption of the communications between the interconnected devices.

EtherChannel

EtherChannel is Cisco's link aggregation port trunking technology. Like [LAG](#), it unifies physical Ethernet links into one link to provide high-speed links between switches, routers, and servers. An EtherChannel can be formed from two to eight active Fast Ethernet, Gigabit Ethernet, or 10 Gigabit Ethernet ports. It also provides fault tolerance in the form of from one to eight inactive failover ports, which can also be aggregated and which become active if the other active ports fail. EtherChannel is primarily a backbone network technology, providing up to 800 Mbps, 8 Gbps, or 80 Gbps of aggregate bandwidth depending on the speeds of the underlying links (100 Mbps, 1 Gbps, or 10 Gbps). Cisco's Virtual Switching System also provides Multichassis EtherChannel (MEC), in which ports can be aggregated toward different physical chassis, forming a single virtual switch.

STP

Spanning Tree Protocol (STP) is a Layer 2 link management protocol that provides path redundancy while preventing undesirable loops in the network. For a Layer 2 Ethernet network to function properly, only one active path can exist between any two devices.

STP defines a tree with a root bridge and a loop-free path from the root to all network devices in the Layer 2 network. STP forces redundant data paths into a standby (blocked) state. If a network segment in the spanning tree fails and a redundant path exists, the STP algorithm recalculates the spanning tree topology and activates the standby path.

Cisco ANA STP modeling supports devices that use the following STP variants:

- STP as defined in the 802.1D standard
- Rapid Spanning Tree Protocol (RSTP) as defined in the 802.1w standard
- Per-VLAN STP (PvSTP and PvSTP+), which are proprietary Cisco protocols, or any per-VLAN spanning tree protocol
- Multiple Spanning Tree protocol (MST) as defined in the 802.1s standard

Note that Cisco ANA does not support these STP modes when they are configured along with a bridge group.

SVI

A switch virtual interface (SVI) is a VLAN of switch ports, represented by one interface to a routing or bridging system. There is no physical interface for the VLAN. The SVI provides the Layer 3 processing for packets from all switch ports associated with the VLAN.

There is one-to-one mapping between a VLAN and SVI. Only a single SVI can be mapped to a VLAN, and the SVI cannot be activated unless associated with a physical port.

SVIs simplify VLAN routing by providing default gateway for the VLAN. They also provide layer 3 switch connectivity to the switch, and provide fallback bridging when required for non routable protocols.

VTP

VLAN Trunk (or Trunking) Protocol (VTP) is a Cisco proprietary Layer 2 messaging protocol that reduces administrative chores in a switched network by managing the addition, deletion, and renaming of VLANs on a network-wide basis. It permits configuration of VLANs on a single VTP server, with the VLAN distributed through all switches in the domain. To enable this, VTP carries VLAN information to all the switches in the VTP domain, using advertisements sent over Inter-Switch Link (ISL), 802.1q, IEEE 802.10 or LAN Emulation (LANE) trunks. VTP traffic is sent over the management VLAN (VLAN1), so all VLAN trunks must be configured to pass VLAN1.

VPLS

Virtual Private LAN Services (VPLS) is a class of Layer 2 VPN that provides Ethernet-based multipoint-to-multipoint communication over MPLS networks. It allows geographically dispersed sites to share an Ethernet broadcast domain by connecting sites through pseudowires. The network then emulates the function of a LAN switch or bridge to connect the different LAN segments to create a single bridged (Ethernet) LAN.

VPLS uses the provider core to join multiple attachment circuits together to simulate a virtual bridge that connects the multiple attachment circuits together. From a customer point of view, there is no topology for VPLS. All of the CE devices appear to connect to a logical bridge emulated by the provider core. The logical bridge performs MAC address learning, just like a physical bridge.

The Virtual Switching Instance (VSI), also known as the Virtual Forwarding Instance (VFI), is the main component in the PE router which constructs the logical bridge. All VSIs which construct a provider logical bridge are connected with MPLS PWs.

Learning is done based on the customer Ethernet frame arriving at the VSI. A Forwarding Information Base (FIB) keeps track of the mapping of customer Ethernet frame addressing and the appropriate pseudowire to use.

H-VPLS

Hierarchical VPLS (H-VPLS) improves the scalability characteristics of VPLS by reducing signaling overhead and packet replication requirements for the provider edge. Two types of provider edge devices are defined in this model:

- User-facing provider edge (u-PE)
- Network provider edge (n-PE)

Customer edge devices connect to u-PEs directly and aggregate VPLS traffic before it reaches the n-PE, where the VPLS forwarding takes place based on the VSI. In this hierarchical model, u-PEs are expected to support Layer 2 switching and to perform normal bridging functions. Cisco VPLS uses 802.1Q Tunneling, a double 802.1Q or QinQ encapsulation, to aggregate traffic between the u-PE and n-PE. The QinQ trunk becomes an access port to a VPLS instance on an n-PE.

REP

Cisco Resilient Ethernet Protocol (REP) is a new technology implemented on Cisco Carrier Ethernet switches and intelligent service edge routers. It extends network resiliency across Cisco IP Next-Generation Network (NGN) Carrier Ethernet Design. Requiring no hardware upgrades, REP is designed to provide network and application convergence within 50 ms. In some scenarios, the network convergence times may increase to within 250 ms, but a 250-ms convergence time is still expected to have limited or no discernible effect on most network applications. REP is a segment protocol that integrates easily into existing Carrier Ethernet networks. It is not intended to replace STP, but allows network architects to limit the scope of STP domains. Since Cisco REP can also notify STP about potential topology changes, it allows for interoperability with STP. Ideally, REP can be positioned as a migration strategy from legacy spanning tree domains.

Because REP is a distributed and secure protocol, it does not rely on a master node controlling the status of the ring. Hence failures can be detected locally either through loss of signal (LOS) or loss of neighbor adjacency. Any REP port can initiate a switchover as long as it has acquired the secure key to unblock the alternate port. By default, REP elects an alternate port unless the administrator defines a preferred port. For optimal bandwidth usage and for traffic engineering, REP supports load balancing per group of VLANs.

Information Model Objects (IMOs)

This section describes the following IMOs:

- [Link Aggregation Group \(ILinkAggregationGroup802dot3ad\)](#)
- [Link Aggregation Group Port Entry \(ILagPortEntry\)](#)
- [Ethernet Interface \(IEthernet\)](#)
- [Ethernet Physical \(IPhysicalLayer\)](#)
- [Virtual LAN Interface \(IVlanInterface\)](#)
- [Virtual LAN Entry \(IVlanEntry\)](#)
- [Virtual LAN Multiplexer \(IVlanEncapMux\)](#)
- [Virtual LAN Encapsulation \(IIEEE802\)](#)
- [Virtual LAN Mapping \(IVlanMapping\)](#)
- [Data Link Aggregation Container \(IDataLinkAggregationContainer\)](#)
- [Spanning Tree Protocol Service \(IStpService\)](#)
- [Multiple Spanning Tree Protocol Service \(IMstService\)](#)
- [Multiple Spanning Tree Protocol Properties \(IMstProperties\)](#)
- [Spanning Tree Protocol Instance Information \(IStpInstanceInfo\)](#)
- [Multiple Spanning Tree Protocol Instance Information \(IMstInstanceInfo\)](#)
- [Per-VLAN Spanning Tree Protocol Service \(IPvstpService\)](#)
- [Per-VLAN Spanning Tree Protocol Instance Information \(IPvstpInstanceInfo\)](#)
- [Per-VLAN Spanning Tree Protocol Port Information \(IPvstPortInfo\)](#)
- [Rapid Spanning Tree Protocol Instance Information \(IRstpInstanceInfo\)](#)
- [Spanning Tree Protocol Port Information \(IStpPortInfo\)](#)

- [Multiple Spanning Tree Protocol Port Information \(IMstPortInfo\)](#)
- [Virtual Switch Interface \(IVsi\)](#)
- [Pseudowire Properties \(IPseudowireProperties\)](#)
- [VLAN Tagged Interface \(IVLANTaggedInterface\)](#)
- [Ethernet Flow Point \(IEfp\)](#)
- [VLAN Trunking Protocol Service \(IVtpService\)](#)

Link Aggregation Group

The data link layer [Link Aggregation Group](#) object aggregates multiple [Ethernet Interfaces](#), which it is bound to by its Containing Termination Points attribute. It is accessed primarily by the [Virtual LAN Multiplexer](#) bound by its Contained Connection Termination Points attribute. It is also accessed by the [Common Components](#).

Table 18-1 *Link Aggregation Group (ILinkAggregationGroup802dot3ad)*

Attribute Name	Attribute Description	Scheme	Polling Interval
Group Number	Group identifier of the aggregated Ethernet interfaces	Any	Configuration
Bandwidth	Accumulated bandwidth of all aggregated Ethernet interfaces in Mb/s	Any	Configuration
Aggregation Protocol	Aggregation protocol (<i>None, LACP, PAGP</i>)	Any	Configuration
IANA Type	Internet Assigned Numbers Authority (IANA) type of the sublayer	N/A	N/A
Containing Connection Termination Points	Underlying termination points (Ethernet Interface)	Any	N/A
Contained Connection Termination Points	Bound connection termination points	Any	N/A

Link Aggregation Group Port Entry

The [Link Aggregation Group Port Entry](#) object describes the Link Aggregation Control configuration parameters for each aggregation port of a [Link Aggregation Group](#).

Table 18-2 *Link Aggregation Group Port Entry (ILagPortEntry)*

Attribute Name	Attribute Description	Scheme	Polling Interval
Actor and Partner Administrative Keys	Actor and partner administrative keys	Any	Configuration
Actor and Partner Operational Keys	Actor and partner operational keys	Any	Configuration
Selected and Attached Aggregation Identification	Selected and attached aggregation identifier	Any	Configuration
Actor Port	Actor port	Any	Configuration
Actor Port Priority	Actor port priority	Any	Configuration
Partner Administrative and Operational Port	Partner administrative and operational port	Any	Configuration

Table 18-2 *Link Aggregation Group Port Entry (ILagPortEntry) (continued)*

Attribute Name	Attribute Description	Scheme	Polling Interval
Partner Administrative and Operational Port Priority	Partner administrative and operational port priority	Any	Configuration
Actor and Partner Administrative States	Actor and partner administrative states	Any	Configuration
Actor and Partner Operational States	Actor and partner operational states	Any	Configuration

Ethernet Interface

The data link layer [Ethernet Interface](#) object is bound by its Containing Termination Points attribute to a physical layer interface ([Ethernet Physical](#)) object. It is accessed primarily by the [Virtual LAN Multiplexer/Interface](#), [Link Aggregation Group](#), [Cisco Ethernet Channel](#) or [IP Interface](#) bound by its Contained Connection Termination Points attribute. It is also accessed by the [Bridging Entity](#).

Table 18-3 *Ethernet Interface (IEthernet)*

Attribute Name	Attribute Description	Scheme	Polling Interval
MAC Address	MAC address	Product	Configuration
Duplex Mode	Duplex mode (<i>Unknown, Full, Half</i>)	Any	Configuration
Output Flow Control	Output flow control (<i>Enable, Disable</i>)	Any	Configuration
Input Flow Control	Input flow control (<i>Enable, Disable</i>)	Any	Configuration
IANA Type	Internet Assigned Numbers Authority (IANA) type of the sublayer	N/A	N/A
Containing Connection Termination Points	Underlying termination points (connection or physical)	Any	N/A
Contained Connection Termination Points	Bound Connection Termination Point	Any	N/A
Port Type	The port type	Any	N/A
Is ELMI Enabled	Determines whether ELMI is enabled on the interface. See Ethernet OAM for more information.	Any	Configuration
OAM Admin Status	The OAM technology administrative status (<i>Down, Testing, Unknown, Up</i>). See Ethernet OAM for more information.	Any	Configuration
Aggregation Group	Ethernet Aggregation technologies such as Link Aggregation (IEEE 802.1ad) and Cisco EtherChannel are used to group several physical Ethernet interfaces/links into one logical interface/link to provide higher bandwidth and availability in fault scenarios. If this Ethernet Interface participates in an aggregation group, this property specifies the OID of the aggregation group. This information is updated by the VNE model based on polling of the LAG and EtherChannel information.	Any	Configuration
Auto-Negotiate	Specify if the Ethernet port is configured to auto-negotiate with its connected peer on communication parameters such as Speed and Duplex mode. Auto-negotiation was originally defined in the FastEthernet Standard (IEEE 802.3u) and later was significantly extended in the GigabitEthernet standard (IEEE 802.3ab).	Any	Configuration

Table 18-3 Ethernet Interface (IEthernet) (continued)

Attribute Name	Attribute Description	Scheme	Polling Interval
Efps	The list of EFPs (L2 sub-interfaces/service instances) which are configured on this Ethernet interface. This information is updated by the VNE model based on polling of the EFP information (L2 sub-interfaces or Service Instances).	Any	Configuration
UNI Properties	A set of User-Network-Interface properties which are available as part of the ELMI configuration of the Ethernet interface.	Any	Configuration

Ethernet Physical

The physical layer [Ethernet Physical](#) object is bound by its Containing Termination Points attribute to a [Port Connector](#) object. It is accessed by the data link layer [Ethernet Interface](#) bound by its Contained Connection Termination Points attribute.

Table 18-4 Ethernet Physical (IPhysicalLayer)

Attribute Name	Attribute Description	Scheme	Polling Interval
All attributes are the same as those of Physical Layer (IPhysicalLayer) .			

Virtual LAN Interface

The data link layer [Virtual LAN Interface](#) object, which is used in a switched LAN environment, is bound by its Containing Termination Points attribute to an [Ethernet Interface](#) object. It is accessed primarily by the network layer object (such as [IP Interface](#)) bound by its Contained Connection Termination Points attribute. It is also accessed by the [Bridging Entity](#).

Table 18-5 Virtual LAN Interface (IVlanInterface)

Attribute Name	Attribute Description	Scheme	Polling Interval
Mode	VLAN mode (<i>Access, Trunk, 802.1Q Tunnel</i>)	Any	Configuration
Native VLAN Identification	VLAN identifier, used for untagged received and transmitted frames	Any	Configuration
Virtual LAN Table	Array of Virtual LAN Entries (instances of IVlanEntry) configured for this VLAN interface	Any	Configuration
VlanMappings	Array of all Virtual LAN Mappings (instances of IVlanMapping) defined for this VLAN interface	Product	Configuration
IANA Type	Internet Assigned Numbers Authority (IANA) type of the sublayer	N/A	N/A
Containing Connection Termination Points	Underlying termination points (connection or physical)	Any	N/A
Contained Connection Termination Points	Bound connection termination points	Any	N/A

Virtual LAN Entry

The [Virtual LAN Entry](#) object describes the association of a [Virtual LAN Interface](#), which operates in Trunk mode, to one of the bridged Virtual LANs configured in the device.

Table 18-6 *Virtual LAN Entry (IVlanEntry)*

Attribute Name	Attribute Description	Scheme	Polling Interval
VLAN Identification	VLAN identifier of received and transmitted frames	Any	Configuration
Encapsulation Type	VLAN encapsulation (<i>Unknown, ISL, IEEE 802.10, IEEE 802.1Q</i>)	Any	Configuration
Upper Layer	Upper layer Object Identifier (OID)	Any	Configuration

Virtual LAN Multiplexer

The [Virtual LAN Multiplexer](#) object, used in a routed LAN environment, is bound by its Containing Termination Points attribute to an [Ethernet Interface](#) object. It is accessed primarily by the data link layer [Virtual LAN Encapsulations](#) bound by its Contained Connection Termination Points attribute.

Table 18-7 *Virtual LAN Multiplexer (IVlanEncapMux)*

Attribute Name	Attribute Description	Scheme	Polling Interval
IANA Type	Internet Assigned Numbers Authority (IANA) type of the sublayer	N/A	N/A
Containing Termination Points	Underlying termination points (Ethernet Interface)	Any	N/A
Contained Connection Termination Points	Bound connection termination points (Virtual LAN Encapsulations)	Any	N/A

Virtual LAN Encapsulation

The data link layer [Virtual LAN Encapsulation](#) object, used in a routed LAN environment, is bound by its Containing Termination Points attribute to a [Virtual LAN Multiplexer](#) object. It is accessed primarily by the Network layer object (such as [IP Interface](#)) bound by its Contained Connection Termination Points attribute. It is also accessed by the [Bridging Entity](#).

Table 18-8 *Virtual LAN Encapsulation (IIEEE802)*

Attribute Name	Attribute Description	Scheme	Polling Interval
VLAN Identification	VLAN identifier	Any	Configuration
IANA Type	Internet Assigned Numbers Authority (IANA) type of the sublayer	N/A	N/A
Containing Connection Termination Points	Underlying termination points (connection or physical)	Any	N/A
Contained Connection Termination Points	Bound Connection Termination Point	Any	N/A

Virtual LAN Mapping

The data link layer [Virtual LAN Mapping](#) object, used in a routed LAN environment, is bound by its Containing Termination Points attribute to a [Virtual LAN Multiplexer](#) object. It is accessed primarily by the Network layer object (such as [IP Interface](#)) bound by its Contained Connection Termination Points attribute. It is also accessed by the [Bridging Entity](#).

Table 18-9 *Virtual LAN Mapping (IVlanMapping)*

Attribute Name	Attribute Description	Scheme	Polling Interval
Direction	Describes whether the VLAN mapping is defined in the egress or ingress direction	Product	Configuration
VLANRewriteDefinition	The rewriting actions (push tag, pop tag, and so on.) to be done over the frames which fit the match criteria.	Product	Configuration
VLANMatchCriteria	Defines the frames which undergo the VLAN mapping.	Product	Status
Drop	Defines if the frame should be dropped, instead of undergoing a rewrite definition.	Product	Status

Data Link Aggregation Container

The [Data Link Aggregation Container](#) object aggregates or contains a single type of data link aggregation, such as [Link Aggregation Group](#) or [Cisco Ethernet Channel](#).

Table 18-10 *Data Link Aggregation Container (IDataLinkAggregationContainer)*

Attribute Name	Attribute Description	Scheme	Polling Interval
Data Link Aggregations	Array of single-type data link aggregations (Link Aggregation Group , Cisco Ethernet Channel)	Any	Configuration
Type	Aggregation type (<i>Null</i> , <i>Ethernet Link Aggregator</i>)	Any	Configuration

Spanning Tree Protocol Service

The [Spanning Tree Protocol Service](#) object is used in a switched LAN environment. It describes the Spanning Tree Protocol service. It is accessed only by the [Logical Root](#)'s Services List attribute.

Table 18-11 *Spanning Tree Protocol Service (IStpService)*

Attribute Name	Attribute Description	Scheme	Polling Interval
Protocol Type	Spanning Tree Protocol type (<i>Unknown</i> , <i>STP</i> , <i>RSTP</i> , <i>PVSTP</i> , <i>MST</i>)	Any	Configuration
Current Maximum Age	The current used value for the maximum age of learned Spanning Tree Protocol port information (in hundredths of seconds)	Any	Configuration
Current Hello Time	The current used value for hello time messages' keepalive interval of a Spanning Tree Protocol root (in hundredths of seconds)	Any	Configuration
Current Forward Delay	The current used value for port delay in each of the listening and learning states, preceding the forwarding one (in hundredths of seconds)	Any	Configuration

Table 18-11 *Spanning Tree Protocol Service (IStpService) (continued)*

Attribute Name	Attribute Description	Scheme	Polling Interval
Instance Information Table	Array of Spanning Tree Protocol Instance Information	Any	Configuration
UplinkFast State	Indicates whether the UplinkFast feature is enabled (<i>true, false</i>)	Any	Configuration
BackboneFast State	Indicates whether the BackboneFast feature is enabled (<i>true, false</i>)	Any	Configuration
Bridge Maximum Age	The value that all bridges should use (when this bridge is acting as the root) for the maximum age of learned Spanning Tree Protocol port information (in hundredths of seconds)	Any	Configuration
Bridge Hello Time	The value that all bridges should use (when this bridge is acting as the root) for hello time messages' keepalive interval of a Spanning Tree Protocol root (in hundredths of seconds)	Any	Configuration
Bridge Forward Delay	The current used value, 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)	Any	Configuration

All additional attributes are the same as [System Service \(ISystemService\)](#)

Multiple Spanning Tree Protocol Service

The [Multiple Spanning Tree Protocol Service](#) object is used in a switched VLAN environment. It describes the Spanning Tree Protocol service. It is accessed only by the [Logical Root](#)'s Services List attribute.

Table 18-12 *Multiple Spanning Tree Protocol Service (IMstService)*

Attribute Name	Attribute Description	Scheme	Polling Interval
Protocol Properties	Multiple Spanning Tree Protocol properties	Any	Configuration

All additional attributes are the same as [Spanning Tree Protocol Service \(IStpService\)](#).

Multiple Spanning Tree Protocol Properties

The [Multiple Spanning Tree Protocol Properties](#) object, used in a switched VLAN environment. It describes the Multiple Spanning Tree Protocol properties. It is accessed only by the [Multiple Spanning Tree Protocol Service](#)'s Protocol Properties attribute.

Table 18-13 *Multiple Spanning Tree Protocol Properties (IMstProperties)*

Attribute Name	Attribute Description	Scheme	Polling Interval
Force Version	Force version (<i>Unknown, STP, RSTP, PVSTP, MST</i>)	Any	Configuration
Configuration Format	Configuration format used by this device and negotiated with other devices	Any	Configuration
Region Name	Region name used by this device and negotiated with other devices	Any	Configuration
Revision Level	Revision level used by this device and negotiated with other devices	Any	Configuration

Table 18-13 Multiple Spanning Tree Protocol Properties (IMstProperties) (continued)

Attribute Name	Attribute Description	Scheme	Polling Interval
External Root Cost	External root cost of this Multiple Spanning Tree Protocol	Any	Configuration
Maximum Instances	Maximum Multiple Spanning Tree Protocol instances	Any	Configuration

Spanning Tree Protocol Instance Information

The following [Rapid Spanning Tree Protocol Instance Information](#) objects describe the instance information associated with and accessed by the [Multiple Spanning Tree Protocol Service](#)'s Instance Information Table attribute.

Table 18-14 Spanning Tree Protocol Instance Information (IStplInstanceInfo)

Attribute Name	Attribute Description	Scheme	Polling Interval
Object Identification	Instance Object Identifier (OID)	Any	Configuration
Identification	Bridge identifier (MAC address)	Any	Configuration
Priority	Bridge priority in the Spanning Tree Protocol	Any	Configuration
Designated Root and Bridge	MAC addresses of the designated root and bridge in the spanning tree	Any	Configuration
Root Cost	Root cost value for this bridge	Any	Configuration
Is Root	Is this bridge currently the root of the Spanning Tree Protocol? (<i>True, False</i>)	Any	Configuration
Root Port Identification	Object Identifier (OID) of the bridge port used to reach the designated root	Any	Configuration
Port Information Table	Array of Spanning Tree Protocol Port Information	Any	Configuration

Multiple Spanning Tree Protocol Instance Information

Table 18-15 Multiple Spanning Tree Protocol Instance Information (IMstInstanceInfo)

Attribute Name	Attribute Description	Scheme	Polling Interval
Instance Identification	Multiple Spanning Tree Protocol instance identifier	Any	Configuration

All additional attributes are the same as [Spanning Tree Protocol Instance Information \(IStplInstanceInfo\)](#)

Per-VLAN Spanning Tree Protocol Service

The [Per-VLAN Spanning Tree Protocol Service](#) object is used in a switched VLAN environment. It describes the Per-VLAN Spanning Tree Protocol service. It is accessed only by the [Logical Root](#)'s Services List attribute.

Table 18-16 Per-VLAN Spanning Tree Protocol Service (IPvstpService)

Attribute Name	Attribute Description	Scheme	Polling Interval
UplinkFast	Indicates whether the UplinkFast feature is enabled (<i>true, false</i>)	Any	Configuration
BackboneFast	Indicates whether the BackboneFast feature is enabled (<i>true, false</i>)	Any	Configuration

Per-VLAN Spanning Tree Protocol Instance Information

Table 18-17 Per-VLAN Spanning Tree Protocol Instance Information (IPvstpInstanceInfo)

Attribute Name	Attribute Description	Scheme	Polling Interval
Protocol Type	Spanning tree protocol type (<i>Unknown, STP, RSTP, PVSTP, MST</i>)	Any	Configuration
Current and Bridge Maximum Age	The current used value, and the value that all bridges should use when this bridge is acting as the root, for the maximum age of learned Spanning Tree Protocol port information (in hundredths of seconds)	Any	Configuration
Current and Bridge Hello Time	The current used value, and the value that all bridges should use when this bridge is acting as the root, for hello time messages' keepalive interval of a Spanning Tree Protocol root (in hundredths of seconds)	Any	Configuration
Current and Bridge Forward Delay	The current used value, 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)	Any	Configuration

All additional attributes are the same as [Spanning Tree Protocol Instance Information \(IStpInstanceInfo\)](#)

Per-VLAN Spanning Tree Protocol Port Information

Table 18-18 Per-VLAN Spanning Tree Protocol Port Information (IPvstpPortInfo)

Attribute Name	Attribute Description	Scheme	Polling Interval
PortFast State	Indicates whether PortFast is enabled on the port (<i>true, false</i>)	Any	Configuration

Rapid Spanning Tree Protocol Instance Information

Table 18-19 *Rapid Spanning Tree Protocol Instance Information (IRstpInstanceInfo)*

Attribute Name	Attribute Description	Scheme	Polling Interval
Force Version	Force version (<i>Unknown, STP, RSTP, PVSTP, MST</i>)	Any	Configuration

All additional attributes are the same as [Spanning Tree Protocol Instance Information \(IStpInstanceInfo\)](#)

Spanning Tree Protocol Port Information

The following [Spanning Tree Protocol Port Information](#) objects describe the port information associated with and accessed by the [Spanning Tree Protocol Instance Information](#)'s Port Information Table attribute.

Table 18-20 *Spanning Tree Protocol Port Information (IStpPortInfo)*

Attribute Name	Attribute Description	Scheme	Polling Interval
Object Identification	Port Object Identifier (OID)	Any	Configuration
Priority	Port priority in the Spanning Tree Protocol	Any	Configuration
State	Port state (<i>Unknown, Disable, Blocking, Listening, Learning, Forwarding, Broken, Down, LoopBack</i>)	Any	Configuration
Path Cost	Port path cost, which represents the media speed for this port	Any	Configuration
Is Edge	Is this an edge port (connected to a nonbridging device)? (<i>True, False</i>)	Any	Configuration
Is Point To Point	Is this port connected to a point-to-point link? (<i>True, False</i>)	Any	Configuration
Role	Port role (<i>Unknown, Disable, Backup, Alternative, Designated, Root, Boundary</i>)	Any	Configuration
Port BPDU Guard State	Indicates whether the PortFast Bridge Protocol Data Unit guard is enabled on the port	Any	Configuration
Port BPDU Filter State	Indicates whether PortFast Bridge Protocol Data Unit filtering is enabled on the port	Any	Configuration

Multiple Spanning Tree Protocol Port Information

Table 18-21 *Multiple Spanning Tree Protocol Port Information (IMstPortInfo)*

Attribute Name	Attribute Description	Scheme	Polling Interval
Hello Time	Hello time messages' keepalive interval of a Spanning Tree Protocol root (in hundredths of a second)	Any	Configuration

All additional attributes are the same as [Spanning Tree Protocol Port Information \(IStpPortInfo\)](#)

Virtual Switching Instance

The [Virtual Switching Instance](#) object represents a Virtual Switching Instance (also known as VFI, Virtual Forwarding Instance) component of a VPLS logical bridge.

Table 18-22 *Virtual Switch Interface (IVsi)*

Attribute Name	Attribute Description	Scheme	Polling Interval
VPLS Instance Name	The unique VPLS instance name	IPCore	Configuration
VPLS VPN ID	The unique VPN ID in the MPLS core	IPCore	Configuration
discoveryMode	The VSI discovery mode (<i>Manual, BGP, LDP, RADIUS, DNS, MSS/OSS, Unknown</i>)	IPCore	Configuration
vsiMode	The VSI mode (<i>point-to-point, multipoint, unknown</i>)	IPCore	Configuration
Operational state	The operational status of the VPLS instance (<i>up, down</i>)	IPCore	Configuration
Administrative state	The configured administrative status of the VPLS instance (<i>enabled, disabled</i>)	IPCore	Configuration
Pseudowires	An array of Pseudowire Properties (IPseudowireProperties) .	IPCore	System

Pseudowire Properties

The [Pseudowire Properties](#) object represents an MPLS pseudowire connecting two or more [Virtual Switching Instances](#).

Table 18-23 *Pseudowire Properties (IPseudowireProperties)*

Attribute Name	Attribute Description	Scheme	Polling Interval
Pseudowire OID	The Object Identifier of the pseudowire	IPCore	System
isSplitHorizonEnabled	Indicates whether split horizon is enabled on the pseudowire (<i>true, false</i>). The split horizon policy determines whether packets are returned to the MPLS core.	IPCore	System
isAutoDiscovered	Indicates how the pseudowire was discovered (<i>manual, automatic</i>).	IPCore	System

VLAN Tagged Interface

This IMO represents the VLAN layer of a L3 Ethernet sub-interface. It includes the configuration information of the sub-interface, for example, the VLAN tags Match Criteria, and the status of the sub-interface.

The VLANTaggedInterface IMO deprecates the IEEE802dot1q IMO that represents only a single VLAN tagged sub-interface.

Table 18-24 VLAN Tagged Interface (IVLANTaggedInterface)

Attribute Name	Attribute Description	Scheme	Polling Interval
InterfaceName	The interface name of the Ethernet sub-interface. This name is unique in the context of a device and is used to identify the sub-interface in the CLI interface. In Cisco IOS/IOS-XR devices the format of the interface name for Ethernet sub-interface is: <type><port-location>.<sub-interface-id> For example: GigaEthernet0/0.100	Any	Configuration
Inner Vlan Id	The configured customer-edge VLAN (CE-VLAN) ID.	Any	Configuration
Outer Vlan Id	The configured service-provider VLAN (SP-VLAN) ID.	Any	Configuration
SP VLAN ID	Service Provider VLAN ID, also referred to as the Outer VLAN. This value represents the outer VLAN ID used in a specific path trace. This attribute is used only in PathTool when doing a path trace that traverses the Ethernet sub-interface.	N/A	N/A
CE VLAN ID	Customer Edge VLAN ID, also referred to as the Inner VLAN. This value represents the inner VLAN ID used in a specific path trace. This attribute is used only in PathTool when doing a path trace that traverses the Ethernet sub-interface.	N/A	N/A
Encap Type	The encapsulation type (<i>dot1Q</i> , <i>QinQ</i>).	Any	Configuration
Match Criteria	VLAN layer-related information used to define matching criteria performed on the traffic ingress on this Ethernet sub interface. This is a general class used for L2 and L3 Ethernet sub-interfaces. For L3 Ethernet sub-interfaces only, Tagged VLANMatchCriteria is used, which defines one of two VLAN tags as the traffic match criteria.	Any	Configuration
Operational state	The operational state of the Ethernet sub-interface (<i>Up</i> , <i>Down</i> , <i>Unknown</i> , <i>Testing</i>). This state is derived from the ifOperStatus (1.3.6.1.2.1.2.2.1.7) defined in IF-MIB. For more information please refer to IF-MIB definition (section 6) http://www.rfc-editor.org/rfc/rfc2863.txt	Any	System
Administrative state	The administrative state of the Ethernet sub-interface (<i>Up</i> , <i>Down</i> , <i>Unknown</i> , <i>Testing</i>). This state is derived from the ifAdminStatus (1.3.6.1.2.1.2.2.1.7) defined in IF-MIB. For more information please refer to IF-MIB definition (section 6) http://www.rfc-editor.org/rfc/rfc2863.txt	Any	System

Table 18-24 VLAN Tagged Interface (IVLANTaggedInterface) (continued)

Attribute Name	Attribute Description	Scheme	Polling Interval
Configured Description	A free text string configured on the device on the sub-interface. The description is mainly used to help adlp administration by adding non-networking information that cannot be captured as part of the sub-interface configuration.	Any	Configuration
Binding	The OID of the entity in the VNE to which the sub-interface is bound. Possible values are the IBridgeOid, IPTPLayer2MplsTunnelOid (Pseudowire edge OID), ILocalSwitchingEntry.	Any	Configuration

Ethernet Flow Point

This IMO represents a L2 Ethernet sub-interface (or Service Instance) configured on an Ethernet port. It includes the configuration information of the sub-interface, such as the VLAN tags Match Criteria and VLAN manipulation definitions. It also include the status of the sub-interface.

Multiple EFPs can be configured on a single physical L2 traffic port, usually on the User-Network Interface [UNI] port. Each EFP can manipulate inbound frames in a different manner and make different forwarding decisions.

Table 18-25 Ethernet Flow Point (IEfp)

Attribute Name	Attribute Description	Scheme	Polling Interval
EfpId	ID of the Ethernet Flow Point. The possible values of this attribute are non zero unsigned 32 bit integer (based on the definition of Interface Index in IF-MIB rfc1573.txt, and the definition of Service Instance index (cevcSIIndex) in CISCO-EVC-MIB).	Product	Configuration
RewriteDefinition	The rewrite definition defines the VLAN tag manipulation that will be done on ingress/egress traffic on this sub interface. There are multiple types of Rewrite Definitions that define different types of actions, such as Pop, Push, and Translate, which can operate on 1 or 2 tags.	IPCore	Configuration
AdminStatus	The operational state of the Ethernet sub-interface (<i>Up, Down, Unknown, Testing</i>). This state is derived from the ifOperStatus (1.3.6.1.2.1.2.2.1.7) defined in IF-MIB. For more information please refer to IF-MIB definition (section 6) http://www.rfc-editor.org/rfc/rfc2863.txt	Any	System
OperStatus	The administrative state of the Ethernet sub-interface (<i>Up, Down, Unknown, Testing</i>). This state is derived from the ifAdminStatus (1.3.6.1.2.1.2.2.1.7) defined in IF-MIB. For more information please refer to IF-MIB definition (section 6) http://www.rfc-editor.org/rfc/rfc2863.txt	Any	System
SplitHorizonGroup	The split horizon group to which the EFP is associated. EFPs which are bound to a L2 forwarding entity, specifically a Bridge (representing Bridge Domain configuration), can be divided into groups such that EFPs in the same split horizon group will not be able to communicate directly with each other. If the EFP is not associated to a Bridge, the value will be null, which means no split horizon group is defined. In a configuration in which only one split horizon group exists and it is enabled for the EFP, this value will always be the default group 0.	IPCore	Configuration

Table 18-25 **Ethernet Flow Point (IEfp) (continued)**

Attribute Name	Attribute Description	Scheme	Polling Interval
matchCriteria	VLAN layer-related information used to define matching criteria performed on the traffic ingress on this Ethernet sub-interface. This is a general class used for L2 and L3 Ethernet sub-interfaces. For L3 Ethernet sub-interfaces only, Tagged VLANMatchCriteria is used, which defines one of two VLAN tags as the traffic match criteria.	IPCore	Configuration
Configured Description	A free text string configured on the device on the sub-interface. The description is mainly used to help adlp administration by adding non-networking information that cannot be captured as part of the sub-interface configuration.	Any	Configuration
Binding	The OID of the entity in the VNE to which the sub-interface is bound. Possible values are the IBridgeOid, IPTPLayer2MplsTunnelOid (Pseudowire edge OID), ILocalSwitchingEntry.	Any	Configuration
SP VLAN ID	Service Provider VLAN ID, also referred to as the Outer VLAN. This value represents the outer VLAN ID used in a specific path trace. This attribute is used only in PathTool when doing a path trace that traverses the Ethernet sub-interface.	N/A	N/A
CE VLAN ID	Customer Edge VLAN ID, also referred to as the Inner VLAN. This value represents the inner VLAN ID used in a specific path trace. This attribute is used only in PathTool when doing a path trace that traverses the Ethernet sub-interface.	N/A	N/A
SP Translated VLAN ID	Service Provider translated VLAN ID, also referred to as the translated Outer VLAN. This value represents the outer VLAN ID used in a specific path trace after the VLAN manipulation occurs. This attribute is used only in PathTool when doing a path trace that traverses the Ethernet L2 sub-interface.	N/A	N/A
CE Translated VLAN ID	Customer translated VLAN ID, also referred to as the translated Inner VLAN. This value represents the inner VLAN ID used in a specific path trace after the VLAN manipulation occurs. This attribute is used only in PathTool when doing a path trace that traverses the Ethernet L2 sub-interface.	N/A	N/A

VLAN Trunking Protocol Service

The [VLAN Trunking Protocol Service](#) object represents a VTP configuration on a switch. It extends [System Service](#).

Table 18-26 *VLAN Trunking Protocol Service (IVtpService)*

Attribute Name	Attribute Description	Scheme	Polling Interval
Version	The VTP version (<i>Version1</i> , <i>Version2</i> , <i>Version3</i>)	Product	Configuration
OperatingMode	The VTP mode (<i>Server</i> , <i>Client</i> , <i>Transparent</i> , <i>Primary Server</i> , <i>Secondary Server</i> , <i>Off</i>)	Product	Configuration
DomainName	The VTP domain name	Product	Configuration
ConfigurationRevision	The VTP's configuration revision number	Product	Configuration
isPruningEnabled	Indicates whether VTP is enabled on the switch (<i>True</i> , <i>False</i>)	Product	Configuration
isAuthenticationEnabled	Indicates whether VTP authentication is enabled on the switch (<i>True</i> , <i>False</i>)	Product	Configuration

Vendor-Specific Inventory and IMOs

Vendor-specific IMOs are implemented only for specific vendor devices. The following sections describe vendor-specific objects for this technology:

- [Cisco Ethernet Channel](#)
- [Cisco REP Service](#)
- [Cisco REP Segment Information](#)
- [Cisco REP Port Information](#)

Cisco Ethernet Channel

The [Cisco Ethernet Channel](#) data link layer object aggregates multiple [Ethernet Interfaces](#), to which it is bound by its Containing Termination Points attribute. It is accessed primarily by the [Virtual LAN Multiplexer](#)/Interface or [IP Interface](#) bound by its Contained Connection Termination Points attribute. It is also accessed by the [Bridging Entity](#).

Table 18-27 *Cisco Ethernet Channel (IEthernetChannel)*

Attribute Name	Attribute Description	Scheme	Polling Interval
Group Number	Group identifier of the aggregated Ethernet interfaces	Any	Configuration
Bandwidth	Accumulated bandwidth of all aggregated Ethernet interfaces, in Mb/s	Any	Configuration
Aggregation Protocol	Aggregation protocol (<i>Manual</i> , <i>LACP</i> , <i>PAGP</i>)	Any	Configuration
IANA Type	Internet Assigned Numbers Authority (IANA) type of the sublayer	N/A	N/A
MAC Address	MAC address of the aggregated Ethernet interfaces	Any	Configuration

Table 18-27 Cisco Ethernet Channel (IEthernetChannel) (continued)

Attribute Name	Attribute Description	Scheme	Polling Interval
Administrative Status	Administrative status of the aggregated interfaces	Any	Configuration
Operational Status	Operational status of the aggregated interfaces	Any	Configuration
Containing Connection Termination Points	Underlying termination points (Ethernet Interface)	Any	N/A
Contained Connection Termination Points	Bound connection termination points	Any	N/A

Cisco REP Service

The [Cisco REP Service](#) object represents REP protocol configured on a device.

Table 18-28 Cisco REP Service (IREPService)

Attribute Name	Attribute Description	Scheme	Polling Interval
version	The version of REP being used.	IP Core	Configuration
administrativeVlan	The ID of the administrative VLAN used by REP to transmit its hardware flooding layer messages (an integer from 1 to 4094).	IP Core	Configuration
notificationEnabled	Indicates whether the device will generate REP notifications.	IP Core	Configuration
segmentsTable	An array of Cisco REP Segment Information objects.	IP Core	Configuration

Cisco REP Segment Information

The [Cisco REP Segment Information](#) object represents a single REP segment.

Table 18-29 Cisco REP Segment Information (IREPSegmentInfo)

Attribute Name	Attribute Description	Scheme	Polling Interval
segmentId	The ID of the segment.	IP Core	Configuration
segmentComplete	Indicates whether the segment is complete (that is, no port in the segment is in the “failed” state).	IP Core	Configuration
portsTable	An array of Cisco REP Port Information objects.	IP Core	Configuration

Cisco REP Port Information

The [Cisco REP Port Information](#) object represents a REP port.

Table 18-30 Cisco REP Port Information (IREPPortInfo)

Attribute Name	Attribute Description	Scheme	Polling Interval
portName	The interface name.	IP Core	Configuration
portKey	The Object Identifier of the port.	IP Core	Configuration

Table 18-30 Cisco REP Port Information (IREPPortInfo) (continued)

Attribute Name	Attribute Description	Scheme	Polling Interval
segmentId	The segment of which the interface is a part.	IP Core	Configuration
portType	The type of port (<i>Primary, Secondary, Intermediate</i>).	IP Core	Configuration
portRole	The role the REP port is playing, determined by its link state and whether it is forwarding or blocking traffic (<i>Failed, Alternate, Open</i>).	IP Core	Configuration
operStatus	The current operational link state of the REP port (<i>None, Init Down, No Neighbor, One Way, Two Way, Flapping, Wait, Unknown</i>).	IP Core	Configuration
blockedVlans	The list of VLANs configured to be blocked at the alternate port. This value is only effective on the alternate port (i.e. if the portRole value is <i>alternate</i>). Formats are: <i>800-850,1050-1200,2900-2999,3555</i> .	IP Core	Configuration
preemptTimer	Specifies the time interval that REP waits before triggering preemption after the segment is complete (an integer from 0 to 300, or <i>Disabled</i>) <i>Disabled</i> indicates that no time delay is configured and the preemption will happen manually. This value is only effective on the device acting as the REP primary edge.	IP Core	Configuration
lslAgeoutTimer	The link status layer age-out timer; that is, the time, in milliseconds, for which the REP interface remains up without receiving a hello from a neighbor.	IP Core	Configuration
remoteDeviceName	The name of the neighbor device on the segment to which this port is connected (may be null).	IP Core	Configuration
remoteDeviceMac	The MAC address of the neighbor bridge on the segment to which this port is connected (may be null).	IP Core	Configuration
remotePortName	The name of the neighbor port on the neighbor bridge on the segment to which this port is connected (may be null)	IP Core	Configuration

Network Topology

Cisco ANA conducts discovery of Ethernet data link layer topology by using various types of data. This includes information from 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.

Connections between CDP and LLDP ports are straightforward, as they expose neighbor information.

For STP topology, the STP port information is used in the following way: The Bridge ID, Designated Bridge, and Port identifier are compared with the relevant remote information. If a match is found, a link is created.

MAC-based topology is traced by searching for the local MAC address on any remote side's bridge or in ARP tables related to the same type of the local Ethernet port. The basic assumption, which is not always valid, is that every Ethernet port has a unique MAC address. This topology is also applied to the underlying physical links.

Verification is done based on STP, CDP, and LLDP. Further verification is preformed by matching the traffic signature of these ports using Cisco's confidential scheme, which requires a substantial amount of network traffic to function correctly.

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. Users can overcome this problem by configuring static links on these ports. These static links will override any incorrect dynamically discovered links.

Service Alarms

The following alarms are supported for this technology:

- [Cloud Problem, page 41-22](#)
- [Discard Packets, page 41-26](#)
- [Dropped Packets, page 41-27](#)
- [Link Down, page 41-42](#)
- [Port Down, page 41-51](#)
- [Rx Utilization, page 41-53](#)
- [Tx Utilization, page 41-57](#)
- [VSI Down, page 41-57](#)
- [EFP Down, page 41-32](#)
- [Subinterface Down, page 41-55](#)

Note that these alarms, apart from Cloud Problem, are related to the underlying physical interface (see [Common Components](#)).

Cisco ANA does not generate service alarms specific to QinQ technology. However, correlation takes this technology into account when performing flow analysis.



CHAPTER 19

Ethernet OAM

This chapter describes the level of support that Cisco ANA provides for Ethernet Operations, Administration, and Management (OAM), as follows:

- [Technology Description, page 19-1](#)
- [Information Model Objects \(IMOs\), page 19-2](#)
- [Vendor-Specific Inventory and IMOs, page 19-11](#)
- [Network Topology, page 19-11](#)
- [Service Alarms, page 19-11](#)

Technology Description

This section provides the following Ethernet OAM technology descriptions:

- [CFM](#)
- [Link OAM](#)
- [Ethernet LMI](#)

Please see Part 1: Cisco VNEs in this guide for information about which devices support the various technologies.

CFM

Ethernet Connectivity Fault Management (CFM) is an end-to-end, per-service-instance Ethernet layer operations, administration, and maintenance (OAM) protocol. It includes proactive connectivity monitoring, fault verification, and fault isolation for large Ethernet MANs and WANs. “End-to-end” can mean PE-to-PE or CE-to-CE. A service can be identified as a service provider VLAN (S-VLAN) or an Ethernet Virtual Connection (EVC) service. Cisco ANA supports both

Cisco Proprietary Draft 1 (CFM D1) and Ethernet CFM IEEE 802.1ag Standard, using a common IMO model.

Link OAM

Link OAM allows network operators to monitor and troubleshoot a single Ethernet link. It is an optional sublayer implemented in the Data Link Layer between the Logical Link Control (LLC) and MAC sublayers of the Open Systems Interconnect (OSI) model. You can monitor a link for critical events and, if needed, put a remote device into loopback mode for link testing. Link OAM also discovers unidirectional links, which are created when one transmission direction fails.

OAM information is conveyed in Slow Protocol frames (see Annex 57A) called OAM Protocol Data Units (OAMPDUs). OAMPDUs contain the appropriate control and status information used to monitor, test and troubleshoot OAM-enabled links. OAMPDUs traverse a single link, being passed between peer OAM entities, and as such, are not forwarded by MAC clients (e.g., bridges or switches).

Ethernet LMI

Ethernet Local Management Interface (Ethernet LMI) is a protocol that runs on the Provider Edge (PE) to Customer Edge (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.

Ethernet LMI provides information that enables autoconfiguration of customer edge (CE) devices and provides the status of Ethernet virtual connections (EVCs) for large Ethernet metropolitan-area networks (MANs) and WANs. Specifically, Ethernet LMI notifies a CE device of the operating state of an EVC and the time when an EVC is added or deleted. Ethernet LMI also communicates the attributes of an EVC and a user-network interface (UNI) to a CE device.

Information Model Objects (IMOs)

This section describes the following IMOs:

- [CFM Service \(ICfmService\)](#)
- [CFM Maintenance Domain \(IMaintenanceDomain\)](#)
- [CFM Maintenance Point \(IMaintenancePoint\)](#)
- [CFM Maintenance Endpoints \(IMaintenanceEndPoints\)](#)
- [CFM Maintenance Association \(IMaintenanceAssociation\)](#)
- [CFM Maintenance Intermediate Point \(IMaintenanceIntermediatePoint\)](#)
- [OAM Data \(IOAMData\)](#)
- [OAM Remote Data \(IOAMRemoteData\)](#)
- [UNI Properties \(IUNIProperties\)](#)
- [Ethernet LMI \(IEthernetLMI\)](#)
- [Device EVC \(IDeviceEVC\)](#)
- [UNI Interfaces \(IUNIInterfaces\)](#)
- [ELMI Interfaces \(IELMIInterfaces\)](#)

CFM Service

The [CFM Service](#) object represents an instance of CFM enabled on a device.

Table 19-1 *CFM Service (ICfmService)*

Attribute Name	Attribute Description	Scheme	Polling Interval
cacheSize	The CFM traceroute cache size used by the CFM service.	IP Core, Product	Configuration
maximumCacheSize	The CFM traceroute maximum cache size used by the CFM service.	IP Core, Product	Configuration
holdTime	The configured hold-time value used to indicate to the receiver the validity of traceroute and loopback messages transmitted by this device. The default is 2.5 times the transmit interval.	IP Core, Product	Configuration
version	The CFM version running on the device.	IP Core, Product	Configuration
maintenanceIntermediatePointsTable	An array of all the CFM Maintenance Intermediate Point objects configured on the device.	IP Core, Product	Configuration
maintenanceDomain	The CFM Maintenance Domain configured on the device.	IP Core, Product	Configuration

CFM Maintenance Domain

The [CFM Maintenance Domain](#) object represents an instance of a CFM management space used to manage and administer a network. A CFM management domain is owned and operated by a single entity and defined by the set of ports internal to it and at its boundary.

Table 19-2 *CFM Maintenance Domain (IMaintenanceDomain)*

Attribute Name	Attribute Description	Scheme	Polling Interval
name	The name of the management domain. This must be unique and cannot be used within a different maintenance level.	IP Core, Product	Configuration
level	The domain level (an integer in the range 0 to 7). Domain levels permit creation of a domain hierarchy. The larger the level value, the larger the domain. For instance, the customer domain will have a level of 7, and the operator domain will have a level of 0.	IP Core, Product	Configuration
Id	The domain ID. Optional and may not be defined. When undefined, the domain name is used as the default value.	IP Core, Product	Configuration
maintenanceAssociation	A list of the domain's CFM Maintenance Associations . These are the associations represented by the service. In Cisco devices, the domain is mapped to a VLAN.	IP Core, Product	Configuration

CFM Maintenance Point

The [CFM Maintenance Point](#) object represents an instance of a CFM maintenance point configured on one or more of a device's interfaces.

Table 19-3 *CFM Maintenance Point (IMaintenancePoint)*

Attribute Name	Attribute Description	Scheme	Polling Interval
macAddress	The MAC address on the interface on which the maintenance point is configured. In different interface modes, the MAC address may hold different values. For example, an inward facing interface uses the Bridge-Brain MAC address; an outward facing interface, such as a routed port, uses the port MAC address; and outward facing MEPs on port channels use the Bridge-Brain MAC address of the first member link. When port channel members change, the identities of outward facing MEPs do not have to change.	IP Core, Product	Configuration
Interface	A link to the interface on which the maintenance point is configured. This property includes all interface types that can be configured with CFM maintenance points.	IP Core, Product	Configuration

CFM Maintenance Endpoint

The [CFM Maintenance Endpoint](#) object represents an instance of a CFM Maintenance Endpoint (MEP). Unlike MIPs, MEPs are associated by a [CFM Maintenance Association](#) (S-VLAN).

Table 19-4 *CFM Maintenance Endpoints (IMaintenanceEndPoints)*

Attribute Name	Attribute Description	Scheme	Polling Interval
Id	The ID of the MEP (an integer from 1 and 8191). It identifies the MEP in CFM communications and to catalog CFM frames in the local CFM database. The MEP ID is meaningful throughout the CFM domain and through the maintenance association.	IP Core, Product	Configuration
Continuity Check Status	Current MEP status sent to other MEPs and MIPs via multicast CCMs (<i>Unknown, MEP active, MEP inactive, MEP enabled, MEP disabled</i>). CCMs are confined to a domain and S-VLAN.	IP Core, Product	Configuration
direction	Direction of the MEP (<i>inward facing, outward facing</i>). Inward facing means the MEP communicates through the Bridge Relay function and uses the Bridge-Brain MAC address. Outward facing means that the MEP communicates through the wire. Outward facing MEPs can be configured on routed ports and switch ports. A MIP configuration at a level higher than the level of the outward facing MEP is not required.	IP Core, Product	Configuration
cfmRemoteMaintenanceEndPoints	An array listing all the remote CFM MEPs that were discovered through this MEP. Properties for each remote MEP are used to establish CFM topology between CFM MEPs.	IP Core, Product	Configuration

CFM Maintenance Association

The [CFM Maintenance Association](#) object models a grouping of [CFM Maintenance Endpoint](#).

Table 19-5 *CFM Maintenance Association (IMaintenanceAssociation)*

Attribute Name	Attribute Description	Scheme	Polling Interval
name	The Association name.	IP Core, Product	Configuration
associationType	The Association type (<i>Unknown, Bridge Domain VLAN, Bridge Domain, Port, Pseudowire</i>).	IP Core, Product	Configuration
maximalMeps	The maximum number of MEPs that can be configured on the Maintenance Association.	IP Core, Product	Configuration
continuityCheckInterval	The configured time interval between continuity checks performed by the Maintenance Association's MEPs.	IP Core, Product	Configuration

Table 19-5 CFM Maintenance Association (IMaintenanceAssociation) (continued)

Attribute Name	Attribute Description	Scheme	Polling Interval
continuityCheckEnable	Indicates whether continuity checking is enabled for the Association. CFM continuity checks are periodic heartbeat messages exchanged between the MEPs under the association. They allow MEPs to discover each other and CFM Maintenance Intermediate Points to discover the MEPs.	IP Core, Product	Configuration
crossCheckEnable	Indicates whether cross-checking is enabled for the Association. CFM cross-checking verifies that all endpoints of a service are operational. It is timer-driven and performed once.	IP Core, Product	Configuration
Direction	The direction of the association (<i>up</i> , <i>down</i> , <i>unknown</i>).	IP Core, Product	Configuration
Inner VLAN	The inner or customer VLAN ID.	IP Core, Product	Configuration
MaximalMeps	Maximum number of maintenance endpoints that can be configured on the maintenance association.	IP Core, Product	Configuration
bridge	Object Identifier of the bridge on which the association (VLAN) is configured.	IP Core, Product	Configuration
maintenanceEndPoints	An array of the CFM Maintenance Endpoint configured within the bounds of the CFM Maintenance Domain .	IP Core, Product	Configuration
RemoteMaintenanceEndPoints	Remote MEPs configured on other CFM-configured devices in the network. Each MEP can communicate with several remote MEPs.	IP Core, Product	Configuration

CFM Maintenance Intermediate Point

The [CFM Maintenance Intermediate Point](#) object represents a single instance of a CFM Maintenance Intermediate Point (MIP). Unlike MEPs, MIPs are not grouped by [CFM Maintenance Associations](#) (S-VLAN). Instead, they are grouped by [CFM Maintenance Domain](#) (using the Level parameter) and for all S-VLANs enabled or allowed on a port.

Table 19-6 CFM Maintenance Intermediate Point (IMaintenanceIntermediatePoint)

Attribute Name	Attribute Description	Scheme	Polling Interval
level	The level defined for this MIP. This is the same as the Level parameter defined for CFM Maintenance Domains : An integer from 0 to 7, assigned to each MIP for the purpose of creating hierarchical relationships among MIPs. All CFM frames at a level lower than the level assigned to the MIP are stopped and dropped, independent of whether they originate from the wire or relay function. All CFM frames at a higher level than the MIP are forwarded, independent of whether they arrive from the wire or relay function.	IP Core, Product	Configuration
cfmInterface	The normalized name of the interface on which the MIP is configured.	IP Core, Product	Configuration
isAutocreated	Indicates whether this MIP was created automatically (<i>true</i>) or by entering properties manually using the command-line interface (CLI) (<i>false</i>).	IP Core, Product	Configuration

Table 19-6 *CFM Maintenance Intermediate Point (IMaintenanceIntermediatePoint) (continued)*

Attribute Name	Attribute Description	Scheme	Polling Interval
Vlans	A list of the VLANs in which this MIP participates. A MIP configured on an interface normally functions via maintenance domain (level) and for all S-VLANs enabled or allowed on that port. To limit its functionality, however, a CFM MIP can also be configured with a list of S-VLANs or associations.	IP Core, Product	Configuration
InnerVlans	A list of the inner VLANs in which this MIP participates. A CFM maintenance intermediate point configured on an interface functions per maintenance domain (level) and for all inner VLANs enabled or allowed on a port.	IP Core, Product	Configuration
macAddress	The MAC address that identifies the CFM entity (for example, <i>bridge-brain MAC</i>).	IP Core, Product	Configuration

OAM Data

The [OAM Data](#) object represents support and status of OAM functions on Ethernet-like interfaces.

Table 19-7 *OAM Data (IOAMData)*

Attribute Name	Attribute Description	Scheme	Polling Interval
Admin Status	Used to enable and disable the OAM sublayer entity.	IP Core, Product	Configuration
Maximum PDU Rate	The maximum transmission and reception rate of OAM PDUs as part of the discovery process (packets per second).	IP Core, Product	Configuration
Minimum PDU Rate	The minimum transmission and reception rate of OAM PDUs as part of the discovery process (packets per second).	IP Core, Product	Configuration
Link Timeout	The time (in seconds) after which a device declares the OAM peer to be non-operational and resets its state machine.	IP Core, Product	Configuration
High Threshold Action	The action to be taken when a monitored error has been detected to have crossed a user-specified threshold.	IP Core, Product	Configuration
Link Fault Action	The action to be taken when loss of signal (link fault) is detected.	IP Core, Product	Configuration
Dying Gasp Action	Used to indicate unrecoverable event conditions that should be transmitted to the peer OAM entity.	IP Core, Product	Configuration
Critical Event Action	Used to signal an unspecified critical link event condition.	IP Core, Product	Configuration
Mode	The local client OAM sublayer entity configuration status, either active or passive controlling of the peer's OAM configurations.	IP Core, Product	Configuration
Unidirectional	Indicates whether the OAM local entity supports the transmission of OAMPDUs on links that are operating in unidirectional mode.	IP Core, Product	Configuration
Link Monitor	Indicates whether a mechanism is provided to support event notification that permits the inclusion of diagnostic information.	IP Core, Product	Configuration

Table 19-7 OAM Data (IOAMData) (continued)

Attribute Name	Attribute Description	Scheme	Polling Interval
Remote Loopback	Indicates whether data link layer frame-level loopback mode is supported.	IP Core, Product	Configuration
Port Status	The operational status of the local port.	IP Core, Product	Configuration
Loopback Status	Indicates the Ethernet OAM loopback status of this interface (no loopback, remote loopback, initiating loopback, terminating loopback, local loopback, unknown.)	IP Core, Product	Configuration
Remote Data	OAM provides a mechanism to detect the presence of an OAM sublayer at the remote DTE.	IP Core, Product	Configuration
Ethernet Port	OID of the Ethernet Port	IP Core, Product	Configuration

OAM Remote Data

The [OAM Remote Data](#) object consists of interface remote peer summarized OAM data.

Table 19-8 OAM Remote Data (IOAMRemoteData)

Attribute Name	Attribute Description	Scheme	Polling Interval
MAC Address	The MAC address of the remote client.	IP Core, Product	Configuration
Vendor	The vendor name of the remote client.	IP Core, Product	Configuration
Mode	The remote client OAM sublayer entity configuration status, either active or passive controlling of the peer's OAM configurations.	IP Core, Product	Configuration
Unidirectional	Indicates whether the remote OAM entity supports the transmission of OAMPDUs on links that are operating in unidirectional mode	IP Core, Product	Configuration
Link Monitor	Indicates whether a mechanism is provided to support event notification that permits the inclusion of diagnostic information.	IP Core, Product	Configuration
Remote Loopback	Indicates whether data link layer frame-level loopback mode is supported.	IP Core, Product	Configuration

Ethernet LMI

The [Ethernet LMI](#) object contains the properties that control the Ethernet LMI protocol between the customer edge (CE) network element and the provider edge (PE) network element, on the PE-CE UNI link. It 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. Such a service will exist once per context and per device. It contains [ELMI Interfaces \(IELMIInterfaces\)](#) and [Device EVC \(IDeviceEVC\)](#).

Table 19-9 Ethernet LMI (IEthernetLMI)

Attribute Name	Attribute Description	Scheme	Polling Interval
ELMI Enabled State	Indicates whether or not the Ethernet LMI protocol is enabled on the interface.	IP Core, Product	Configuration
ELMI Mode	The Ethernet LMI mode, either CE or PE.	IP Core, Product	Configuration
ELMI Interfaces	The interfaces on which Ethernet LMI is configured.	IP Core, Product	Configuration
Device EVCs	The Ethernet Virtual Connections configured on the device.	IP Core, Product	Configuration

Device EVC

The [Device EVC](#) object represents a port-level point-to-point or multipoint-to-multipoint Layer 2 circuit. It is an end-to-end representation of a single instance of a Layer 2 service being offered by a provider to a customer. It embodies the different parameters on which the service is being offered. A service instance is the instantiation of an EVC on a given port on a given router.

Table 19-10 Device EVC (IDeviceEVC)

Attribute Name	Attribute Description	Scheme	Polling Interval
EVC Name	The name of the EVC.	IP Core, Product	Configuration
EVC Status	The status of the EVC (<i>Active, Partially Active, Inactive</i>). The EVC status can be used by a customer edge (CE) device either to find an alternative path in to the service provider network or, in some cases, to revert to a backup path over Ethernet or over another alternative service such as Frame Relay or ATM.	IP Core, Product	Status
EVC Type	The type of EVC (<i>Point-to-point, Multipoint-to-Multipoint</i>).	IP Core, Product	Configuration
Maintenance Association	The CFM Maintenance Association which uniquely identifies a service profile within the Maintenance Domain.	IP Core, Product	Configuration
Configured Remote UNI Count	The number of configured remote UNIs.	IP Core, Product	Configuration
Active Remote UNI Count	The number of active remote UNIs.	IP Core, Product	Configuration
UNI Interfaces	The UNI interfaces configured for Ethernet LMI.	IP Core, Product	Configuration

UNI Properties

The [UNI Properties](#) object holds the properties for the user-network interface (UNI). This IMO is mapped to the UniProperties in maps.xml.

Table 19-11 *UNI Properties (IUNIProperties)*

Attribute Name	Attribute Description	Scheme	Polling Interval
UNI ID	The ID of the local user-network interface (UNI).	IP Core, Product	Configuration
Service Multiplexing Enabled	Returns a boolean value (true or false), to indicate whether service multiplexing is enabled. If more than one EVC is allowed, service multiplexing can be enabled (true).	IP Core, Product	Configuration
Bundling Enabled	Returns a boolean value (true or false) to indicate whether bundling is enabled. This is set as true when configuring the UNI by supporting only one EVC with one or more VLANs.	IP Core, Product	Configuration
Bundling Type	The Bundling service attribute enables two or more VLAN IDs to be mapped to a single EVC at a UNI. With bundling, the provider and subscriber must agree on the VLAN IDs used at the UNI and the mapping between each VLAN ID and a specific EVC. A special case of bundling is where every VLAN ID at the UNI interface maps to a single EVC. This service attribute is called all-to-one bundling.	IP Core, Product	Configuration

UNI Interfaces

The [UNI Interfaces](#) object represents the identity and the status of the UNI interfaces configured for Ethernet LMI.

Table 19-12 *UNI Interfaces (IUNIInterfaces)*

Attribute Name	Attribute Description	Scheme	Polling Interval
UNI Status	The status of the UNI interface (<i>up</i> , <i>down</i>).	IP Core, Product	Status
UNI ID	The ID of the UNI.	IP Core, Product	Configuration
Interface Name	The name of the UNI.	IP Core, Product	Configuration
VLAN List	List of VLANs configured on the interface.	IP Core, Product	Configuration
LMI Link Status	The status of the LMI link (<i>up</i> , <i>down</i>).	IP Core, Product	Status
Interface OID	OID of the UNI.	N/A	N/A
Is UNI Local	Boolean UNI location, either local or remote.	IP Core, Product	Configuration

ELMI Interfaces

The [ELMI Interfaces](#) object holds the timers and counters used to assess and notify the CE of connectivity status and configuration parameters of Ethernet services available on the CE port.

Table 19-13 *ELMI Interfaces (IELMIInterfaces)*

Attribute Name	Attribute Description	Scheme	Polling Interval
Interface Name	The name of the Ethernet LMI interface.	IP Core, Product	Configuration
Interface OID	The OID of the Ethernet LMI interface.	N/A	N/A
T391	Polling timer on the customer equipment. A polling timer sends status inquiries and records errors when status messages are not received. The range is from 5 to 30 seconds; the default is 10 seconds.	IP Core, Product	Configuration
T392	Polling verification timer for the metro Ethernet network or the timer to verify received status inquiries. The range is from 5 to 30 seconds, or 0 for disabled timer. The default is 15 seconds.	IP Core, Product	Configuration
N391	Event counter on the customer equipment. The counter polls the status of the UNI and all Ethernet virtual connections (EVCs). The range is from 1 to 65000; the default is 360.	IP Core, Product	Configuration
N393	Event counter for the metro Ethernet network. The range is from 1 to 10; the default is 4.	IP Core, Product	Configuration

Vendor-Specific Inventory and IMOs

There are no vendor-specific IMOs for this technology.

Network Topology

Please see [Chapter 38, “Cisco ANA VNE Topology”](#). There is no topology support for CFM.

Service Alarms

The following alarms are supported for this technology:

- [CFM Domain Fault, page 41-15](#)



CHAPTER 20

Asynchronous Transfer Mode

This chapter describes the level of support that Cisco ANA provides for ATM, as follows:

- [Technology Description, page 20-1](#)
- [Information Model Objects \(IMOs\), page 20-3](#)
- [Vendor-Specific Inventory and IMOs, page 20-9](#)
- [Network Topology, page 20-14](#)
- [Service Alarms, page 20-14](#)

Technology Description

This section provides the following ATM technology descriptions:

- [ATM](#)
- [IMA](#)
- [IP over ATM, Ethernet over ATM \(MPoA\)](#)
- [ATM Cross Connect](#)

Please see Part 1: Cisco VNEs in this guide for information about which devices support the various technologies.

ATM

ATM is a cell-switching and multiplexing technology that combines the benefits of circuit switching (guaranteed capacity and constant transmission delay) with those of packet switching (flexibility and efficiency for intermittent traffic). It provides data link (Layer 2) services with scalable bandwidth from a few megabits per second (Mb/s) to many gigabits per second (Gb/s), which usually run over SONET/SDH physical (Layer 1) links.

ATM networks consist of ATM switches interconnected by point-to-point ATM links or interfaces and are fundamentally connection oriented, which means that a virtual channel (VC) must be set up across the ATM network prior to any data transfer.

IMA

Inverse Multiplexing over ATM (IMA) involves inverse multiplexing and demultiplexing of ATM cells in a cyclical fashion among physical links grouped to form a higher bandwidth and logical link. The rate of the logical link is approximately the sum of the rate of the physical links in the IMA group. Streams of cells are distributed in a round-robin manner across the multiple T1/E1 links and reassembled at the destination to form the original cell stream. Sequencing is provided using IMA Control Protocol (ICP) cells.

The ATM cell stream received from the ATM layer is distributed on a cell-by-cell basis across the multiple links within the IMA group. At the far end, the receiving IMA unit reassembles the cells from each link on a cell-by-cell basis, recreates the original ATM cell stream, and passes it to the ATM layer.

IP over ATM, Ethernet over ATM (MPoA)

IP over ATM (MPoA 1483R) and Ethernet over ATM (MPoA 1483B) are both implementations of Multi protocol over ATM (MPoA), an ATM Forum standard that provides for routing of legacy protocols (such as IP and Ethernet) over ATM networks.

Based on ATM UNI signaling, and integrating LANE and Next Hop Resolution Protocol (NHRP), MPoA preserves the benefits of LANE while allowing intersubnet, internetwork layer protocol communication over virtual channel connections (VCCs). Unlike LANE, it requires no routers in the data path. MPoA provides a framework for effectively synthesizing bridging and routing with ATM in an environment of diverse protocols, network technologies, and IEEE 802.1 VLANs. MPoA can use routing and bridging information to locate optimal exits from the ATM cloud and allows the physical separation of internetwork layer route calculation and forwarding (virtual routing).

MPoA defines two components—MPoA Clients (MPCs) and MPoA Servers (MPSS)—and the protocols that are required to communicate and receive services. An MPS is a router component, and requires a Next Hop Server (NHS) and interfaces to one or more LAN Emulation Clients (LECs). This MPS route server performs the routing calculations and sends its results to the ATM switches and edge devices, which perform high-speed forwarding of IP datagrams and Ethernet packets.

ATM Cross Connect

ATM networks are based on virtual connections over a high-bandwidth medium. By using cross-connects to interconnect virtual path or virtual channel links, it is possible to build an end-to-end virtual connection.

An ATM cross-connect can be mapped at either of the following levels:

- Virtual path—Cross-connecting two virtual paths maps one Virtual Path Identifier (VPI) on one port to another VPI on the same port or a different port.
- Virtual channel—Cross-connecting at the virtual channel level maps a Virtual Channel Identifier (VCI) of one virtual channel to another VCI on the same virtual path or a different virtual path.

Cross-connect tables translate the VPI and VCI connection identifiers in incoming ATM cells to the VPI and VCI combinations in outgoing ATM cells.

Information Model Objects (IMOs)

This section describes the following IMOs:

- [ATM Interface \(IAtm\)](#)
- [ATM Virtual Connection \(IAtmVc\)](#)
- [Inverse Multiplexing for ATM \(IMA\) Group \(IIMAGroup\)](#)
- [ATM Traffic Descriptor \(IAtmTrafficDescriptor\)](#)
- [ATM Traffic Shape Descriptor \(IAtmTrafficShapingDescriptor\)](#)
- [Virtual Connection Switching Entity \(IVcSwitchingEntity\)](#)

ATM Interface

The data link layer [ATM Interface](#) object aggregates multiple [ATM Virtual Connections](#) by its VC Table attributes. It is bound by its Containing Termination Points attribute to a physical layer interface. It is accessed primarily by the [VC Encapsulation](#) Multiplexer bound by its Contained Connection Termination Points attribute.

Table 20-1 *ATM Interface (IAtm)*

Attribute Name	Attribute Description	Scheme	Polling Interval
ATM Address	ATM 20-byte address (<i>Address Prefix MAC Address Address Selector</i>)	Any	Configuration
Interface Type	ATM interface type (<i>N/A, UNI, Private UNI, Public UNI, NNI, Private NNI, Public NNI, STI, Unconfigured, VNNI, VUNI, EVNNI, EVUNI, VP TRUNK UNI</i>)	Any	Configuration
VP and VC Ranges	Numeric ranges of the allowed Virtual Path Identifier/Virtual Channel Identifier (VPI/VCI) values	Any	Configuration
VC Table	Array of ATM Virtual Connections	Any	Configuration
Cross Connect Table	Array of Virtual Cross Connections	Any	Configuration
IANA Type	Internet Assigned Numbers Authority (IANA) type of the sublayer	N/A	N/A
Containing Termination Points	Underlying termination points (connection or physical)	Any	N/A
Contained Connection Termination Points	Bound connection termination points	Any	N/A
Tx Allocated Bandwidth	ATM allocated transmit bandwidth	Product	Configuration
Tx Maximum Bandwidth	ATM maximum transmit bandwidth	Product	Configuration
Tx UBR Allocated Bandwidth	ATM allocated transmit bandwidth at unspecified bit rate	Product	Configuration
Tx CBR Allocated Bandwidth	ATM allocated transmit bandwidth at constant bit rate	Product	Configuration
Rx Allocated Bandwidth	ATM allocated receive bandwidth	Product	Configuration
Rx Maximum Bandwidth	ATM maximum transmit bandwidth	Product	Configuration
Rx UBR Allocated Bandwidth	ATM allocated transmit bandwidth at unspecified bit rate	Product	Configuration
Rx CBR Allocated Bandwidth	ATM allocated transmit bandwidth at constant bit rate	Product	Configuration

ATM Virtual Connection

The data link layer [ATM Virtual Connection](#) object is bound by its Containing Termination Points attribute to a data link layer [ATM Interface](#) object. It is accessed primarily by the [Virtual Cross Connection](#) and data link layer [VC Encapsulation](#), but is not bound to any of them by any of its attributes.

Table 20-2 **ATM Virtual Connection (IAtmVc)**

Attribute Name	Attribute Description	Scheme	Polling Interval
Virtual Channel Identifier	Virtual Channel Identifier (VCI)	Any	Configuration
Virtual Path Identifier	Virtual Path Identifier (VPI)	Any	Configuration
Shaping Profile	Shaping profile (ATM Traffic Shape Descriptor)	Any	Configuration
Discarded and Received Input Data Counters	Discarded and received input octets and reassembled packet counters	Any	Topology L2
Dropped and Forward Output Data Counters	Dropped and forwarded output octets and reassembled packet counters	Any	Topology L2
Ingress Traffic Descriptor	Ingress traffic descriptor (ATM Traffic Descriptor)	Any	Configuration
Egress Traffic Descriptor	Egress traffic descriptor (ATM Traffic Descriptor)	Any	Configuration
Administrative Status	Administrative status (<i>Unknown, Up, Down</i>)	Any	Status
Operational Status	Operational status (<i>Unknown, Up, Down</i>)	Any	Status
IANA Type	Internet Assigned Numbers Authority (IANA) type of the sublayer	N/A	N/A
Containing Termination Points	Underlying termination points (connection or physical)	Any	N/A
Contained Connection Termination Points	Bound connection termination points	Any	N/A

Inverse Multiplexing for ATM (IMA) Group

The [Inverse Multiplexing for ATM \(IMA\) Group](#) object is bound to its multiple [DS1 Physicals](#) by its Containing Termination Points attribute. It is accessed by a single data link layer [ATM Interface](#).

Table 20-3 *Inverse Multiplexing for ATM (IMA) Group (IIMAGroup)*

Attribute Name	Attribute Description	Scheme	Polling Interval
Administrative Status	Administrative status of the IMA Group interface (<i>Unknown, Up, Down, Testing</i>).	Any	Status
Operational Status	Operational status of the IMA Group interface (<i>Unknown, Up, Down, Testing, Dormant, Not Present</i>).	Any	Status
Group Number	The IMA Group number.	Any	Configuration
IMA Version	The configured IMA version (<i>1.0, 1.1</i>).	Any	Configuration
Speed	The active bandwidth of the IMA Group.	Any	Configuration
Configured Bandwidth	The total bandwidth of the IMA Group (the sum of all individual links in the Group).	Any	Configuration
Number of Links	The number of DS1 links in the IMA Group.	Any	Configuration
Number of Active Links	The number of DS1 links active in the IMA Group.	Any	Configuration
Minimum Number of Transmit Links	The minimum number of transmit links needed for the IMA Group to be operational.	Any	Configuration
Minimum Number of Receive Links	The minimum number of receive links needed for the IMA Group to be operational.	Any	Configuration
Clock Mode	The IMA Group's clock mode (<i>CTC, ITC</i>).	Any	Configuration
Frame Length	The length of IMA frames.	Any	Configuration
Group Failure Status	Reason for the IMA Group failure (<i>noFailure, startup, invalidMValueNe, invalidMValueFe, failedAssymmetricNe, failedAssymmetricFe, insufficientLinksFe, insufficientLinksMe, blockedNe, blockedFe, invalidImaVersionNe, invalidImaVersionFe, otherFailure</i>).	Any	Configuration
Operational Status Last Change	Date of last operational status change.	Any	Configuration
Description	The IMA Group interface name (for example, <i>ATM8/0/IMA1</i>).	Any	Configuration
IANA Type	Internet Assigned Numbers Authority (IANA) type of the sublayer.	N/A	N/A
Containing Termination Points	Underlying termination points (DS1 Physicals).	Any	N/A

ATM Traffic Descriptor

The [ATM Traffic Descriptor](#) object describes the traffic of a single [ATM Virtual Connection](#). It is aggregated by a [Traffic Descriptor Container](#) object (see [Common Components](#)).

Table 20-4 *ATM Traffic Descriptor (IAtmTrafficDescriptor)*

Attribute Name	Attribute Description	Scheme	Polling Interval
Traffic Descriptor Type	ATM traffic descriptor type (<i>Null, Best Effort, No CLP and no SCR, CLP with no tagging and no SCR, CLP with tagging and no SCR, No CLP with SCR, CLP with no tagging and with SCR, CLP with tagging and with SCR, CLP with no tagging and with MCR, CLP-transparent with no SCR, CLP-transparent with SCR, No CLP with tagging and no SCR, No CLP and no SCR with CDVT, No CLP with SCR and CDVT, No CLP and no SCR with CDVT, No CLP with SCR and CDVT</i>)	Any	Configuration
Service Category	ATM service category (<i>Unknown, UBR, UBR1, UBR2, CBR, CBR1, CBR2, CBR3, ABR, VBR, RT VBR, NRT VBR, VBR1RT, VBR2RT, VBR3RT, VBR1NRT, VBR2NRT, VBR3NRT, GFR</i>)	Any	Configuration
Cell Loss Priority	Cell loss priority (<i>Unknown, True, False</i>)	Any	Configuration
Cell Delay Variation	Cell delay variation	Any	Configuration
Cell Delay Variation Tolerance	Cell delay variation tolerance	Any	Configuration
Maximum High Priority and Aggregate Burst Sizes	Maximum high priority and aggregate (CLP=0 and CLP=0+1) burst sizes	Any	Configuration
Minimum High Priority and Aggregate Cell Rates	Minimum high priority and aggregate (CLP=0 and CLP=0+1) cell rates	Any	Configuration
Sustainable High Priority and Aggregate Cell Rates	Sustainable high priority and aggregate (CLP=0 and CLP=0+1) cell rates	Any	Configuration
Peak High Priority and Aggregate Cell Rates	Peak high priority and aggregate (CLP=0 and CLP=0+1) cell rates	Any	Configuration
Name	Traffic descriptor name	Any	Configuration
Index	Traffic descriptor index	Any	Configuration

ATM Traffic Shape Descriptor

The [ATM Traffic Shape Descriptor](#) object describes the traffic shape of a single [ATM Virtual Connection](#). It is aggregated by a [Traffic Descriptor Container](#) object (see [Common Components](#)).

Table 20-5 *ATM Traffic Shape Descriptor (IAtmTrafficShapingDescriptor)*

Attribute Name	Attribute Description	Scheme	Polling Interval
Maximum Burst Size	Maximum burst sizes	Any	Configuration
Sustainable and Peak Cell Rates	Sustainable and peak cell rates	Any	Configuration
Cell Delay Variation	Cell delay variation	Any	Configuration
State	Descriptor state (<i>Null, Enabled, Disabled</i>)	Any	Configuration
Buffer Size	Buffer size	Any	Configuration
Cell Loss Priority Discarded Size	Cell loss priority discarded size	Any	Configuration
Name	Traffic descriptor name	Any	Configuration
Index	Traffic descriptor index	Any	Configuration

Virtual Connection Switching Entity

The [Virtual Connection Switching Entity](#) object describes the standard forwarding component of an ATM or Frame Relay Switch. It is bound by its Logical Sons attribute to all the data link layer objects (such as [ATM Interfaces](#) or [Frame Relay Interfaces](#)) for which this [Virtual Connection Switching Entity](#) is switching cells or frames.

Table 20-6 *Virtual Connection Switching Entity (IVcSwitchingEntity)*

Attribute Name	Attribute Description	Scheme	Polling Interval
Cross Connect Table	Array of virtual cross connections.	Any	Configuration
Cross Connect Table Size	Size of the cross-connect table.	Any	Configuration
Logical Sons	Array of all ATM Interfaces or Frame Relay Interfaces for which this Virtual Connection Switching Entity is switching cells or frames.	Any	N/A

Vendor-Specific Inventory and IMOs

Vendor-specific IMOs are implemented only for specific vendor devices. The following sections describe vendor-specific objects for this technology:

- [Lucent ATM Trunk Interface](#)
- [Cisco or Lucent ATM Logical Interface](#)
- [Cisco or Lucent ATM Trunk Virtual Connection](#)
- [Cisco or Lucent ATM Soft Permanent Virtual Connection](#)
- [Alcatel ASAM ATM Interface](#)
- [ECI HiFocus ATM Interface](#)
- [Alcatel ASAM ATM Traffic Descriptor](#)
- [ECI HiFocus ATM Traffic Descriptor](#)
- [Lucent WAN Switch ATM Traffic Descriptor](#)
- [Alcatel ATM Access Traffic Descriptor](#)
- [Alcatel ASAM Access Traffic Descriptor](#)

Lucent ATM Trunk Interface

The [Lucent ATM Trunk Interface](#) data link layer object aggregates multiple [ATM Virtual Connections](#), to which it is bound by its VC Table attributes. It is bound by its Containing Termination Points attribute to a physical layer interface. It is accessed primarily by a [Virtual Connection Switching Entity](#).

Table 20-7 *Lucent ATM Trunk Interface (IAtmTrunk)*

Attribute Name	Attribute Description	Scheme	Polling Interval
All attributes are the same as ATM Interface (IAtm)			

Cisco or Lucent ATM Logical Interface

The [Cisco or Lucent ATM Logical Interface](#) data link layer object aggregates multiple [ATM Virtual Connections](#), to which it is bound by its VC Table attributes. It is bound by its Containing Termination Points attribute to a physical layer interface. It is accessed primarily by a [Virtual Connection Switching Entity](#) and data link layer [VC Encapsulation](#) bound by its Contained Connection Termination Points attribute.

Table 20-8 *Cisco or Lucent ATM Logical Interface (IAtmLogicalPort/Trunk)*

Attribute Name	Attribute Description	Scheme	Polling Interval
Resource Management Cell Termination	Resource management cell termination (<i>Unknown, CCRM Only, CCRM, BCM</i>)	Any	Configuration
Resource Management Cell Generation	Resource management cell generation (<i>Unknown, None, CCRM, BCM</i>)	Any	Configuration
Effective Check	Effective check (<i>Unknown, No, Yes</i>)	Any	Configuration
Input and Output Capacities	Input and output capacities	Any	Configuration
Administrative Status	Administrative status (<i>Null, Up, Down, Testing</i>)	Any	Status
Operational Status	Operational status (<i>Null, Up, Down, Testing, Unknown, Dormant, Not Present</i>)	Any	Status

All additional attributes are the same as [ATM Interface \(IAtm\)](#)

Cisco or Lucent ATM Trunk Virtual Connection

The [Cisco or Lucent ATM Trunk Virtual Connection](#) and [Cisco or Lucent ATM Soft Permanent Virtual Connection](#) data link layer objects are bound by their Containing Termination Points attributes to an [ATM Interface](#) object. They are accessed primarily by a [Virtual Cross Connection](#) object, although they are not bound to it by any of their attributes.

Table 20-9 *Cisco or Lucent ATM Trunk Virtual Connection (IAtmTrunkVc)*

Attribute Name	Attribute Description	Scheme	Polling Interval
Destination Description	Destination party description	Any	Configuration

All additional attributes are the same as [ATM Virtual Connection \(IAtmVc\)](#)

Cisco or Lucent ATM Soft Permanent Virtual Connection

Table 20-10 Cisco or Lucent ATM Soft Permanent Virtual Connection (IAtmSpVc)

Attribute Name	Attribute Description	Scheme	Polling Interval
Remote Virtual Channel Identifier	Remote Virtual Channel Identifier (VCI)	Any	Configuration
Remote Virtual Path Identifier	Remote Virtual Path Identifier (VPI)	Any	Configuration
Remote Network Service Access Point	Remote Network Service Access Point (NSAP), which is the destination ATM address	Any	Configuration

All additional attributes are the same as [ATM Virtual Connection \(IAtmVc\)](#)

Alcatel ASAM ATM Interface

The [Alcatel ASAM ATM Interface](#) and [ECI HiFocus ATM Interface](#) data link layer objects aggregate multiple [ATM Virtual Connections](#), which they are bound to by their VC Table attributes. They are bound by their Containing Termination Points attributes to a physical layer interface. They are accessed primarily by [Virtual Connection Switching Entity](#) and data link layer [VC Encapsulation](#) objects bound by their Contained Connection Termination Points attributes.

Table 20-11 Alcatel ASAM ATM Interface (IASamAtm)

Attribute Name	Attribute Description	Scheme	Polling Interval
CAC Traffic Descriptor	Connection admission control (CAC) traffic descriptor (Alcatel ASAM ATM Traffic Descriptor)	Product	Configuration
Access Traffic Descriptor	Access traffic descriptor (Alcatel ASAM Access Traffic Descriptor)	Product	Configuration

All additional attributes are the same as [ATM Interface \(IAtm\)](#)

ECI HiFocus ATM Interface

Table 20-12 ECI HiFocus ATM Interface (IHiFocusAtm)

Attribute Name	Attribute Description	Scheme	Polling Interval
CAC Traffic Descriptor	Connection admission control (CAC) traffic descriptor (ECI HiFocus ATM Traffic Descriptor)	Product	Configuration
Access Traffic Descriptor	Access traffic descriptor (Alcatel ATM Access Traffic Descriptor)	Product	Configuration

All additional attributes are the same as [ATM Interface \(IAtm\)](#)

Alcatel ASAM ATM Traffic Descriptor

The following objects — [Alcatel ASAM ATM Traffic Descriptor](#), [ECI HiFocus ATM Traffic Descriptor](#), [Lucent WAN Switch ATM Traffic Descriptor](#) and [Lucent WAN Switch ATM Traffic Descriptor](#) — describe traffic of a single [ATM Virtual Connection](#). They are aggregated by a [Traffic Descriptor Container](#) object.

Table 20-13 Alcatel ASAM ATM Traffic Descriptor (*IASamAtmTrafficDescriptor*)

Attribute Name	Attribute Description	Scheme	Polling Interval
User VP and VC Ranges	Numeric ranges of the allowed user VPI/VCI values	Product	Configuration
All additional attributes are the same as ATM Traffic Descriptor (IAtmTrafficDescriptor)			

ECI HiFocus ATM Traffic Descriptor

Table 20-14 ECI HiFocus ATM Interface (*IHiFocusAtm*)

Attribute Name	Attribute Description	Scheme	Polling Interval
Service Category	ATM service category (<i>Unspecified</i>)	Product	Configuration
All additional attributes are the same as ATM Traffic Descriptor (IAtmTrafficDescriptor)			

Lucent WAN Switch ATM Traffic Descriptor

Table 20-15 Lucent's WAN Switch ATM Traffic Descriptor (*ILucentWANSwitchAtmTrafficDescriptor*)

Attribute Name	Attribute Description	Scheme	Polling Interval
Priority	Connection priority	Product	Configuration
Type	Connection type	Product	Configuration
All additional attributes are the same as ATM Traffic Descriptor (IAtmTrafficDescriptor)			

Alcatel ATM Access Traffic Descriptor

The [Alcatel ATM Access Traffic Descriptor](#) object describes access traffic of a single [ATM Virtual Connection](#). It is aggregated by a [Traffic Descriptor Container](#).

Table 20-16 Alcatel ATM Access Traffic Descriptor (*IAtmAccessTrafficDescriptor*)

Attribute Name	Attribute Description	Scheme	Polling Interval
Scope	Access scope (<i>Null, Local, Network</i>)	Product	Configuration
Maximum Active VPCs and VCCs	Maximum active virtual path and virtual channel connections	Product	Configuration
Maximum Supported VPI and VCI Bits	Maximum supported virtual path and virtual channel bits	Product	Configuration
Generic Flow Control Mode	Generic flow control mode (<i>Null, UNI, NNI</i>)	Product	Configuration
Police Mode	Police mode (<i>Null, None, VC Only, All</i>)	Product	Configuration
Name	Traffic descriptor name	Product	Configuration
Index	Traffic descriptor index	Product	Configuration

Alcatel ASAM Access Traffic Descriptor

[Alcatel ASAM Access Traffic Descriptor](#) object describes access traffic of a single [ATM Virtual Connection](#). It is aggregated by a [Traffic Descriptor Container](#).

Table 20-17 Alcatel ASAM Access Traffic Descriptor (*IAsamAccessTrafficDescriptor*)

Attribute Name	Attribute Description	Scheme	Polling Interval
Maximum Supported VPCs and VCCs	Maximum supported virtual path and virtual channel connections	Product	Configuration
Maximum Active VPI and VCI Bits	Maximum active virtual path and virtual channel bits	Product	Configuration
All additional attributes are the same as Alcatel ATM Access Traffic Descriptor (IAtmAccessTrafficDescriptor)			

Network Topology

Cisco ANA discovers ATM data link layer topology by searching for the same set of active [ATM Virtual Connections](#) in any remote side's ATM port VC table related to the same type of the local ATM port. This topology also applies to the underlying physical links.

In particular, Cisco ANA looks for harmony between the VC tables of participating ports based on the lowest active VC (registry default to 3). Further verification is done by matching the VC traffic signature of these ports using Cisco's confidential scheme, which requires a substantial amount of traffic to function correctly.

This mechanism 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.

Service Alarms

The following alarms are supported for this technology:

- [Cloud Problem, page 41-22](#)
- [Discard Packets, page 41-26](#)
- [Dropped Packets, page 41-27](#)
- [Link Down, page 41-42](#)
- [Port Down, page 41-51](#)
- [Rx Utilization, page 41-53](#)
- [Tx Utilization, page 41-57](#)
- [ATM IMA Service, page 41-5](#)

Note that these alarms, apart from Cloud Problem, are related to the underlying physical interface (see [Common Components](#)).



CHAPTER 21

Frame Relay

This chapter describes the level of support that Cisco ANA provides for Frame Relay, as follows:

- [Technology Description, page 21-1](#)
- [Information Model Objects \(IMOs\), page 21-1](#)
- [Vendor-Specific Inventory and IMOs, page 21-4](#)
- [Network Topology, page 21-4](#)
- [Service Alarms, page 21-4](#)

Technology Description

Please see Part 1: Cisco VNEs in this guide for information about which devices support the various technologies.

Frame Relay

Frame Relay is a high-performance data link (Layer 2) WAN protocol that uses variable-length packet switching with statistical multiplexing. Although originally designed for use across ISDN interfaces, today it is used over a variety of additional network interfaces.

Frame Relay networks consist of Frame Relay switches interconnected by point-to-point Frame Relay links or interfaces. Frame Relay is fundamentally connection oriented, which means that a VC must be set up across the Frame Relay network prior to any data transfer.

Information Model Objects (IMOs)

This section describes the following IMOs:

- [Frame Relay Interface \(IFrameRelay/IFrTrunk\)](#)
- [Frame Relay Virtual Connection \(IFrVc\)](#)
- [Frame Relay Traffic Descriptor \(IFRTrafficDescriptor\)](#)
- [Frame Relay Logical Interface \(IFrameRelayLogicalPort/Trunk\)](#)
- [Frame Relay Trunk Virtual Connection \(IFrTrunkVc\)](#)

Frame Relay Interface

The data link layer [Frame Relay Interface](#) object aggregates multiple [Frame Relay Virtual Connections](#), which it is bound to by its VC Table attributes. It is bound by its Containing Termination Points attribute to a physical layer interface. It is accessed primarily by the data link layer [VC Multiplexer](#) bound by its Contained Connection Termination Points attribute. It is also accessed by the [Virtual Connection Switching Entity](#).

Table 21-1 *Frame Relay Interface (IFrameRelay/IFrTrunk)*

Attribute Name	Attribute Description	Scheme	Polling Interval
Address Format	Frame Relay address format (<i>Unknown, q921, q922March90, q922November90, q922</i>)	Any	Configuration
Maximum Supported VCs	Maximum supported virtual connections	Any	Configuration
Protocol Type	Frame Relay protocol type (<i>Unknown, Frame Relay, FR FUNI, Frame Forward</i>)	Any	Configuration
VC Table	Array of Frame Relay Virtual Connections	Any	Configuration
Cross Connect Table	Array of Virtual Cross Connections	Any	Configuration
IANA Type	Internet Assigned Numbers Authority (IANA) type of the sublayer	N/A	N/A
Containing Termination Points	Underlying termination points (connection or physical)	Any	N/A
Contained Connection Termination Points	Bound connection termination points	Any	N/A

Frame Relay Virtual Connection

The data link layer [Frame Relay Virtual Connection](#) object is bound by its Containing Termination Points attribute to a data link layer [Frame Relay Interface](#) object. It is accessed primarily by a [Virtual Cross Connection](#) and data link layer [VC Encapsulation](#), but is not bound to them by any of its attributes.

Table 21-2 *Frame Relay Virtual Connection (IFrVc)*

Attribute Name	Attribute Description	Scheme	Polling Interval
Data Link Connection Identifier	Data Link Connection Identifier (DLCI)	Any	Configuration
Traffic Descriptor	Traffic descriptor (Frame Relay Traffic Descriptor)	Any	Configuration
Discarded and Received Input Data Counters	Discarded and received input octet and packet counters	Any	Configuration
Dropped and Forwarded Output Data Counters	Dropped and forwarded output octet and packet counters	Any	Configuration
Ingress Traffic Descriptor	Ingress traffic descriptor (Frame Relay Traffic Descriptor)	Any	Configuration
Egress Traffic Descriptor	Egress traffic descriptor (Frame Relay Traffic Descriptor)	Any	Configuration
Administrative Status	Administrative status (<i>Unknown, Up, Down</i>)	Any	Status
Operational Status	Operational status (<i>Unknown, Up, Down</i>)	Any	Status

Table 21-2 *Frame Relay Virtual Connection (IFrVc) (continued)*

Attribute Name	Attribute Description	Scheme	Polling Interval
IANA Type	Internet Assigned Numbers Authority (IANA) type of the sublayer	N/A	N/A
Containing Termination Points	Underlying termination points (connection or physical)	Any	N/A
Contained Connection Termination Points	Bound connection termination points	Any	N/A

Frame Relay Traffic Descriptor

The [Frame Relay Traffic Descriptor](#) object describes the traffic of a single [Frame Relay Virtual Connection](#). It is aggregated by a [Traffic Descriptor Container](#) object (see [Common Components](#)).

Table 21-3 *Frame Relay Traffic Descriptor (IFRTrafficDescriptor)*

Attribute Name	Attribute Description	Scheme	Polling Interval
Committed Rate	Committed burst rate	Any	Configuration
Excess Burst Rate	Excess burst rate	Any	Configuration
Name	Traffic descriptor name	Any	Configuration
Index	Traffic descriptor index	Any	Configuration

Frame Relay Logical Interface

The data link layer [Frame Relay Logical Interface](#) object aggregates multiple [Frame Relay Virtual Connections](#), which it is bound to by its VC Table attributes. It is bound by its Containing Termination Points attribute to a physical layer interface. It is accessed primarily by the [Virtual Connection Switching Entity](#) and data link layer [VC Encapsulation](#) bound by its Contained Connection Termination Points attribute.

Table 21-4 *Frame Relay Logical Interface (IFrameRelayLogicalPort/Trunk)*

Attribute Name	Attribute Description	Scheme	Polling Interval
Administrative Status	Administrative status (<i>Null, Up, Down, Testing</i>)	Any	Status
Operational Status	Operational status (<i>Null, Up, Down, Testing, Unknown, Dormant, Not Present</i>)	Any	Status

All additional attributes are the same as [Frame Relay Interface \(IFrameRelay/IFrTrunk\)](#)

Frame Relay Trunk Virtual Connection

The data link layer [Frame Relay Trunk Virtual Connection](#) object is bound by its Containing Termination Points attribute to a [Frame Relay Interface](#) object. It is accessed primarily by a [Virtual Cross Connection](#) and data link layer [VC Encapsulation](#), but is not bound to them by any of its attributes.

Table 21-5 *Frame Relay Trunk Virtual Connection (IFrTrunkVc)*

Attribute Name	Attribute Description	Scheme	Polling Interval
Destination Description	Destination party description	Any	Configuration
All additional attributes are the same as Frame Relay Virtual Connection (IFrVc)			

Vendor-Specific Inventory and IMOs

There are no vendor-specific inventory or IMOs for this technology.

Network Topology

Cisco ANA does not support discovery of Frame Relay data link layer topology. This topology is manually (statically) configured by the system administrator.

Service Alarms

The following alarms are supported for this technology:

- [Cloud Problem](#), page 41-22
- [Discard Packets](#), page 41-26
- [Dropped Packets](#), page 41-27
- [Link Down](#), page 41-42
- [Port Down](#), page 41-51
- [Rx Utilization](#), page 41-53
- [Tx Utilization](#), page 41-57

Note that these alarms, apart from Cloud Problem, are related to the underlying physical interface (see [Common Components](#)).



CHAPTER 22

Integrated Services Digital Network

This chapter describes the level of support that Cisco ANA provides for ISDN, as follows:

- [Technology Description, page 22-1](#)
- [Information Model Objects \(IMOs\), page 22-1](#)
- [Vendor-Specific Inventory and IMOs, page 22-3](#)
- [Network Topology, page 22-3](#)
- [Service Alarms, page 22-3](#)

Technology Description

Please see Part 1: Cisco VNEs in this guide for information about which devices support the various technologies.

ISDN

ISDN is a digital telephony and data transport service offered by regional telephone carriers. ISDN involves digitization of the telephone network, which permits voice, data, text, graphics, music, video, and other source material to be transmitted over existing telephone wires.

ISDN offers two types of channels: A 64-Kb/s Bearer (B) channel used for data, and a 64-Kb/s (maximum) Delta (D) channel used for signaling and control over layers 1, 2, and 3 of the Open Systems Interconnection (OSI) model. It also offers two types of channel-based services: The 192-Kb/s Basic Rate Interface (BRI) service, which offers two B channels and one D channel (2B+D); and the 1.544/2.048-Mb/s Primary Rate Interfaces (PRI) service, which offers 23 to 31 B channels and one D channel, respectively, for the xDSL interface backup.

Information Model Objects (IMOs)

This section describes the following IMOs:

- [ISDN Interface \(IIsdnLayer2\)](#)
- [ISDN Channel \(IIsdnChannel\)](#)
- [ISDN Physical \(IIsdnLayer1\)](#)

ISDN Interface

The data link layer [ISDN Interface](#) object is bound by its Containing Termination Points attribute to a physical layer [ISDN Physical](#) object. It is accessed primarily by a [PPP Encapsulation](#) bound by its Contained Connection Termination Points attribute.

Table 22-1 *ISDN Interface (IIsdnLayer2)*

Attribute Name	Attribute Description	Scheme	Polling Interval
Control Administrative Status	Administrative status (<i>Unknown, Up, Down, Testing</i>)	Product	Status
Operational Status	Operational status (<i>Unknown, Up, Down, Testing, Dormant, Not Present</i>)	Product	Status
Channels Table	Array of ISDN Channels	Product	Configuration
IANA Type	Internet Assigned Numbers Authority (IANA) type of the sublayer	N/A	N/A
Containing Termination Points	Underlying termination points (connection or physical)	Product	N/A
Contained Connection Termination Points	Bound connection termination points	Product	N/A

ISDN Channel

The data link layer [ISDN Channel](#) object describes an [ISDN Interface](#) channels table's entry.

Table 22-2 *ISDN Channel (IIsdnChannel)*

Attribute Name	Attribute Description	Scheme	Polling Interval
Control Administrative Status	Administrative status (<i>Unknown, Up, Down, Testing</i>)	Product	Status
Operational Status	Operational status (<i>Unknown, Up, Down, Testing, Dormant, Not Present</i>)	Product	Status

ISDN Physical

The physical layer [ISDN Physical](#) object is bound by its Containing Termination Points attribute to a [Port Connector](#) object. It is accessed by the data link layer [ISDN Interface](#) bound by its Contained Connection Termination Points attribute.

Table 22-3 *ISDN Physical (IIsdnLayer1)*

Attribute Name	Attribute Description	Scheme	Polling Interval
All attributes are the same as those of Physical Layer (IPhysicalLayer) .			

Vendor-Specific Inventory and IMOs

There are no vendor-specific inventory or IMOs for this technology.

Network Topology

Cisco ANA does not support discovery of ISDN physical layer topology. This topology is manually (statically) configured by the system administrator.

Service Alarms

The following alarms are supported for this technology:

- [Link Down, page 41-42](#)
- [Port Down, page 41-51](#)



CHAPTER 23

Point-to-Point Protocol

This chapter describes the level of support that Cisco ANA provides for Point-to-Point Protocol (PPP), as follows:

- [Technology Description, page 23-1](#)
- [Information Model Objects \(IMOs\), page 23-3](#)
- [Vendor-Specific Inventory and IMOs, page 23-4](#)
- [Network Topology, page 23-4](#)
- [Service Alarms, page 23-5](#)

Technology Description

This section provides the following PPP technology descriptions:

- [PPP](#)
- [POS](#)
- [PPPoA](#)
- [PPPoE](#)
- [PPPoFR](#)
- [Multilink PPP](#)

Please see Part 1: Cisco VNEs in this guide for information about which devices support the various technologies.

PPP

PPP (RFC 1661) originally emerged as an encapsulation protocol for transporting IP traffic over point-to-point links. PPP also established standards for the assignment and management of IP addresses, octet-synchronous (asynchronous) encapsulation, use of an HDLC-like framing protocol (RFC 1662), bit-synchronous encapsulation, use of HDLC protocols, network protocol multiplexing, link configuration, link quality testing, error detection, and option negotiation for such capabilities as network layer address and data compression negotiation.

PPP supports these functions by providing an extensible Link Control Protocol (LCP) and a family of Network Control Protocols (NCPs) to negotiate optional configuration parameters and facilities.

POS

Packet over SONET/SDH (PoS) is a data link (Layer 2) technology that uses PPP (RFC 1661) in HDLC-like framing (RFC 1662) encapsulation over SONET/SDH framing. The PoS interface supports SONET/SDH-level alarm processing, performance monitoring, synchronization, and protection switching, which enables seamless interoperability with existing SONET infrastructures and provides the capability to migrate to IP+Optical networks without the need for legacy SONET infrastructures.

PPPoA

Point-to-Point Protocol over ATM (PPPoA, RFC 2364) is a protocol for encapsulating PPP frames for transmission over an ATM network. It offers standard PPP features and supports the VC-MUX and LLC based encapsulation. It is used mainly by DOCSIS and DSL carriers.

PPPoE

Point-to-Point Protocol over Ethernet (PPPoE, RFC 2516) is a protocol for encapsulating PPP frames inside Ethernet frames. It is used mainly with DSL services where individual users connect to the DSL modem over Ethernet and in plain Metro Ethernet networks.

PPPoFR

Point-to-Point Protocol over Frame Relay (PPPoFR, RFC 1973) is a protocol for encapsulating PPP frames for transmission across Frame Relay connections. The traditional usage of this interface has been on dial-in access servers, to support multiple PPP dial-in clients terminating their connection on a single interface running IP.

Multilink PPP

Multilink PPP (also referred to as MP, MPPP, MLP, or Multilink) provides a method for spreading traffic across multiple physical WAN links while providing packet fragmentation and reassembly, proper sequencing, multivendor interoperability, and load balancing on inbound and outbound traffic. MPPP allows packets to be fragmented. These fragments are sent simultaneously over multiple point-to-point links to the same remote address. The multiple physical links come up in response to a user-defined load threshold. This load can be measured on just inbound traffic, on just outbound traffic, or on either; however, it cannot be measured on the combined load of both inbound and outbound traffic.

Information Model Objects (IMOs)

This section describes the following IMOs:

- [PPP Encapsulation \(IVcBasedEncapsulation\)](#)
- [Multilink PPP Interface \(IMLPPP\)](#)

PPP Encapsulation

The data link layer [PPP Encapsulation](#) object is bound by its Containing Termination Points attribute to an ATM/Frame Relay [VC Multiplexer](#) object. It is accessed primarily by a network layer object, such as the [IP Interface](#) bound by its Contained Connection Termination Points attribute.

Table 23-1 *PPP Encapsulation (IVcBasedEncapsulation)*

Attribute Name	Attribute Description	Scheme	Polling Interval
Virtual Connection	Virtual connection, if applicable (ATM Virtual Connection , Frame Relay Virtual Connection , or Virtual LAN Interface)	Any	Configuration
Binding Information	Binding information (<i>User Name</i> , and so on)	Any	Configuration
Binding Status	Binding status (<i>Not Bound</i> , <i>Bound</i>)	Any	Configuration
IANA Type	Internet Assigned Numbers Authority (IANA) type of the sublayer	N/A	N/A
Containing Termination Points	Underlying termination points (connection or physical)	Any	N/A
Contained Connection Termination Points	Bound connection termination points	Any	N/A

Multilink PPP Interface

The [Multilink PPP Interface](#) object models a multilink PPP bundle, which is a named virtual interface with multiple member links.

Table 23-2 *Multilink PPP Interface (IMLPPP)*

Attribute Name	Attribute Description	Scheme	Polling Interval
ActiveLink	The number of links currently active for the MLPPP bundle.	Product	Configuration
InterfaceName	The interface name (for example, <i>Multilink</i>).	Product	Configuration
GroupNumber	The numerical group ID of the multilink bundle (for example, 8).	Product	Configuration
MTU	The Maximum Transmission Unit for the bundle link.	Product	Configuration
FragmentDelay	The maximum realtime delay (in milliseconds) between each fragment.	Product	Configuration
FragmentDisable	Indicates whether the multilink fragmentation function is disabled (<i>true</i>) or enabled (<i>false</i>).	Product	Configuration
FragmentMaximum	The maximum number of fragments allowed per packet.	Product	Configuration
FragmentSize	The maximum size of each fragment.	Product	Configuration

Table 23-2 Multilink PPP Interface (IMLPPP)

Attribute Name	Attribute Description	Scheme	Polling Interval
InterleaveEnabled	Indicates whether the fragment interleaving function is enabled (<i>true</i>) or disabled (<i>false</i>).	Product	Configuration
Keepalive	Indicates the status of the keepalive (<i>set</i> , <i>not set</i> , <i>unknown</i>).	Product	Configuration
KeepaliveTime	The keepalive timeout value (in milliseconds) for the member links.	Product	Configuration
KeepaliveRetry	The number of times to attempt keepalive before timing out.	Product	Configuration
MinimumConfigured Link	Minimum number of member interfaces configured to participate in a multilink PPP bundle.	Product	Configuration
MaximumConfigure dLink	Maximum number of member interfaces configured to participate in a multilink PPP bundle.	Product	Configuration
LocalMRRU	The Maximum Received Reconstructed Unit (in bytes) for the local links.	Product	Configuration
RemoteMRRU	The Maximum Received Reconstructed Unit (in bytes) for the remote links.	Product	Configuration
LoadThreshold	The threshold percentage of bandwidth usage at which to add member links and increase the bandwidth of the bundle interface (or delete member links and decrease capacity). Values range from 1 (unloaded) to 255 (fully loaded) and correspond to a percentage of total use (for example, a value of 191 represents a threshold of 75% of total usage).	Product	Configuration
LCPSatus	The Link Control Protocol status code (values 1 through 11).	Product	Configuration
AdminStatus	The administrative status of the bundle (<i>Down</i> , <i>Testing</i> , <i>Up</i>).	Product	Configuration
OperStatus	The operational status of the bundle (<i>Down</i> , <i>Testing</i> , <i>Up</i>).	Product	Configuration

Vendor-Specific Inventory and IMOs

There are no vendor-specific inventory or IMOs for this technology.

Network Topology

Cisco ANA performs discovery of PPP topologies by searching for the local IP subnet in any one-hop-away remote sides of the PPP interfaces. In particular, it compares the local and remote IP subnets gathered from the upper IP Network layers.

Service Alarms

The following alarm is supported for this technology:

- [MLPPP Bundle, page 41-46](#)



CHAPTER 24

High-Level Data Link Control

This chapter describes the level of support that Cisco ANA provides for HDLC, as follows:

- [Technology Description, page 24-1](#)
- [Information Model Objects \(IMOs\), page 24-2](#)
- [Vendor-Specific Inventory and IMOs, page 24-2](#)
- [Network Topology, page 24-2](#)
- [Service Alarms, page 24-2](#)

Technology Description

Please see Part 1: Cisco VNEs in this guide for information about which devices support the various technologies.

HDLC

HDLC is a group of data link (Layer 2) protocols used to transmit synchronous data packets between point-to-point nodes. Data is organized into addressable frames. This format has been used for other multipoint-to-multipoint protocols, and inspired the HDLC-like framing protocol described in RFC 1662.

HDLC uses a zero-insertion/deletion process (bit stuffing) to ensure that the bit pattern of the delimiter flag does not occur in the fields between flags. The HDLC frame is synchronous and therefore relies on the physical layer (Layer 1) to clock and synchronize frame transmission and reception.

Information Model Objects (IMOs)

This section describes the following IMO:

- [HDLC Encapsulation \(IEncapsulation\)](#)

HDLC Encapsulation

The data link layer [HDLC Encapsulation](#) object is bound by its Containing Termination Points attribute to an ATM/Frame Relay [VC Multiplexer](#) object. It is accessed primarily by a network layer object, such as the [IP Interface](#) bound by its Contained Connection Termination Points attribute.

Table 24-1 *HDLC Encapsulation (IEncapsulation)*

Attribute Name	Attribute Description	Scheme	Polling Interval
Virtual Connection	Virtual connection	Any	Configuration
Binding Information	Binding information (<i>User Name, ...</i>)	Any	Configuration
Binding Status	Binding status (<i>Not Bound, Bound</i>)	Any	Configuration
IANA Type	Internet Assigned Numbers Authority (IANA) type of the sublayer	N/A	N/A
Containing Termination Points	Underlying termination points (connection or physical)	Any	N/A
Contained Connection Termination Points	Bound connection termination points	Any	N/A

Vendor-Specific Inventory and IMOs

There are no vendor-specific inventory or IMOs for this technology.

Network Topology

Cisco ANA performs discovery of HDLC topologies by searching for the local IP subnet in any one-hop-away remote sides of the HDLC interfaces. In particular, it compares the local and remote IP subnets gathered from the upper IP Network layers.

Service Alarms

There are no faults or alarms specific to this technology.



CHAPTER 25

Layer 2 Tunnel Protocol

This chapter describes the level of support that Cisco ANA provides for L2TP, as follows:

- [Technology Description, page 25-1](#)
- [Information Model Objects \(IMOs\), page 25-2](#)
- [Vendor-Specific Inventory and IMOs, page 25-3](#)
- [Network Topology, page 25-4](#)
- [Service Alarms, page 25-5](#)



Note

L2TP technology is currently not supported for Cisco devices.

Technology Description

Please see Part 1: Cisco VNEs in this guide for information about which devices support the various technologies.

L2TP

Layer 2 Tunnel Protocol (L2TP) acts like a data link (Layer 2) protocol for tunneling network traffic between two peers over an existing network (usually the Internet). The two endpoints of an L2TP tunnel are the initiator of the tunnel, the L2TP access concentrator (LAC), and the L2TP network server (LNS), which waits for new tunnels. Once a tunnel is established, the network traffic between the peers is bidirectional.

L2TP is, in fact, a session layer (Layer 5) protocol, as the entire L2TP packet is sent within a User Datagram Protocol (UDP) datagram, while it is common to carry PPP sessions within an L2TP tunnel. L2TP does not by itself provide confidentiality or strong authentication. IPsec is often used to secure L2TP packets by providing confidentiality, authentication, and integrity.

Information Model Objects (IMOs)

This section describes the following IMOs:

- [L2TP Interface \(IL2TPTunnel\)](#)
- [L2TP Session Entry \(IL2TPSessionEntry\)](#)

L2TP Interface

The [L2TP Interface](#) object represents one edge of an L2TP tunnel. It aggregates multiple [L2TP Session Entries](#), to which it is bound by its Session Table attributes. It is aggregated by an L2TP peer from which it is created or cloned.

Table 25-1 L2TP Interface (IL2TPTunnel)

Attribute Name	Attribute Description	Scheme	Polling Interval
Local and Remote Tunnel Identifications	Local and remote tunnel identifications	Product	Configuration
Local and Remote Tunnel Names	Local and remote tunnel names	Product	Configuration
Remote Address	Remote IP address	Product	Configuration
Control Errors	Control errors count	Product	Configuration
Last Error Code	Error code value recorded for the last error that caused tunnel disconnection	Product	Configuration
Tunnel State	Tunnel state (<i>Unknown, Idle, Connecting, Established, Disconnecting</i>)	Product	Configuration
Sessions Count	Current session count	Product	Configuration
Sessions Table	Array of L2TP Session Entries	Product	Configuration

L2TP Session Entry

The [L2TP Session Entry](#) object represents a session within an L2TP tunnel. It is primarily accessed by the [L2TP Interface](#) in which it is contained.

Table 25-2 L2TP Session Entry (IL2TPSessionEntry)

Attribute Name	Attribute Description	Scheme	Polling Interval
Local and Remote Session Identifications	Local and remote session identifications	Product	Configuration
Subscriber Name	Subscriber name	Product	Configuration
Session Type	Session type (<i>Unknown, LAC, LNS</i>)	Product	Configuration
Session State	Session state (<i>Unknown, Idle, Connecting, Established, Disconnecting</i>)	Product	Configuration
Input and Output Data Counters	Input and output data octets and packet counters	Product	Configuration

Vendor-Specific Inventory and IMOs

Vendor-specific IMOs are implemented only for specific vendor devices. The following sections describe objects for specific vendors:

- [Redback L2TP Peer](#)
- [Redback L2TP Group](#)
- [Redback L2TP Domain Entry](#)

Redback L2TP Peer

The [Redback L2TP Peer](#) object describes a logical component aggregating multiple [L2TP Interfaces](#) and their configurations. It is bound by its Logical Sons attribute and is used primarily for managing the creation of L2TP tunnels.

Table 25-3 *Redback L2TP Peer (IL2TPPeer)*

Attribute Name	Attribute Description	Scheme	Polling Interval
Local and Peer Addresses	Local and peer IP addresses	Product	Configuration
Local and Peer Names	Local and peer names	Product	Configuration
Tunnel Type	Tunnel type (<i>Unknown, LAC, LNS</i>)	Product	Configuration
Tunnel Mode	Tunnel mode (<i>Null, Static, Dynamic</i>)	Product	Configuration
Maximum and Current Tunnels Counts	Maximum and current tunnel counts	Product	Configuration
Maximum and Current Sessions Counts	Maximum and current session counts	Product	Configuration
Session Authentication Type	Session authentication type (<i>Null, None, Simple, Challenge</i>)	Product	Configuration
Tunnel Password	Tunnel password for the authentication phase of the tunnel establishment	Product	Configuration
RADIUS Identification	RADIUS identifier	Product	Configuration
Hello Time Interval	Time interval at which hello (keepalive) packets should be sent	Product	Configuration
Control Errors	Control errors count	Product	Configuration
Media Type	Underlying media type (<i>Null, Other, None, UDPLP, Frame Relay, ATM</i>)	Product	Configuration
Group Identification	OID of LT2P group (<i>IL2TPGroup</i>)	Product	Configuration
Domains Table	Array of L2TP Domain Entries	Product	Configuration
Logical Sons	Array of aggregated L2TP Interfaces	Product	N/A

Redback L2TP Group

The [Redback L2TP Group](#) object describes a logical component that is load balancing multiple [Redback L2TP Peers](#). The [Redback L2TP Peers](#) are grouped by the [Redback L2TP Group](#) Peer List attribute and aggregated by a [Traffic Descriptor Container](#) object.

Table 25-4 *Redback L2TP Group (IL2TPGroup)*

Attribute Name	Attribute Description	Scheme	Polling Interval
Group Name	Layer 2 tunnel protocol group name	Product	Configuration
Tunnel Algorithm	Tunnel algorithm	Product	Configuration
Dead Time	Dead time	Product	Configuration
RADIUS Identification	RADIUS identifier	Product	Configuration
Peers List	Array of Redback L2TP Peers	Product	Configuration
Domains Table	Array of L2TP Domain Entries	Product	Configuration
Name	Group name	Product	Configuration
Index	Group index	Product	Configuration

Redback L2TP Domain Entry

The [Redback L2TP Domain Entry](#) object describes an Internet domain in which members are allowed to open L2TP sessions within L2TP tunnels, aggregated by the L2TP peers or groups containing the domain. It is aggregated by a [Traffic Descriptor Container](#) object.

Table 25-5 *Redback L2TP Domain Entry (IL2TPDomainEntry)*

Attribute Name	Attribute Description	Scheme	Polling Interval
Domain Name	L2TP domain name	Product	Configuration
Attached To Object	OID of the Redback L2TP Peer or Redback L2TP Group to which this domain is attached	Product	Configuration
Name	Peer or group name	Product	Configuration
Index	Peer or group index	Product	Configuration

Network Topology

Cisco ANA does not support discovery or manual configuration of L2TP data link layer topology.

Service Alarms

The following alarms are supported for this technology:

- [L2TP Peer Not Established, page 41-37](#)
- [L2TP Sessions Threshold, page 41-38](#)



CHAPTER 26

Discovery Protocols

This chapter describes the level of support that Cisco ANA provides for discovery protocols, as follows:

- [Technology Description, page 26-1](#)
- [Information Model Objects \(IMOs\), page 26-2](#)
- [Vendor-Specific Inventory and IMOs, page 26-3](#)
- [Network Topology, page 26-4](#)
- [Service Alarms, page 26-4](#)

Technology Description

This section provides the following discovery protocol descriptions:

- [LLDP](#)
- [CDP](#)

Please see Part 1: Cisco VNEs in this guide for information about which devices support the various technologies.

LLDP

Link Layer Discovery Protocol (LLDP) is an open IEEE-standard (802.1AB) Layer 2 protocol used by network devices to share information about their identities and functionality with other network elements.

LLDP defines a standard method for Ethernet network devices to advertise information about themselves to other nodes on the network and store the information they discover. LLDP runs on all 802 media. The protocol runs over the data-link layer only, allowing two systems running different network layer protocols to learn about each other.

LLDP-enabled devices store the information they gather in a local table that can be queried using SNMP. This information can include:

- System name and description
- Port name and description
- VLAN name
- IP management address

- System capabilities (switching, routing, and so on)
- MAC/PHY information
- MDI power
- Link aggregation

CDP

Cisco Discovery Protocol (CDP) is Cisco's proprietary Layer 2 protocol, used to discover and share information about network-connected Cisco equipment. Cisco devices share their information by sending CDP announcements every 60 seconds on interfaces that support Subnetwork Access Protocol (SNAP) headers.

Each Cisco network element that supports CDP stores in its CDP table the information it receives from other devices to which it is directly connected. Each entry's information is refreshed, and the hold time reset, each time a new announcement is received. The hold time specifies how long entries in the table must be kept. If no announcements are received from a device before the timer expires, the device's information is discarded.

The information contained in CDP announcements varies by the type of device and the version of the operating system running on it, but always contains at least the device's device ID, port ID, and IP address.

Information Model Objects (IMOs)

This section describes the following IMOs:

- [LLDP Service](#)
- [LLDP Neighbor Entry](#)

LLDP Service

The [LLDP Service](#) object represents the LLDP configuration on the network element.

Table 26-1 *LLDP Service Table (LLDPService)*

Attribute name	Attribute Description	Scheme	Polling Interval
status	The LLDP status (<i>enabled, disabled</i>).	Any	Configuration
lldpAdvertisementsInterval	The LLDP advertisement interval.	Any	Configuration
lldpHoldTime	The advertised LLDP hold time.	Any	Configuration
lldpReinitialisationDelay	The LLDP interface reinitialization delay.	Any	Configuration
localChassisID	The local chassis ID.	Any	Configuration
localSystemName	The local system name.	Any	Configuration
NeighborsInfoTable	An array of instances of LLDP Neighbor Entry .	Any	Configuration

LLDP Neighbor Entry

The [LLDP Neighbor Entry](#) object represents information about a network element's neighbor discovered using the [LLDP Service](#).

Table 26-2 *LLDP Neighbor Entry (ILLDPNeighbor)*

Attribute name	Attribute Description	Scheme	Polling Interval
localPortName	The local port name.	Any	Configuration
localPortId	The local port ID.	Any	Configuration
remotePortDesc	Description of the remote port.	Any	Configuration
remoteChassisId	The neighbor's chassis ID.	Any	Configuration
remotePortId	The remote port ID.	Any	Configuration
remoteDeviceId	The remote device ID.	Any	Configuration
localPortOid	The link for the port.	Any	Configuration
remoteManagementIP	The IP address of the remote management IP.	Any	Configuration

Vendor-Specific Inventory and IMOs

Vendor-specific IMOs are implemented only for specific vendor devices. The following sections describe objects for specific vendors:

- [CDP Service](#)
- [CDP Neighbor Entry](#)

CDP Service

The [CDP Service](#) object represents the CDP configuration on the network element.

Table 26-3 *CDP Service (ICdpService)*

Attribute name	Attribute Description	Scheme	Polling Interval
cdpHoldtime	The configured hold time.	Any	Configuration
cdpMessageInterval	The configured CDP message interval.	Any	Configuration
cdpDeviceId	The ID of the device on which CDP is configured.	Any	Configuration
cdpState	The state of the CDP service on the device (<i>enabled, disabled</i>).	Any	Configuration
cdpVersion	The CDP version supported on the device.	Any	Configuration
NeighborsInfoTable	An array of instances of CDP Neighbor Entry .	Any	Configuration

CDP Neighbor Entry

The [CDP Neighbor Entry](#) object represents information about a network element's neighbor discovered using the [CDP Service](#).

Table 26-4 CDP Neighbor Entry (ICdpNeighbor)

Attribute name	Attribute Description	Scheme	Polling Interval
remoteDeviceId	The neighbor device ID.	Any	Configuration
remotePortId	The neighbor port number.	Any	Configuration
remoteIPAddress	The neighbor IP address.	Any	Configuration
localPortId	The local port ID.	Any	Configuration
localPortOid	The link for the port.	Any	Configuration

Network Topology

The Cisco Discovery Protocol (CDP), although proprietary, plays a major role in discovery of all Cisco network equipment. Cisco ANA uses it as part of the data link topology discovery for all Cisco network elements. It uses CDP by searching for the existence of local CDP neighbor signatures, gathered from the CDP process, in any remote side port of the same type.

LLDP, which is a standard discovery protocol for data link layer, is also used for link discovery on a few Cisco devices which support this protocol. Cisco ANA uses LLDP by searching for the existence of local LLDP neighbor signatures, gathered from the LLDP Process, in any remote side port of the same type.

Service Alarms

There are no faults or alarms associated with this technology.



CHAPTER 27

Local Switching

This chapter describes the level of support that Cisco ANA provides for local switching, as follows:

- [Technology Description, page 27-1](#)
- [Information Model Objects \(IMOs\), page 27-2](#)
- [Vendor-Specific Inventory and IMOs, page 27-2](#)
- [Network Topology, page 27-3](#)
- [Service Alarms, page 27-3](#)

Technology Description

Please see Part 1: Cisco VNEs in this guide for information about which devices support the various technologies.

Local Switching

Local switching allows switching of Layer 2 data between two attachment circuits on the same device. Local switching operates in several modes and technologies.

In local switching (also known as *hairpin connection*), frames from one attachment circuit are switched to another attachment circuit on the same router. The attachment interfaces can be on the same line card or on different cards. During this type of switching, no address information is used at all. The local switching act as a kind of tube between the two interfaces.



Note

Cisco ANA version 3.6 SP4 and later provides support for local switching only in Ethernet and VLAN modes on CRS-1 devices running IOS-XR software.

Information Model Objects (IMOs)

This section describes the following IMOs:

- [Local Switching Entity](#)
- [Local Switching Entry](#)

Local Switching Entity

The [Local Switching Entity](#) is the container for [Local Switching Entry](#) objects.

Table 27-1 *Local Switching Entity Interface (ILocalSwitchingEntity)*

Attribute Name	Attribute Description	Scheme	Polling Interval
Local Switching Table	A set of ILocalSwitchingEntry objects	IPCore	Configuration
PW Switching Table	A local switching table that contains the pseudowire switching points (VFI point-to-point in the case of IOS and cross-connect group in the case of IOS-XR).		

Local Switching Entry

Each [Local Switching Entry](#) describes a single locally switched cross-connect entry.

Table 27-2 *Local Switching Entry Interface (ILocalSwitchingEntry)*

Attribute name	Attribute Description	Scheme	Polling Interval
Local Switching Entry Key	Entry key for the cross-connect group	Product	Configuration
Local Switching Entry Status	Status of the cross-connect	Product	Configuration
Segment 1	Object Identifier of the first cross-connect endpoint	Product	Configuration
Segment 1 Port Name	Name of the first cross-connect endpoint	Product	Configuration
Segment 1 Status	Status of first cross-connect endpoint	Product	Configuration
Segment 2	Object Identifier of the second cross-connect endpoint	Product	Configuration
Segment 2 Port Name	Name of the second cross-connect endpoint	Product	Configuration
Segment 2 Status	Status of second cross-connect endpoint	Product	Configuration

Vendor-Specific Inventory and IMOs

There are no vendor-specific inventory or IMOs for this technology. Currently, only the Cisco CRS-1 device running IOS-XR is supported.

Network Topology

There is no network topology to be discovered specifically for local switching. Local switching is viewable from the Cisco ANA logical inventory through an appropriate cross-connect container. This modeling enables flow functions to operate according to the cross-connect, permitting correlation and path-tracing.

Service Alarms

The following alarm is supported for this technology:

- [Local Switching Down, page 41-43](#)



CHAPTER 28

Digital Subscriber Line

This chapter describes the level of support that Cisco ANA provides for DSL, as follows:

- [Technology Description, page 28-1](#)
- [Information Model Objects \(IMOs\), page 28-2](#)
- [Vendor-Specific Inventory and IMOs, page 28-5](#)
- [Network Topology, page 28-6](#)
- [Service Alarms, page 28-6](#)

Technology Description

Please see Part 1: Cisco VNEs in this guide for information about which devices support the various technologies.

xDSL

DSL is a modem technology that uses existing twisted-pair telephone lines to transport high-bandwidth data, such as multimedia and video, to service subscribers. The term *xDSL* covers a number of similar yet competing forms of DSL, including asymmetric:

- DSL (ADSL/ADSL 2)
- Symmetric DSL (SDSL)
- High-speed DSL (HDSL)
- Rate-adaptive DSL (RADSL)
- Very high bit data rate DSL (VDSL) for delivering up to 52 Mb/s downstream

At the customer end of the connection, a DSL modem converts data from the digital signals used by computers into a voltage signal of a suitable frequency range, which is then applied to the phone line. At the exchange end, a digital subscriber line access multiplexer (DSLAM) terminates the DSL circuits, aggregates them, and hands them off to other networking transports. In the case of ADSL, the voice component is also separated at this step, either by a filter integrated into the DSLAM or by specialized filtering equipment installed upstream.

Information Model Objects (IMOs)

This section describes the following IMOs:

- [DSL Interface \(IDsl/IIdsl/ISdsl/IShdsl\)](#)
- [ADSL Interface \(IADsl\)](#)
- [ADSL 2 Interface \(IADsl2\)](#)
- [DSL Traffic Descriptor \(IIdslTrafficDescriptor\)](#)
- [ADSL Traffic Descriptor \(IAdslTrafficDescriptor\)](#)
- [ADSL 2 Spectrum Traffic Descriptor \(IAdsl2TrafficDescriptor\)](#)
- [Symmetric DSL Traffic Descriptor \(ISdslTrafficDescriptor\)](#)
- [Symmetric High Bit Rate DSL Traffic Descriptor \(IShdslTrafficDescriptor\)](#)

DSL Interface

The following physical layer [DSL Interface](#) (which represents any DSL interface), [ADSL Interface](#), and [ADSL 2 Interface](#) objects are bound by their Containing Termination Points attribute to a [Port Connector](#) object. Each of these objects is accessed primarily by a data link (Layer 2) [ATM Interface](#) bound by its Contained Connection Termination Points attribute.

Table 28-1 *DSL Interface (IDsl/IIdsl/ISdsl/IShdsl)*

Attribute Name	Attribute Description	Scheme	Polling Interval
Modulation Type	Modulation type (<i>Null, DMT, CAP, QAM, GLite, GDMT, 2B1Q</i>)	Product	Configuration
Customer Identification	Customer identifier	Product	Configuration
Traffic Descriptor	Traffic descriptor (DSL Traffic Descriptor)	Product	Configuration

Additional attributes are the same as [Physical Layer \(IPhysicalLayer\)](#)

ADSL Interface

Table 28-2 *ADSL Interface (IADsl)*

Attribute Name	Attribute Description	Scheme	Polling Interval
Maximum Reception and Transmission Bandwidth	Maximum reception and transmission bandwidth	Product	Configuration

Additional attributes are the same as [DSL Interface \(IDsl/IIdsl/ISdsl/IShdsl\)](#)

ADSL 2 Interface

Table 28-3 *ADSL 2 Interface (IADsl2)*

Attribute Name	Attribute Description	Scheme	Polling Interval
Spectrum Traffic Descriptor	Spectrum traffic descriptor (ADSL 2 Spectrum Traffic Descriptor)	Product	Configuration
Traffic Descriptor	Traffic descriptor (ADSL Traffic Descriptor)	Product	Configuration

Additional attributes are the same as [ADSL Interface \(IADsl\)](#)

DSL Traffic Descriptor

The following [DSL Traffic Descriptor](#), [ADSL Traffic Descriptor](#), [ADSL 2 Spectrum Traffic Descriptor](#), [Symmetric DSL Traffic Descriptor](#), and [Symmetric High Bit Rate DSL Traffic Descriptor](#) objects describe the traffic of various standard DSL interfaces. Each object is aggregated by a [Traffic Descriptor Container](#) object.

Table 28-4 *DSL Traffic Descriptor (IldslTrafficDescriptor)*

Attribute Name	Attribute Description	Scheme	Polling Interval
Target Bit Rate	Target bit rate	Product	Configuration
Name	Traffic descriptor name	Product	Configuration
Index	Traffic descriptor index	Product	Configuration

ADSL Traffic Descriptor

Table 28-5 *ADSL Traffic Descriptor (IAdslTrafficDescriptor)*

Attribute Name	Attribute Description	Scheme	Polling Interval
Maximum, Minimum and Target Transmission and Reception Noise Margins	Maximum, minimum, and target transmission and reception noise margins	Product	Configuration
Maximum, Minimum and Planned Transmission and Reception Bit Rates	Maximum, minimum, and planned transmission and reception bit rates	Product	Configuration
Maximum Transmission Power Spectral Density	Maximum transmission Power Spectral Density (PSD)	Product	Configuration
Transmission and Reception Rate Adaptation	Transmission and reception rate adaptation mode (<i>Null, Fixed, Adapt at Startup, Adapt at Runtime</i>)	Product	Configuration
Channel Type	ADSL channel type (<i>Null, Fast, Interleaved, Fast or Interleaved, Fast and Interleaved</i>)	Product	Configuration
Name	Traffic descriptor name	Product	Configuration
Index	Traffic descriptor index	Product	Configuration

ADSL 2 Spectrum Traffic Descriptor

Table 28-6 *ADSL 2 Spectrum Traffic Descriptor (IAdsl2TrafficDescriptor)*

Attribute Name	Attribute Description	Scheme	Polling Interval
Maximum, Minimum and Target Transmission and Reception Noise Margins	Maximum, minimum, and target transmission and reception noise margins	Product	Configuration
Name	Traffic descriptor name	Product	Configuration
Index	Traffic descriptor index	Product	Configuration

Symmetric DSL Traffic Descriptor

Table 28-7 *Symmetric DSL Traffic Descriptor (ISdslTrafficDescriptor)*

Attribute Name	Attribute Description	Scheme	Polling Interval
Target and Minimum Bit Rate	Target and minimum line bit rate	Product	Configuration
Target Noise Margin	Target noise margin	Product	Configuration
Name	Traffic descriptor name	Product	Configuration
Index	Traffic descriptor index	Product	Configuration

Symmetric High Bit Rate DSL Traffic Descriptor

Table 28-8 *Symmetric High Bit Rate DSL Traffic Descriptor (IShdsITrafficDescriptor)*

Attribute Name	Attribute Description	Scheme	Polling Interval
Target Bit Rate	Target line bit rate	Product	Configuration
Wire Mode	Wire mode (<i>Null, Two Wire, Four Wire</i>)	Product	Configuration
Spectral Mode	Spectral mode (<i>Null, Symmetric, Asymmetric</i>)	Product	Configuration
Name	Traffic descriptor name	Product	Configuration
Index	Traffic descriptor index	Product	Configuration

Vendor-Specific Inventory and IMOs

Vendor-specific IMOs are implemented only for specific vendor devices.

The following vendors' DSL Traffic Descriptor objects describe traffic of these vendors' standard DSL interfaces, and are aggregated by a [Traffic Descriptor Container](#) object.

- [ECI HiFocus ADSL Traffic Descriptor \(IECIHiFocusAdslTrafficDescriptor\)](#)
- [Alcatel ASAM SHDSL Traffic Descriptor \(IAlcatelAsamShdslTrafficProfile\)](#)

ECI HiFocus ADSL Traffic Descriptor

Table 28-9 *ECI HiFocus ADSL Traffic Descriptor (IECIHiFocusAdslTrafficDescriptor)*

Attribute Name	Attribute Description	Scheme	Polling Interval
Discrete Multi-Tone Coding Model	Discrete multitone coding model (<i>Null, discrMultiTone</i>)	Product	Configuration
ATUC Downstream and ATUR Upstream Usage	ATUC downstream and ATUR upstream usage (<i>Null, Yes, No</i>)	Product	Configuration
ATUC Downstream Fast and Interleave Check Bytes	ATUC downstream fast and interleave check bytes	Product	Configuration
ATUR Upstream Fast and Interleave Check Bytes	ATUR upstream fast and interleave check bytes	Product	Configuration
ATUC Downstream and ATUR Upstream Interleaved Depth	ATUC downstream and ATUR interleave depth (<i>Power of 2, 0, Non</i>)	Product	Configuration
ATUC Downstream and ATUR Upstream Code Word Length	ATUC downstream and ATUR upstream code word length in symbols per code word	Product	Configuration
Trellis Coded Modulation Option Usage	Trellis coded modulation option usage (<i>Null, Enabled, Disabled</i>)	Product	Configuration
Echo Cancellation Option	Echo cancellation option (<i>Null, Enabled, Disabled</i>)	Product	Configuration
Coding Mode	Coding mode (<i>Null, Automatic, Manual</i>)	Product	Configuration

All additional attributes are the same as [ADSL Traffic Descriptor \(IAdslTrafficDescriptor\)](#)

Alcatel ASAM SHDSL Traffic Descriptor

Table 28-10 *Alcatel ASAM SHDSL Traffic Descriptor (IAlcatelAsamShdslTrafficProfile)*

Attribute Name	Attribute Description	Scheme	Polling Interval
Minimum and Maximum Required Bit Rate	Minimum and maximum required bit rate	Product	Configuration

All additional attributes are the same as [Symmetric High Bit Rate DSL Traffic Descriptor \(IShdslTrafficDescriptor\)](#)

Network Topology

Cisco ANA does not support discovery of DSL physical layer topology. This topology is manually (statically) configured by the system administrator.

However, it is used in conjunction with the data link layer above it, such as ATM, for discovering its physical topology, while further verifying it by matching the traffic signature of these ports using Cisco's confidential scheme, which requires a substantial amount of traffic in order to function correctly.

Service Alarms

The following alarms are supported for this technology:

- [Link Down, page 41-42](#)
- [Port Down, page 41-51](#)



CHAPTER 29

SONET/SDH

This chapter describes the level of support that Cisco ANA provides for synchronous optical technology (SONET/SDH), as follows:

- [Technology Description, page 29-1](#)
- [Information Model Objects \(IMOs\), page 29-2](#)
- [Vendor-Specific Inventory and IMOs, page 29-5](#)
- [Network Topology, page 29-5](#)
- [Service Alarms, page 29-5](#)

Technology Description

Please see Part 1: Cisco VNEs in this guide for information about which devices support the various technologies.

SONET/SDH

SONET/SDH was originally standardized for connecting one fiber system to another at the optical level, to form a single international standard for fiber interconnects between telephone networks of different countries. Today it is a widely deployed, mature technology used in implementing high-speed, large-scale IP networks. It combines high bandwidth capacity with efficient link utilization, making it a major building block for accommodating fast-growing IP infrastructure both in the core and at the edge.

SONET/SDH can handle a variety of transmission rates and applications by defining a synchronous, flexible, optical hierarchy for carrying many signals of different capacities. This is accomplished using a byte-interleaved multiplexing scheme, which simplifies multiplexing and offers end-to-end network management. It is a layered protocol that defines four separate layers—Photonic, Section, Line, and Path—within the OSI physical layer (Layer 1).

SONET/SDH networks consist of path terminating elements (PTEs), which represent the physical layer interfaces; add/drop multiplexers (ADMs) or Digital Crossconnect Systems (DCSs); and regenerators interconnected by point-to-point SONET/SDH links called *sections*. These are fundamentally connection oriented, which means that a VC must be set up across the SONET/SDH network prior to any data transfer.

**Note**

This physical technology is supported only insofar as the underlying physical layer is supported in conjunction with other data link layer technologies, such as ATM and PoS.

Information Model Objects (IMOs)

This section describes the following IMOs:

- [SONET/SDH Physical \(ISonetSdh\)](#)
- [DS1 Channelized Interface \(IDS1PdhChannelized\)](#)
- [DS3 Channelized Interface \(IDS3PdhChannelized\)](#)
- [SONET SDH Hop \(ISonet_SdhHop\)](#)
- [SONET STS 1 \(ISonetSts1\)](#)
- [SDH AU 4 \(ISdhAu4\)](#)
- [SDH AU 3 \(ISdhAu3\)](#)

SONET/SDH Physical

The physical layer [SONET/SDH Physical](#) object is bound by its Containing Termination Points attribute to a [Port Connector](#) object. It is accessed primarily by the data link layer object, such as [Asynchronous Transfer Mode](#) and [Frame Relay](#) interfaces, as well as the PoS interface (implemented using [PPP Encapsulation](#)), bound by its Contained Connection Termination Points attribute.

Table 29-1 *SONET/SDH Physical (ISonetSdh)*

Attribute Name	Attribute Description	Scheme	Polling Interval
Specific Type	Specific type (<i>Null, SONET/SDH Mux, OC3, OC12, OC24, OC48, OC192, STM1, STM4, STM16, STM64</i>)	IPCore	Configuration
Loop Back Type	Loopback type (<i>Null, Cell, Payload, Diag, Line, None, Other, Path, Metallic, Non Metallic, Serial, Parallel, Local, Internal, Network, Inward, Dual, Remote, Inbound Local, No Loop, Facility Loop, Terminal Loop, Other Loop</i>)	IPCore	Configuration
Scrambling Mode	Scrambling mode (<i>Null, On, Off, Payload, Frame, Payload and Frame</i>)	IPCore	Configuration
TCAThresholdB1	The threshold for B1 threshold crossing alarms (B1-TCA). The value specifies a negative exponent to the power of 10 (10 to the power of minus value) for the threshold value, with a default value of 6 (10e-6).	IPCore	Configuration
TCAThresholdB2	The threshold for B2 threshold crossing alarms (B2-TCA). The value specifies a negative exponent to the power of 10 (10 to the power of minus value) for the threshold value, with a default value of 6 (10e-6).	IPCore	Configuration
TCAThresholdB3	The threshold for B3 threshold crossing alarms (B3-TCA). The value specifies a negative exponent to the power of 10 (10 to the power of minus value) for the threshold value, with a default value of 6 (10e-6).	IPCore	Configuration

Table 29-1 SONET/SDH Physical (ISonetSdh) (continued)

Attribute Name	Attribute Description	Scheme	Polling Interval
Clocking	The SONET port TX clock source where the internal keyword sets the internal clock (<i>line</i> , <i>internal</i>). The <i>line</i> keyword sets the clock recovered from the line (this is the default).	IPCore	Configuration

All additional attributes are the same as [Physical Layer \(IPhysicalLayer\)](#)

DS1 Channelized Interface

The physical layer [DS1 Channelized Interface](#) object represents a high-order SONET/SDH DS1 circuit.

Table 29-2 DS1 Channelized Interface (IDS1PdhChannelized)

Attribute Name	Attribute Description	Scheme	Polling Interval
Description	The description of the channelized DS1 PDH.	IPCore	Configuration
PathType	The type of SONET/SDH high-order interface.	IPCore	Configuration
Sts1OrAu4OrAu3Number	The STS1 number inside a channelized controller configured in SONET framing mode, or the AU4 or AU3 number inside a channelized controller configured in SDH framing mode	IPCore	Configuration
Tug3Number	The TUG-3 number inside a channelized controller configured in SDH framing mode	IPCore	Configuration
T3OrE3Number	The T3 or E3 number inside a channelized controller configured in SONET framing mode.	IPCore	Configuration
PortIps	An array of subinterfaces configured on top of this channelized DS1 PDH.	IPCore	Configuration

DS3 Channelized Interface

The physical layer [DS3 Channelized Interface](#) object represents a high-order SONET/SDH DS3 circuit.

Table 29-3 DS3 Channelized Interface (IDS3PdhChannelized)

Attribute Name	Attribute Description	Scheme	Polling Interval
Description	The description of the channelized DS3 PDH	IPCore	Configuration
PathType	The type of SONET/SDH high-order interface.	IPCore	Configuration
Sts1OrAu4OrAu3Number	The STS1 number inside a channelized controller configured in SONET framing mode, or the AU4 or AU3 number inside a channelized controller configured in SDH framing mode	IPCore	Configuration
Tug3Number	The TUG-3 number inside a channelized controller configured in SDH framing mode	IPCore	Configuration
T3OrE3Number	The T3 or E3 number inside a channelized controller configured in SONET framing mode.	IPCore	Configuration
PortIps	An array of subinterfaces configured on top of this channelized DS3 PDH.	IPCore	Configuration

SONET SDH Hop

The physical layer [SONET SDH Hop](#) object represents an interface on a high-order SONET/SDH circuit.

Table 29-4 *SONET SDH Hop (ISonet_SdhHop)*

Attribute Name	Attribute Description	Scheme	Polling Interval
Description	The description of the high-order SONET/SDH interface (for example, <i>STS1</i> , <i>AU4</i> , <i>AU3</i> , and so on)	IPCore	Configuration
AppliqueType	Indicates the lowest level channel type to which this interface will convert (for example, <i>DS1</i> , <i>E1</i> , and so on)	IPCore	Configuration
PathType	The type of high-order SONET/SDH circuit (for example, <i>STS1</i> , <i>AU4</i> , <i>AU3</i> , and so on)	IPCore	Configuration
Sts1OrAu4OrAu3Number	The STS1 number inside a channelized controller configured in SONET framing mode, or the AU4 or AU3 number inside a channelized controller configured in SDH framing mode	IPCore	Configuration

SONET STS 1

The physical layer [SONET STS 1](#) object represents an instance of an STS1 circuit.

Table 29-5 *SONET STS 1 (ISonetSts1)*

Attribute Name	Attribute Description	Scheme	Polling Interval
All attributes are the same as SONET SDH Hop (ISonet_SdhHop)			

SDH AU 4

The physical layer [SDH AU 4](#) object represents an instance of an AU4 circuit.

Table 29-6 *SDH AU 4 (ISdhAu4)*

Attribute Name	Attribute Description	Scheme	Polling Interval
All attributes are the same as SONET SDH Hop (ISonet_SdhHop)			

SDH AU 3

The physical layer [SDH AU 3](#) object represents an instance of an AU3 circuit.

Table 29-7 *SDH AU 3 (ISdhAu3)*

Attribute Name	Attribute Description	Scheme	Polling Interval
All attributes are the same as SONET SDH Hop (ISonet_SdhHop)			

Vendor-Specific Inventory and IMOs

There are no vendor-specific inventory or IMOs for this technology.

Network Topology

Cisco ANA does not support discovery of SONET/SDH physical layer topology. This topology is manually (statically) configured by the system administrator.

However, it is used in conjunction with the data link layer above it, such as ATM, for discovering its physical topology, while further verifying it by matching the traffic signature of these ports using Cisco's confidential scheme, which requires a substantial amount of traffic in order to function correctly.

Service Alarms

The following alarms are supported for this technology:

- [Discard Packets, page 41-26](#)
- [Dropped Packets, page 41-27](#)
- [Link Down, page 41-42](#)
- [Port Down, page 41-51](#)
- [Rx Utilization, page 41-53](#)
- [Tx Utilization, page 41-57](#)
- [DS1 Path Port Down, page 41-29](#)
- [DS1 Path Link Down, page 41-28](#)
- [DS3 Path Port Down, page 41-30](#)
- [DS3 Path Link Down, page 41-29](#)
- [SONET Path Port Down, page 41-55](#)
- [SONET Path Link Down, page 41-54](#)



CHAPTER 30

Internet Protocol Over Dense Wave Division Multiplexing

This chapter describes the level of support that Cisco ANA provides for IPoDWDM, as follows:

- [Technology Description, page 30-1](#)
- [Information Model Objects \(IMOs\), page 30-2](#)
- [Vendor-Specific Inventory and IMOs, page 30-4](#)
- [Network Topology, page 30-4](#)
- [Service Alarms, page 30-4](#)

Technology Description

Please see Part 1: Cisco VNEs in this guide for information about which devices support the various technologies.

IPoDWDM

IPoDWDM is a network architecture approach that integrates layer 1 (optical) and layer 3 (IP) technologies by combining DWDM transponder features and functions into the router interface. Instead of being limited to a short-reach gray wavelength, the router is able to emit a tunable, ITU-grid compatible colored wavelength, with G.709 Digital Wrapper and Enhanced Forward Error Correction (EFEC) functions. This combination provides multiple advantages, including savings in capital and operational expenditures due to the elimination of multiple transponder shelves, cross-connect shelves, and associated short-reach interfaces. The total number of optical-electronic components is reduced by 50 percent, further lowering costs, improving availability, lowering the time needed to provision services on the network, and increasing mean time between failures (MTBF). It also halves the number of patch cables needed at the terminating sites, reduces power consumption, and shrinks the overall physical footprint of the equipment.



Note

Cisco ANA version 3.6.6 and later provides support for IPoDWDM only on CRS-1 devices running IOS-XR software.

Information Model Objects (IMOs)

This section describes the following IMOs:

- [DWDM Interface](#)
- [DWDM G709 Information](#)
- [DWDM PM Settings](#)

DWDM Interface

The [DWDM Interface](#) object represents a DWDM controller physical termination point. It is accessed by the [Module](#) containing it.

Table 30-1 *DWDM Interface (IDWDM)*

Attribute Name	Attribute Description	Scheme	Polling Interval
Location	Indicates the port location on which the controller resides. It is the postfix of the Physical Port which has this DWDM controller.	IPCore	Configuration
Loopback	Transponder loopback setting (<i>none, internal, line</i>).	IPCore	Configuration
ControllerStatus	Status of the controller status (<i>up, down</i>).	IPCore	Configuration
WavelengthBand	Indicates the wavelength band (<i>C-band, L-band</i>).	IPCore	Configuration
Channel	The Multisource Agreement (MSA) ITU channel number. The ITU channel number is an integer from 1 to 83 (for the C-band) or from 106 to 185 (for the L-band).	IPCore	Configuration
Frequency	Frequency of the channel, in terahertz.	IPCore	Configuration
Wavelength	Wavelength corresponding to the channel number, in nanometers.	IPCore	Configuration
OpticsType	Indicates the optics type of the DWDM controller (<i>DWDM, Cisco 10Gb DWDM, LR-2/L-64.2a (80km), 10Gb MSA WDM (65km)</i> , and so on).	IPCore	Configuration
TxPower	Transmit power level. Values are in units of 0.1 dBm and can range from -190 to +10. This corresponds to a range of -19 dBm to +1 dBm.	IPCore	Configuration
RxPower	Receive power level. Values are in units of 0.1 dBm and can range from -200 to 0. This corresponds to a range of -20 dBm to 0 dBm.	IPCore	Configuration
RxLosThreshold	Indicates the transponder receive power LOS threshold value (in units of 0.1dBm).	IPCore	Configuration
G709Info	The raw string output value of G709 status, as retrieved using the command line interface (CLI).	IPCore	Configuration
PMSettings	An array of one or more instances of DWDM PM Settings objects	IPCore	Configuration

DWDM G709 Information

The [DWDM G709 Information](#) object represents the G709 wrapper data for a [DWDM Interface](#) on a DWDM controller.

Table 30-2 *DWDM G709 Information (IDwdmG709Info)*

Attribute Name	Attribute Description	Scheme	Polling Interval
Location	The location of the DWDM controller.	IPCore	Configuration
Status	The administrative status of the DWDM controller.	IPCore	Configuration
OTUAlarmCounters	A list of OTU alarm counters. Each entry has a counter value and an alarm type (<i>AIS, BDI, BEI, BIP, FECMISMATCH, IAE, LOF, LOM, LOS, TIM</i>).	IPCore	Configuration
ODUAlarmCounters	A list of ODU alarm counters. Each entry has a counter value and an alarm type (<i>AIS, BDI, BEI, BIP, LCK, OCI, PTIM, TIM</i>).	IPCore	Configuration
OTUAlarmReporting	A list of OTU alarm types in the DWDM controller which are enabled to report in the command line interface (CLI).	IPCore	Configuration
ODUAlarmReporting	A list of ODU alarm types in the DWDM controller which are enabled to report in the CLI.	IPCore	Configuration
OTUAssertedAlarms	A list of asserted OTU alarm types in the DWDM controller.	IPCore	Configuration
ODUAssertedAlarms	A list of asserted ODU alarm types in the DWDM controller.	IPCore	Configuration
OTUDetectedAlarms	A list of detected OTU alarm types in the DWDM controller.	IPCore	Configuration
ODUDetectedAlarms	A list of detected ODU alarm types in the DWDM controller.	IPCore	Configuration
OTUAlertCounters	A list of OTU alert counters. Each entry has a counter value and an alarm type (<i>SD_BER, SF_BER, PM_TCA, SM_TCA</i>).	IPCore	Configuration
OTUAlertReporting	A list of OTU alert types in the DWDM controller which are enabled to report in CLI.	IPCore	Configuration
OTUAssertedAlerts	A list of asserted OTU alert types in the DWDM controller.	IPCore	Configuration
OTUDetectedAlerts	A list of detected OTU alert types in the DWDM controller.	IPCore	Configuration
ODUAlertCounters	A list of ODU alert counters. Each entry has a counter value and an alarm type (<i>D_BER, SF_BER, PM_TCA, SM_TCA</i>).	IPCore	Configuration
ODUAlertReporting	A list of ODU alert types in the DWDM controller which are enabled to report in CLI.	IPCore	Configuration
ODUAssertedAlerts	A list of asserted ODU alert types in the DWDM controller.	IPCore	Configuration
ODUDetectedAlerts	A list of detected ODU alert types in the DWDM controller.	IPCore	Configuration
OTUTTI	The OTU trail trace identifier. It contains the TTI type (<i>SENT, EXPECTED, RECEIVED</i>), the stringType (<i>ASCII, HEX</i>), and the string value.	IPCore	Configuration
ODUTTI	The ODU trail trace identifier.	IPCore	Configuration
FECInfo	The FEC data in the G709 wrapper. It contains the FECMode, RemoteFECMode, ecTCA, ucTCA, ecCounter, and ucCounter.	IPCore	Configuration

DWDM PM Settings

The [DWDM PM Settings](#) object contains the PM setting for the threshold crossing alarm (TCA) values and the threshold values on a DWDM controller.

Table 30-3 DWDM PM Settings (*IDwdmPmSettings*)

Attribute Name	Attribute Description	Scheme	Polling Interval
Location	The Location of the DWDM controller.	IPCore	Configuration
IntervalType	The sampling interval type (<i>15_min</i> , <i>24_hour</i>).	IPCore	Configuration
FECPMSettings	The FEC type (<i>EC-BITS</i> , <i>UC_WORDS</i>), TCA, and threshold values.	IPCore	Configuration
OpticsPMSettings	The optics PM type (<i>LBC</i> , <i>OPR</i> , <i>OPT</i>), maxTCA, minTCA, maxThreshold, minThreshold, and thresholdUnit.	IPCore	Configuration
OTNPmSettings	The OTN PM type, TCA, and threshold value. Possible values of the OTN PM type are <i>BBE_PM_FE</i> , <i>BBE_PM_NE</i> , <i>BBE_SM_FE</i> , <i>BBE_SM_NE</i> , <i>BBER_PM_FE</i> , <i>BBER_PM_NE</i> , <i>BBER_SM_FE</i> , <i>BBER_SM_NE</i> , <i>ES_PM_FE</i> , <i>ES_PM_NE</i> , <i>ES_SM_FE</i> , <i>ES_SM_NE</i> , <i>ESR_PM_FE</i> , <i>ESR_PM_NE</i> , <i>ESR_SM_FE</i> , <i>ESR_SM_NE</i> , <i>FC_PM_FE</i> , <i>FC_PM_NE</i> , <i>FC_SM_FE</i> , <i>FC_SM_NE</i> , <i>SES_PM_FE</i> , <i>SES_PM_NE</i> , <i>SES_SM_FE</i> , <i>SES_SM_NE</i> , <i>SESR_PM_FE</i> , <i>SESR_PM_NE</i> , <i>SESR_SM_FE</i> , <i>SESR_SM_NE</i> , <i>UAS_PM_FE</i> , <i>UAS_PM_NE</i> , <i>UAS_SM_FE</i> , <i>UAS_SM_NE</i> .	IPCore	Configuration

Vendor-Specific Inventory and IMOs

There are no vendor-specific inventory or IMOs for this technology. Currently, only the Cisco CRS-1 device running IOS-XR is supported.

Network Topology

There is no network topology to be discovered specifically for IPoDWDM. The command line interface (CLI) is used to discover physical inventory attributes for DWDM controllers in the chassis. Cisco ANA models them as it does other physical ports.

Service Alarms

The following alarms are supported for this technology:

- [DWDM Controller Down](#), page 41-31
- [DWDM G709 Status Down](#), page 41-32



CHAPTER 31

TDM/DSx

This chapter describes the level of support that Cisco ANA provides for time-division multiplexing (TDM), Digital Signal (DSx) Hierarchy, and related physical technologies, as follows:

- [Technology Description, page 31-1](#)
- [Information Model Objects \(IMOs\), page 31-2](#)
- [Vendor-Specific Inventory and IMOs, page 31-5](#)
- [Network Topology, page 31-5](#)
- [Service Alarms, page 31-5](#)

Technology Description

This section provides the following TDM/DSx technology descriptions:

- [TDM](#)
- [DSx](#)
- [T3/E3](#)
- [Channelized T3, OC3, DS3 Interface](#)
- [Circuit Emulation over MPLS](#)

Please see Part 1: Cisco VNEs in this guide for information about which devices support the various technologies.

TDM

Time-Division Multiplexing (TDM) is a type of digital multiplexing in which two or more signals or bit streams are transferred apparently as subchannels in one communication channel. The transmission of these streams appears to be simultaneous, but they are actually taking turns on the channel. This is done by dividing the transmission time domain into several recurrent slots of fixed length, one for each subchannel. A sample byte or data block of subchannel 1 is transmitted during timeslot 1, subchannel 2 during timeslot 2, and so on. One TDM frame consists of one timeslot per subchannel. After the last subchannel, the cycle starts again with a new frame, starting with the second sample, byte or data block from subchannel 1, and so on.

DSx

Digital Signal (DSx) Hierarchy refers to the rate and format of digital telecommunication circuits, as part of the North American Digital Hierarchy. DSx is related to the T-carrier designations. However, DS refers to multiplexing techniques, while the T designations refer to the underlying equipment and signaling. There are various DS levels, the most common being:

- DS0/Fractional T1 (64 Kb/s), which represents a single voice telephone call.
- DS1/T1 (1.544 Mb/s), with 24 user channels.
- DS2/T2 (6.312 Mb/s), with 96 user channels.
- DS3/T3 (44.736 Mb/s), with 672 user channels.

T3/E3

T-carrier telecommunications is a generic name for several digitally multiplexed telecommunications carrier systems used in North America, Japan, and Korea. The basic unit of the T-carrier system is the Fractional T1, which corresponds to the Digital Signal Hierarchy's DS0, and is commonly used for one voice circuit.

The E-carrier system (the "E" stands for "European") is incompatible with the T-carrier system (though cross-compliant cards exist). It is in common use everywhere outside of North America, Japan, and Korea. It typically uses the E1 (2.048 Mb/s) and E (334.368 Mb/s) line rates.

Channelized T3, OC3, DS3 Interface

Channelization, coupled with native edge-aggregation services such as MPLS and QoS, allows service providers and large enterprises to save dramatically on power, floor space, local-loop charges, and equipment costs, by permitting receipt and transmission of multiplexed T3, OC3 and DS 3 circuits over high-bandwidth physical media.

Circuit Emulation over MPLS

In CEM, TDM bitstream connections (T1, E1, T3, E3) are encapsulated as pseudowires over the MPLS backbone. Both structured and structure-agnostic TDM bitstreams are supported.

Information Model Objects (IMOs)

This section describes the following IMOs:

- [DS0 Bundle Interface \(IDS0Bundle\)](#)
- [DS1 Physical \(IDS1Pdh\)](#)
- [DS3 Physical \(IDS3Pdh\)](#)

DS0 Bundle Interface

The data link layer [DS0 Bundle Interface](#) object is bound by its Containing Termination Points attribute to either [DS1 Physical](#) or [DS3 Physical](#) Layer objects. It is accessed primarily by the data link layer object, such as the [ATM Interface](#) and the [Frame Relay Interface](#), bound by its Contained Connection Termination Points attribute.

Table 31-1 *DS0 Bundle Interface (IDS0Bundle)*

Attribute Name	Attribute Description	Scheme	Polling Interval
Bundled Time Slots	Bundled time slots (DS1 channels).	Product	Configuration
Bundle Location	Bundle location/index.	Product	Configuration
AdminStatus	The administrative status of the interface (<i>Down, Testing, Up</i>).	IPCore	Configuration
OperStatus	The operational status of the interface (<i>Down, Testing, Up</i>).	IPCore	Configuration
IANA Type	Internet Assigned Numbers Authority (IANA) type of the sublayer.	N/A	N/A
Containing Termination Points	Underlying termination points (connection or physical).	Product	N/A
Contained Connection Termination Points	Bound connection termination points.	Product	N/A

DS1 Physical

The physical layer [DS1 Physical](#) and [DS3 Physical](#) objects are bound by their Containing Termination Points attribute to a [Port Connector](#) object. Each of these objects is accessed primarily by the data link layer object (such as an [ATM Interface](#), [Frame Relay Interface](#), or [DS0 Bundle Interface](#)) bound by its Contained Connection Termination Points attribute.

Table 31-2 *DS1 Physical (IDS1Pdh)*

Attribute Name	Attribute Description	Scheme	Polling Interval
Framing Type	Framing type (<i>Null, OTHER, ESF, ANSI ESFf, D4, E1, E1 CRC, E1 MF, E1 CRC MF, UNFRAMED, E1 UNFRAMED, DS2 M12, E2, E1 Q50, E1 Q50 CRC, ANSI SF, E1 CAS CRC4, E1 CAS No CRC4, E1 No CAS CRC4, E1 No CAS No CRC4, E1 Unstructured, T1 Unstructured, CLEAR CHANNEL</i>).	Product	Configuration
Cell Mapping Type	Cell mapping type (<i>Null, PLCP, HEC, HCS, Direct, ADM</i>).	Product	Configuration
Loop Back Type	Loopback type (<i>Null, Cell, Payload, Diag, Line, None, Other, Path, Metallic, Non Metallic, Serial, Parallel, Local, Internal, Network, Inward, Dual, Remote, Inbound Local, No Loop</i>).	Product	Configuration
Scrambling Mode	Scrambling mode (<i>Null, On, Off</i>).	Product	Configuration
Port Description	Port description.	Product	Configuration
International Bit	Indicates whether the E3 international bit is set.	Product	Configuration
Line Code	Line-code type for T1 or E1 lines (<i>ami, b8zs, hdb3</i>).	Product	Configuration
Cable Length	Set cable length.	Product	Configuration
Recovered Clocking ID	Recovered clocking ID.	Product	Configuration

Table 31-2 DS1 Physical (IDS1Pdh) (continued)

Attribute Name	Attribute Description	Scheme	Polling Interval
Clocking	Clocking type (<i>stratum1</i> , and so on).	Product	Configuration
Loopback	Transponder loopback setting (<i>none</i> , <i>internal</i> , <i>line</i>).	Product	Configuration

All additional attributes are the same as [Physical Layer \(IPhysicalLayer\)](#)

DS3 Physical

Table 31-3 DS3 Physical (IDS3Pdh)

Attribute Name	Attribute Description	Scheme	Polling Interval
Framing Type	Framing type (<i>Null</i> , <i>Other</i> , <i>M23</i> , <i>SYNTRAN</i> , <i>CBIT</i> , <i>Clear Channel</i> , <i>E3 Other</i> , <i>E3 Framed</i> , <i>Unframed</i> , <i>E3 Unframed</i> , <i>ITU-T G.804</i> , <i>ITU-T G.832</i> , <i>M13</i>).	Product	Configuration
Cell Mapping Type	Cell mapping type (<i>Null</i> , <i>PLCP</i> , <i>HEC</i> , <i>HCS</i> , <i>Direct</i> , <i>ADM</i>).	Product	Configuration
Loop Back Type	Loopback type (<i>Null</i> , <i>Cell</i> , <i>Payload</i> , <i>Diag</i> , <i>Line</i> , <i>None</i> , <i>Other</i> , <i>Path</i> , <i>Metalic</i> , <i>Non Metalic</i> , <i>Serial</i> , <i>Parallel</i> , <i>Local</i> , <i>Internal</i> , <i>Network</i> , <i>Inward</i> , <i>Dual</i> , <i>Remote</i> , <i>Inbound Local</i> , <i>No Loop</i>).	Product	Configuration
Scrambling Mode	Scrambling mode (<i>Null</i> , <i>On</i> , <i>Off</i>).	Product	Configuration
Port Description	Port description.	Product	Configuration
International Bit	Indicates whether the E3 international bit is set.	Product	Configuration
Line Code	Line-code type for T1 or E1 lines (<i>ami</i> , <i>b8zs</i> , <i>hdb3</i>).	Product	Configuration
Cable Length	Set cable length.	Product	Configuration
Recovered Clocking ID	Recovered clocking ID.	Product	Configuration
Clocking	Clocking type (<i>stratum1</i> , and so on).	Product	Configuration
Loopback	Transponder loopback setting (<i>none</i> , <i>internal</i> , <i>line</i>).	Product	Configuration

All additional attributes are the same as [Physical Layer \(IPhysicalLayer\)](#)

Vendor-Specific Inventory and IMOs

There are no vendor-specific inventory or IMOs for this technology.

Network Topology

Cisco ANA does not support discovery of physical layer topology. This topology is manually (statically) configured by the system administrator. However, it is used in conjunction with the data link layer above it, such as ATM, for discovering its physical topology, while further verifying it by matching the traffic signature of these ports using Cisco's confidential scheme, which requires a substantial amount of traffic in order to function correctly.

Service Alarms

The following alarms are supported for this technology:

- [Discard Packets, page 41-26](#)
- [Dropped Packets, page 41-27](#)
- [Link Down, page 41-42](#)
- [Port Down, page 41-51](#)
- [Rx Utilization, page 41-53](#)
- [Tx Utilization, page 41-57](#)
- [DS0 Bundle Service Alarm, page 41-28](#)



CHAPTER 32

Clocking

This chapter describes the level of support that Cisco ANA provides for clocking, as follows:

- [Technology Description, page 32-1](#)
- [Information Model Objects \(IMOs\), page 32-2](#)
- [Vendor-Specific Inventory and IMOs, page 32-9](#)
- [Network Topology, page 32-9](#)
- [Service Alarms, page 32-9](#)

Technology Description

This section provides the following Clocking technology descriptions:

- [1588 Clocking](#)
- [SyncE Clocking](#)
- [Adaptive Clock Recovery \(ACR\)](#)

Please see Part 1: Cisco VNEs in this guide for information about which devices support the various technologies.

1588 Clocking

TDM 1588 is known as Precision Time Protocol (PTP). The PTP standard specifies a clock synchronization protocol applicable to distributed systems consisting of one or more nodes communicating over a network. Nodes are modeled as containing a real-time clock that may be used by applications within the node for various purposes, such as generating time stamps for data or ordering events managed by the node. The protocol provides a mechanism for synchronizing the clocks of participating nodes to a high degree of accuracy and precision.

SyncE Clocking

One of the fundamental requirements placed on next-generation networks is to provide the ability to distribute precision frequency or timing synchronization around the network. Frequency synchronization is provided by SONET/SDH equipment, used in conjunction with external timing technology, such as Cesium oscillators and GPS.

As SONET/SDH equipment is replaced by Ethernet equipment, this frequency synchronization ability is required over Ethernet ports. Synchronous Ethernet (SyncE) provides SONET/SDH physical layer (POS-PHY) frequency distribution of known, common precision frequency references.

To maintain SyncE links, a set of operations messages is required. These messages provide information about the quality of the timing source being used to clock the SyncE link, ensuring that each node is always deriving timing from the most reliable source. In SONET/SDH networks, these messages are known as Synchronization Status Messages (SSM). Each timing source has a Quality Level (QL) associated with it, which gives the accuracy of the clock. This QL information is transmitted across the network via SSMs over the Ethernet Synchronization Messaging Channel (ESMC), or via SSMs contained in the SONET/SDH frames, so that devices can know the best available source with which to synchronize. To define a preferred network synchronization flow and help prevent timing loops, users can assign priority values to particular timing sources on each router. The combination of QL information and user-assigned priority levels allows each router to choose a timing source to clock its SyncE and SONET/SDH interfaces.

**Note**

Cisco ANA supports these technologies only in conjunction with data link layer technologies, such as ATM or PoS.

Adaptive Clock Recovery (ACR)

ACR is an averaging process that negates the effect of random packet delay variation and captures the average rate of transmission of the original bit stream.

Information Model Objects (IMOs)

This section describes the following IMOs:

- [CEM Interface \(ICEMEncap\)](#)
- [CEM Group \(ICEMGroup\)](#)
- [Clock Service \(IClockService\)](#)
- [Clock Source \(IClockSource\)](#)
- [PTP Service \(IPtpService\)](#)
- [PTP Interface \(IPtpInterface\)](#)
- [ACR Service \(IACRService\)](#)
- [Recovered Clock \(IRecoveredClock\)](#)
- [SyncE Service \(ISyncE\)](#)
- [SyncE Interface \(ISyncEInterface\)](#)

CEM Interface

The [CEM Interface](#) object represents a CEM-encapsulated E1/T1 circuit interface.

Table 32-1 *CEM Interface (ICEMEncap)*

Attribute Name	Attribute Description	Scheme	Polling Interval
cemIfName	The interface name (for example, <i>CEM8/0/0</i> or <i>Virtual-cem8/0/24</i>).	IPCore	Configuration

CEM Group

The [CEM Group](#) object represents a CEM Group configured on a physical or virtual [CEM Interface](#).

Table 32-2 CEM Group (ICEMGroup)

Attribute Name	Attribute Description	Scheme	Polling Interval
ID	The DS0 bundle CEM group identifier.	IPCore	Configuration
IdlePattern	The 8-bit hexadecimal number that is transmitted on a T1 or E1 line when missing packets are detected on the PW circuit.	IPCore	Configuration
IdleCAS	When channel associated signaling (CAS) is used, the 8-bit hexadecimal signal that is sent when the CEM interface is identified as idle.	IPCore	Configuration
DeJitter	The size of the dejitter buffer in milliseconds (ms) (in the range 4-500, 4 is the default).	IPCore	Configuration
PayloadSize	The size of the payload (in bytes) for packets on the CEM interface (in the range 32-1312).	IPCore	Configuration
RTP	Indicates whether RTP compression is <i>enabled</i> or <i>disabled</i> .	IPCore	Configuration
RTPHeader	Indicates whether RTP header compression is <i>enabled</i> or <i>disabled</i> .	IPCore	Configuration
TimeSlots	The range of timeslots (DS0 channels) allotted to the CEM interface. Empty if the Structure-Agnostic TDM over Packet (SAToP) method is used.	IPCore	Configuration
Pseudowire	The name of the pseudowire configured on the CEM interface.	IPCore	Configuration
AdminStatus	The administrative status of the CEM interface (<i>Down</i> , <i>Testing</i> , <i>Unknown</i> , <i>Up</i>).	IPCore	Configuration
OperStatus	The operational status of the CEM interface (<i>Dormant</i> , <i>Down</i> , <i>Not Present</i> , <i>Testing</i> , <i>Unknown</i> , <i>Up</i>).	IPCore	Configuration

Clock Service

The [Clock Service](#) object models the generic clocking configuration and clocking features of a network element, independent of any particular timing scheme, such as PTP or Anonymous Call Rejection (ACR).

Table 32-3 Clock Service (IClockService)

Attribute Name	Attribute Description	Scheme	Polling Interval
ActiveClockSource	The current active clock source used by the network element.	Any	Configuration
NcsMode	The network clock selection mode (<i>revert</i> , <i>nonrevert</i> , <i>unknown</i>). NCS is used in case of master device failure.	Any	Configuration
HoldTimeout	The network clock selection hold timeout in seconds (in the range 0-86400, -1 for no timeout).	Any	Configuration
UseStratum4	Indicates whether the Stratum4 clock is used (<i>true</i>) or not (<i>false</i>). The default is <i>false</i> , which means the Stratum3 clock is used.	Any	Configuration
Mode	The network element clocking mode (<i>unknown</i> , <i>slave</i> , <i>master</i> , <i>hybrid</i>).	Any	Configuration
NcsPriorityList	The network clock selection priority list.	Any	Configuration

Table 32-3 Clock Service (*IClockService*) (continued)

Attribute Name	Attribute Description	Scheme	Polling Interval
Pseudowire Clock Recovery	An array of zero or more instances of ACR Service (IACRService) .	Any	Configuration
PtpService	An array of zero or more instances of PTP Service (IPtpService) .	Any	Configuration

Clock Source

The [Clock Source](#) object represents the network clock source defined in an instance of the [Clock Service](#) object.

Table 32-4 Clock Source (*IClockSource*)

Attribute Name	Attribute Description	Scheme	Polling Interval
Priority	The priority of the defined clock source.	Any	Configuration
Source	The clock source.	Any	Configuration
Status	Indicates that the clock source status is valid (<i>true</i>) or non existent/non functional (<i>false</i>).	Any	Configuration
Type	The clock source type (<i>BITS</i> , <i>packet-timing</i> , <i>sync</i> , <i>E1/T1</i>).	Any	Configuration

PTP Service

The [PTP Service](#) object represents PTP (IEEE-1588) configurations on a network element at the device level.

Table 32-5 PTP Service (*IPtpService*)

Attribute Name	Attribute Description	Scheme	Polling Interval
Mode	The PTP operating mode (<i>unknown</i> , <i>ordinary</i> , <i>boundary</i> , <i>e2transparent</i> , <i>p2pttransparent</i>). On the Cisco MWR-2941, only <i>ordinary</i> is supported.	Any	Configuration
ClockId	The PTP clock ID.	Any	Configuration
Domain	The PTP domain ID (in the range 0 to 127).	Any	Configuration
Priority1	PTP clock selection priority-1 (in the range 0 to 255).	Any	Configuration
Priority2	PTP clock selection priority-2 (in the range 0 to 255).	Any	Configuration
PtpEnabled	Indicates whether PTP is enabled (<i>true</i>) or disabled (<i>false</i>).	Any	Configuration
PtpInterfaceList	An array of one or more instances of PTP Interface (IPtpInterface)	Any	Configuration

PTP Interface

The [PTP Interface](#) object represents PTP (IEEE-1588) configurations on a network element at the interface level.

Table 32-6 *PTP Interface (IPtpInterface)*

Attribute Name	Attribute Description	Scheme	Polling Interval
Version	The PTP version (default is 2).	Any	Configuration
AnnounceInterval	The PTP interface announce interval (in the range 0 to 4)	Any	Configuration
AnnounceTimeout	The PTP interface announce timeout (in the range 2 to 10).	Any	Configuration
DestinationAddress	The clock destination IP address (can be <i>null</i> , set only when in Master mode).	Any	Configuration
SourceAddress	The clock source IP address (can be <i>null</i> , set only when in Slave mode).	Any	Configuration
DelayReq	The PTP interface delay request message interval.	Any	Configuration
MasterMode	The PTP communication mode in Master mode (<i>notset</i> , <i>multicast</i> , <i>unicast</i> , <i>unicastnegotiation</i>).	Any	Configuration
SlaveMode	The PTP communication mode in Slave mode (<i>notset</i> , <i>multicast</i> , <i>unicast</i> , <i>unicastnegotiation</i>).	Any	Configuration
SyncInterval	The PTP interface sync interval.	Any	Configuration
SyncLimit	The PTP interface maximum offset (in the range 1000 to 50000).	Any	Configuration
InterfaceXid	The XID of the associated interface.	Any	Configuration

ACR Service

The [ACR Service](#) object represents the pseudowire clock recovery.

Table 32-7 *ACR Service (IACRService)*

Attribute Name	Attribute Description	Scheme	Polling Interval
RecoveredClockSource	The interface (slot or subslot) on which the clock recovery will occur.	Any	Configuration
RecoveredClockMode	The recovered clock mode.	Any	Configuration
CemInterface	The corresponding CEM or Virtual CEM interface instance ID.	Any	Configuration
RecoveredClockList	An array of one or more instances of Recovered Clock (IRecoveredClock) .	Any	Configuration

Recovered Clock

The [Recovered Clock](#) object represents the clock information derived from the RNC or from other n-PE, P, or u-PE devices.

Table 32-8 **Recovered Clock (*IRecoveredClock*)**

Attribute Name	Attribute Description	Scheme	Polling Interval
ClockId	The clock ID.	Any	Configuration
RecoveredClockMode	The recovered clock mode.	Any	Configuration
Port	The port number.	Any	Configuration
Cem	The CEM Group.	Any	Configuration
Status	The priority.	Any	Configuration
FrequencyOffset	The value of the frequency offset.	Any	Configuration

SyncE Service

The [SyncE Service](#) object represents the global Synchronous Ethernet configuration for a network element.

Table 32-9 **SyncE Service (*ISyncE*)**

Attribute Name	Attribute Description	Scheme	Polling Interval
synchronousMode	Enable automatic synchronization selection process.	Any	Configuration
equipmentClock	Indicates the currently selected Ethernet Equipment Clock option (EEC-Option I, EEC-Option II).	Any	Configuration
clockMode	Indicates whether Quality Level is enabled (<i>QL-Disable</i> , <i>QL-Enable</i>).	Any	Configuration
ssmOption	Indicates which of the Synchronization Status Messages (SSM) options is currently in use on the NE (<i>ITU-T Option I</i> , <i>ITU-T Option II generation 1</i> , <i>ITU-T Option II generation 2</i>).	Any	Configuration
esmcMode	Indicates whether Ethernet Synchronization Messaging Channel is enabled on the NE (<i>true</i>) or not (<i>false</i>).	Any	Configuration
holdOffTimer	The amount of time (in milliseconds) the NE waits before removing a source that has gone down (values in the range 0 to 50000, default is 300).	Any	Configuration
waitToRestore	The amount of time (in milliseconds) the NE waits before adding a source that has just come up (values in the range 0 to 86400).	Any	Configuration
Revertive	Indicates whether Revertive mode is enabled (<i>true</i>) or disabled (<i>false</i>) on the NE.	Any	Configuration

SyncE Interface

The [SyncE Interface](#) object represents the Synchronous Ethernet configuration for a single interface on an NE.

Table 32-10 *SyncE Interface (ISyncEInterface)*

Attribute Name	Attribute Description	Scheme	Polling Interval
selectionInput	Assign the interface as a timing source to be passed to the selection algorithm.	Any	Configuration
ingressESMCMode	Indicates whether Ethernet Synchronization Messaging Channel is enabled (<i>true</i>) or disabled (<i>false</i>) for incoming QL information on the interface.	Any	Configuration
egressESMCMode	Indicates whether Ethernet Synchronization Messaging Channel is enabled (<i>true</i>) or disabled (<i>false</i>) for outgoing QL information on the interface.	Any	Configuration
ingressQLMode	Indicates whether incoming quality level information is enabled (<i>true</i>) or disabled (<i>false</i>) on the interface.	Any	Configuration
ingressQuality	Indicates the type of incoming quality level information, depending on the globally configured SSM option. For <i>ITU-T Option I</i> , available values are <i>QL-PRC</i> , <i>QL-SSU-A</i> , <i>QL-SSU-B</i> , <i>QL-SEC</i> , and <i>QL-DNU</i> . For <i>ITU-T Option II generation 1</i> , available values are <i>QL-PRS</i> , <i>QL-STU</i> , <i>QL-ST2</i> , <i>QL-SMC</i> , <i>QL-ST4</i> , <i>QL-DUS</i> . For <i>ITU-T Option II generation 2</i> , available values are <i>QL-PRS</i> , <i>QL-STU</i> , <i>QL-ST2</i> , <i>QL-TNC</i> , <i>QL-ST3</i> , <i>QL-SMC</i> , <i>QL-ST4</i> , <i>QL-DUS</i> .	Any	Configuration
egressQLMode	Indicates whether incoming quality level information is enabled (<i>true</i>) or disabled (<i>false</i>) on the interface.	Any	Configuration
egressQuality	Indicates the type of outgoing quality level information, depending on the globally configured SSM option. For <i>ITU-T Option I</i> , available values are <i>QL-PRC</i> , <i>QL-SSU-A</i> , <i>QL-SSU-B</i> , <i>QL-SEC</i> , and <i>QL-DNU</i> . For <i>ITU-T Option II generation 1</i> , available values are <i>QL-PRS</i> , <i>QL-STU</i> , <i>QL-ST2</i> , <i>QL-SMC</i> , <i>QL-ST4</i> , <i>QL-DUS</i> . For <i>ITU-T Option II generation 2</i> , available values are <i>QL-PRS</i> , <i>QL-STU</i> , <i>QL-ST2</i> , <i>QL-TNC</i> , <i>QL-ST3</i> , <i>QL-SMC</i> , <i>QL-ST4</i> , <i>QL-DUS</i> .	Any	Configuration
waitToRestore	The amount of time (in milliseconds) the interface waits before adding a source that has just come up (values in the range 0 to 86400).	Any	Configuration
holdOffTimer	The amount of time (in milliseconds) the interface waits before removing a source that has gone down (values in the range 0 to 50000, default is 300).	Any	Configuration

Vendor-Specific Inventory and IMOs

There are no vendor-specific inventory or IMOs for this technology.

Network Topology

Cisco ANA does not support discovery of physical layer topology. This topology is manually (statically) configured by the system administrator. However, it is used in conjunction with the data link layer above it, such as ATM, for discovering its physical topology, while further verifying it by matching the traffic signature of these ports using Cisco's confidential scheme, which requires a substantial amount of traffic in order to function correctly.

Service Alarms

The following alarms are supported for this technology:

- [Discard Packets, page 41-26](#)
- [Dropped Packets, page 41-27](#)
- [Link Down, page 41-42](#)
- [Port Down, page 41-51](#)
- [Rx Utilization, page 41-53](#)
- [Tx Utilization, page 41-57](#)
- [DS0 Bundle Service Alarm, page 41-28](#)



CHAPTER 33

Serial

This chapter describes the level of support that Cisco ANA provides for serial links, as follows:

- [Technology Description, page 33-1](#)
- [Information Model Objects \(IMOs\), page 33-2](#)
- [Vendor-Specific Inventory and IMOs, page 33-2](#)
- [Network Topology, page 33-2](#)
- [Service Alarms, page 33-2](#)

Technology Description

Please see Part 1: Cisco VNEs in this guide for information about which devices support the various technologies.

Serial Links

Serial links take many forms, from 2400 b/s dial-up modems to dedicated T3 leased lines. All share two common traits: they interconnect two hosts, and they transmit a single bit at a time in each direction. The stream of bits is assembled into bytes and then packets. The speed of a serial line is rated in bits per second (b/s). They are either synchronous (in which some kind of clocking signal is transmitted with the data) or asynchronous.



Note

Cisco ANA supports this technology only in conjunction with data link layer technologies, such as ATM or PoS.

Information Model Objects (IMOs)

This section describes the following IMO:

- [Serial Interface \(IPhysicalLayer\)](#)

Serial Interface

Physical layer [Serial Interface](#) objects are bound by their Containing Termination Points attribute to a [Port Connector](#) object. Each object is accessed primarily by the data link layer object, such as the [PPP Encapsulation](#) interface, bound by its Contained Connection Termination Points attribute.

Table 33-1 *Serial Interface (IPhysicalLayer)*

Attribute Name	Attribute Description	Scheme	Polling Interval
All attributes are the same as Physical Layer (IPhysicalLayer)			

Vendor-Specific Inventory and IMOs

There are no vendor-specific inventory or IMOs for this technology.

Network Topology

Cisco ANA does not support discovery of physical layer topology. This topology is manually (statically) configured by the system administrator. However, it is used in conjunction with the data link layer above it, such as ATM, for discovering its physical topology, while further verifying it by matching the traffic signature of these ports using Cisco's confidential scheme, which requires a substantial amount of traffic in order to function correctly.

Service Alarms

The following alarms are supported for this technology:

- [Discard Packets, page 41-26](#)
- [Dropped Packets, page 41-27](#)
- [Link Down, page 41-42](#)
- [Port Down, page 41-51](#)
- [Rx Utilization, page 41-53](#)
- [Tx Utilization, page 41-57](#)



CHAPTER 34

Access Control Lists

This chapter describes the level of support that Cisco ANA provides for Access Control Lists (ACLs), as follows:

- [Technology Description, page 34-1](#)
- [Information Model Objects \(IMOs\), page 34-2](#)
- [Vendor-Specific Inventory and IMOs, page 34-3](#)
- [Network Topology, page 34-3](#)
- [Service Alarms, page 34-3](#)

Technology Description

Please see Part 1: Cisco VNEs in this guide for information about which devices support the various technologies.

ACLs

An ACL is a group of statements. Each defines a pattern of data that can be found in an IP packet. As each packet comes through an interface with an associated ACL, the ACL is scanned from top to bottom, in the exact order in which it was entered, for a pattern that matches the incoming packet. A permit or deny rule associated with each pattern determines that packet's fate. A mask (similar to a wild card) can also be used to determine how much of an IP source or destination address to use when matching against the pattern. The pattern statement can also include a TCP or UDP port.

Note that Cisco ANA currently supports IP ACLs only. MAC ACLs are not supported.

Information Model Objects (IMOs)

This section describes the following IMOs:

- [Access List Traffic Descriptor \(IAccessList\)](#)
- [Access List Entry \(IAccessListEntry\)](#)

Access List Traffic Descriptor

The [Access List Traffic Descriptor](#), with its [Access List Entry](#) objects, describes an access list of a single type (*Unknown*, *Standard*, *Extended*, or *Rate Limit*). It is aggregated by a [Traffic Descriptor Container](#) object (see [Common Components](#)).

Table 34-1 Access List Traffic Descriptor (IAccessList)

Attribute Name	Attribute Description	Scheme	Polling Interval
Type	Access list type (<i>Unknown</i> , <i>Standard</i> , <i>Extended</i> , <i>Rate Limit</i>)	Any	Configuration
Access List Entries Table	Array of instances of Access List Entry	Any	Configuration
Name or ID	Traffic descriptor name or identifier	Any	Configuration
Index	Traffic descriptor index	Any	Configuration

Access List Entry

Table 34-2 Access List Entry (IAccessListEntry)

Attribute Name	Attribute Description	Scheme	Polling Interval
Entry Identification	Entry identifier.	Any	Configuration
Action Logic	Action logic (<i>Unknown</i> , <i>Permit</i> , <i>Deny</i>).	Any	Configuration
Source and Destination Address	Source and destination IP address.	Any	Configuration
Source and Destination Wildcard	Source and destination IP wildcard.	Any	Configuration
Protocol Type	Internet Assigned Numbers Authority (IANA) type of the protocol (<i>HOPORT</i> , <i>ICMP</i> , <i>IGMP</i> , <i>GGP</i> , <i>IP in IP</i> , <i>ST</i> , <i>TCP</i> , <i>CBT</i> , <i>EGP</i> , <i>IGP</i> , and so on).	Any	Configuration
Source and Destination Ports Ranges	Source and destination TCP/UDP port ranges.	Any	Configuration
Source and Destination Port Action	Source and destination port action (<i>Null</i> , <i>Equal</i> , <i>Not Equal</i> , <i>Greater Than</i> , <i>Less Than</i> , <i>Range</i>).	Any	Configuration
Protocol Specific Info	Protocol specific information.	Any	Configuration
Differential Services Code Points	Differential Services Code Points (DSCP).	Any	Configuration

Table 34-2 Access List Entry (*IAccessListEntry*) (continued)

Attribute Name	Attribute Description	Scheme	Polling Interval
Type of Service	Type of Service (ToS) (<i>Normal [0], Min Cost [1], Max Reliability [2], 3, Max Throughput [4], 5, 6, 7, Min Delay [8], 9, 10, 11, 12, 13, 14, 15</i>).	Any	Configuration
Precedence	Precedence (<i>Routine [0], Priority [1], Immediate [2], Flash [3], Flash Override [4], Critical [5], Internet [6], Network [7]</i>).	Any	Configuration
Matches	The number of matches made.	Any	Configuration

Vendor-Specific Inventory and IMOs

There are no vendor-specific inventory or IMOs for this technology.

Network Topology

There is no specific network topology associated with this technology.

Service Alarms

There are no faults or alarms associated with this technology.



CHAPTER 35

Physical Components

This chapter describes the level of support that Cisco ANA provides for basic physical components of network elements, as follows:

- [Information Model Objects \(IMOs\), page 35-1](#)
- [Service Alarms, page 35-4](#)

Information Model Objects (IMOs)

This section describes the following IMOs:

- [Chassis \(IChassis\)](#)
- [Shelf \(IShelf\)](#)
- [Module \(IModule\)](#)
- [Power Supply \(IPowerSupply\)](#)
- [Port Connector \(IPortConnector\)](#)

Please see Part 1: Cisco VNEs in this guide for information about which devices support the various technologies.

Chassis

The [Chassis](#) object represents an equipment chassis. Its Contained Equipment Holders attribute binds it to other equipment holder objects, such as a [Shelf](#).

Table 35-1 **Chassis (IChassis)**

Attribute Name	Attribute Description	Scheme	Polling Interval
Description	Chassis description	Any	Configuration
Equipment Holder Type	Equipment holder type (<i>Chassis</i>)	Any	Configuration
Contained Equipment Holders	Contained equipment holders	Any	Configuration
Contained Equipments	Contained equipment	Any	Configuration
Serial Number	Serial number of the chassis	Any	Configuration
Flash Device	Flash device	Any	Configuration

Shelf

The [Shelf](#) object represents a shelf. Its Contained Equipment Holders and Contained Equipments attributes bind it to other equipment holders and equipment objects it contains.

Table 35-2 Shelf (IShelf)

Attribute Name	Attribute Description	Scheme	Polling Interval
Description	Chassis description	Any	Configuration
Status	Shelf status	Any	Configuration
Equipment Holder Type	Equipment holder type (<i>Shelf</i>)	Any	Configuration
Contained Equipment Holders	Contained equipment holders	Any	Configuration
Contained Equipments	Contained equipment	Any	Configuration
Serial Number	Serial number of the shelf	Any	Configuration

Module

The [Module](#) object represents a module or board. Its Contained Equipment Holders and supported Physical Termination Points attributes bind it to other equipment holders (subslots) and supported physical termination points ([Port Connectors](#)) objects it may contain.

Table 35-3 Module (IModule)

Attribute Name	Attribute Description	Scheme	Polling Interval
Module Name	Module name	Any	Configuration
Module Description	Module description	Any	Configuration
Software Version	Software version	Any	Configuration
Operational Status	Operational status (<i>Unknown, OK, Warning, Minor, Major, Critical, UnManaged, Enabled, Disabled, Information, Cleaning, Standby</i>)	Any	Configuration
Hardware Type and Version	Hardware type and version	Any	Configuration
Managed IP Address	Managed IP address	Any	Configuration
Redundant Equipment	Redundant equipment number	Any	Configuration
Configured Redundancy	Configured redundancy (<i>Null, Working, Protecting, None</i>)	Any	Configuration
Redundancy Status	Redundancy status (<i>Null, Active, Standby, None</i>)	Any	Configuration
Operational Status Last Change	Date of last operational status change	Any	Configuration
Contained Equipment Holders	Contained equipment holders	Any	Configuration
Supported Physical Termination Points	Supported physical termination points	Any	Configuration
Serial Number	Serial number of the module	Any	Configuration

Table 35-3 **Module (IModule) (continued)**

Attribute Name	Attribute Description	Scheme	Polling Interval
Slots Number	Number of slots in the module	Any	Configuration
CGN Service	Reference to the CGN service that is associated with this module.	IPCore	Configuration

Power Supply

The [Power Supply](#) object represents a power supply. Its Contained Equipment Holders attribute binds it to other equipment holder objects it may contain.

Table 35-4 **Power Supply (IPowerSupply)**

Attribute Name	Attribute Description	Scheme	Polling Interval
Operational Status	Operational status (<i>Unknown, OK, Warning, Minor, Major, Critical, UnManaged, Enabled, Disabled, Information, Cleaning, Standby</i>)	Any	Status
Hardware Type and Version	Hardware type and version	Any	Configuration
Management IP Address	Management IP address	Any	Configuration
Redundant Equipment	Redundant equipment number	Any	Configuration
Configured Redundancy	Configured redundancy (<i>Null, Working, Protecting, None</i>)	Any	Configuration
Redundancy Status	Redundancy status (<i>Null, Active, Standby, None</i>)	Any	Configuration
Operational Status Last Change	Date of last operational status change	Any	Configuration
Contained Equipment Holders	Contained equipment holders	Any	Configuration

Port Connector

The [Port Connector](#) object represents a port connector physical termination point. It is accessed by the [Module](#) containing it.

Table 35-5 **Port Connector (IPortConnector)**

Attribute Name	Attribute Description	Scheme	Polling Interval
Location	Port connector location	Any	Configuration
Alias	Port alias	Any	Configuration
Type	Port connector type (<i>Unknown, BNC, RJ11, RJ45, Fiber Optic, RJ48, Fiber Optic FC, Fiber Optic SC, Fiber Optic ST, Fiber Optic LC, Internal, Backplane, Fiber Optics MT RJ, DB 15 Pin, SMB, DB 60 Pin, DB 50 Pin, 34-pin Winchester, Generic, DB 9 Pin</i>)	Any	Configuration
Sub Ports	Subconnection termination points (currently being used only for Lucent SONET/SDH equipment)	Any	Configuration

Table 35-5 *Port Connector (IPortConnector) (continued)*

Attribute Name	Attribute Description	Scheme	Polling Interval
Supporting Equipment	Supporting equipment in which this port connector resides	Any	Configuration
Contained Connection Termination Points	Bound connection termination points	Any	Configuration

Service Alarms

The following alarms are supported for this technology:

- [Card Out, page 41-14](#)
- [Card Down, page 41-14](#)



CHAPTER 36

Logical Components

This chapter describes the level of support that Cisco ANA provides for basic logical components required for network element modeling, as follows:

- [Information Model Objects \(IMOs\), page 36-1](#)
- [Service Alarms, page 36-4](#)

Information Model Objects (IMOs)

This section describes the following IMOs:

- [Managed Element \(IManagedElement\)](#)
- [Logical Root \(ILogicalRoot\)](#)
- [Physical Root \(IPhysicalRoot\)](#)
- [Managed IP \(IManagedIP\)](#)
- [Context \(IContext\)](#)
- [System Service \(ISystemService\)](#)

Managed Element

The [Managed Element](#) object describes the root object of a modeled network element, from which all of its physical (chassis, slots, modules, port connectors) and logical (routing and switching entities, communication and physical termination point) component objects are accessed.

Table 36-1 **Managed Element (IManagedElement)**

Attribute Name	Attribute Description	Scheme	Polling Interval
IP Address	Management IP address	Any	Configuration
Communication State	Communication state with the managed device and the gateway (<i>Agent Unloaded, Device Unreachable, Agent Unreachable, Device Reachable, Connected, Connecting, Partially Connected, Connecting, Unknown</i>)	Any	Configuration
Investigation State	Investigation state of the VNE (<i>Unknown, Initializing, Normal, Incomplete, Unsupported, Device Agent Shutting Down, Device Agent Maintenance, Device Agent Preparing for Maintenance</i>)	Any	Configuration

Table 36-1 *Managed Element (IManagedElement) (continued)*

Attribute Name	Attribute Description	Scheme	Polling Interval
Element Category	Element category (<i>Unknown, DSLAM, Switch, BRAS, Router, Ethernet Switch, Cloud, Metro Central, Server, EMS, Generic Device Agent, ICMP, PC, Printer, Netra, WiFi Element, Service Control Switch</i>)	Any	Configuration
Element Type and its Key	Element type and its key mapped by the registry based on the SNMP system OID	Any	Configuration
Logical and Physical Roots	Logical and physical roots of the VNE model	Any	Configuration
Device Name	Device name as configured by the user in the registry	Any	Configuration
System Name, Description, Location, Contact and Up Time	System name, description, location, contact and up time taken from MIB II (RFC 1213).	Any	Configuration
Software Version	Software version running on the network element	Any	System
Vendor Identity	Vendor identity (<i>Null, Alcatel, Cisco, Copper Mountain, Redback Networks, Marconi, Lucent, Nokia, ADC, TdSoft, RAD, Nortel Networks, ECI Telecom, Juniper Networks, Sheer Networks, SUN Microsystems, NEC, Huawei, Laurel, UTStarcom</i>)	Any	Configuration
Memory and CPU Usage	Memory and CPU usage	Any	Status
Agent Memory and Free Memory Sizes	Agent memory and free memory sizes	Any	Configuration
Number of Device Components	Number of Device Components (DCs)	Any	Configuration
Number of Logical Entries	Number of property holders that are not DCs	Any	Configuration

Logical Root

The [Logical Root](#) and [Physical Root](#) objects aggregate or contain all the logical and physical components of a [Managed Element](#). They are accessed by the later logical and physical root attributes.

Table 36-2 *Logical Root (ILogicalRoot)*

Attribute Name	Attribute Description	Scheme	Polling Interval
Managed IPs List	Array of Managed IPs	Any	Configuration
Contexts List	Array of Contexts	Any	Configuration
Forwarding Components List	Array of Forwarding Component Containers	Any	Configuration
Traffic Descriptors List	Array of Traffic Descriptor Containers	Any	Configuration
Tunnel Containers List	Array of Tunnel Containers	Any	Configuration
Services List	Array of System Services	Any	Configuration
Data Link Aggregation Containers List	Array of data link aggregations (Link Aggregation Groups , Cisco Ethernet Channels)	Any	Configuration

Physical Root

Table 36-3 *Physical Root (IPhysicalRoot)*

Attribute Name	Attribute Description	Scheme	Polling Interval
Equipment Holders	Array of equipment holders such as Chassis and Shelf	Any	Configuration

Managed IP

The [Managed IP](#) object aggregates or contains all logical components of a [Managed Element](#) that are managed by one of the multiple managed IP addresses of this element. It is accessed by a [Logical Root](#).

Table 36-4 *Managed IP (IManagedIP)*

Attribute Name	Attribute Description	Scheme	Polling Interval
System Name, Description, Location, Contact and Up Time	System name, description, location, contact and up time taken from MIB II (RFC 1213).	Any	Configuration
Software Version	Software version	Any	Configuration
Contexts List	Array of Contexts	Any	Configuration
Forwarding Components List	Array of Forwarding Component Containers	Any	Configuration
Traffic Descriptors List	Array of Traffic Descriptor Containers	Any	Configuration
Tunnel Containers List	Array of Tunnel Containers	Any	Configuration
Services List	Array of System Services	Any	Configuration

Context

The [Context](#) object aggregates or contains all the logical components of a [Managed Element](#) with a single context, such as a virtual router, and is accessed by a [Logical Root](#).

Table 36-5 *Context (IContext)*

Attribute Name	Attribute Description	Scheme	Polling Interval
Name	Context name	Any	Configuration
IP Address Pools	Array of IP Address Pools	Any	Configuration
Forwarding Components List	Array of Forwarding Component Containers	Any	Configuration
Traffic Descriptors List	Array of Traffic Descriptor Containers	Any	Configuration
Tunnel Containers List	Array of Tunnel Containers	Any	Configuration
Data Link Aggregation Containers List	Array of data link aggregations (Link Aggregation Groups , Cisco Ethernet Channels)	Any	Configuration
Operating System	NEIM operating system DC.	Any	Configuration

System Service

The [System Service](#) object describes a single system service along with its status and up time, and is accessed by a [Logical Root](#).

Table 36-6 **System Service (*ISystemService*)**

Attribute Name	Attribute Description	Scheme	Polling Interval
Type	Service type (<i>Unknown, Radius, Network Time Protocol, Spanning Tree Protocol</i>)	Any	Configuration
Status	Service status (<i>Null, Running, Down, Reset, Initializing, Other</i>)	Any	Configuration
Up Time	Service up time.	Any	Configuration

Service Alarms

The following alarms are supported for base logical components:

- [Component Unreachable](#), page 41-23
- [CPU Utilization](#), page 41-25
- [Device Unsupported](#), page 41-26
- [Memory Utilization](#), page 41-46



CHAPTER 37

Common Components

This chapter describes the level of support that Cisco ANA provides for components common to all network elements, as follows:

- [Information Model Objects \(IMOs\), page 37-1](#)
- [Network Topology, page 37-7](#)
- [Service Alarms, page 37-7](#)

Information Model Objects (IMOs)

This section describes the following IMOs:

- [Physical Layer \(IPhysicalLayer\)](#)
- [Bridging Entity \(IBridge\)](#)
- [Bridging Entry \(IBridgeEntry\)](#)
- [VC Multiplexer \(EncapMux\)](#)
- [VC Encapsulation \(IVcBasedEncapsulation\)](#)
- [Virtual Cross Connection \(IVcCrossConnect\)](#)
- [Forwarding Component Container \(IFWComponentContainer\)](#)
- [Traffic Descriptor Container \(ITrafficDescriptorContainer\)](#)
- [Tunnel Container \(ITunnelContainer\)](#)

Physical Layer

The **Physical Layer** object is bound by its Containing Termination Points attribute to a **Port Connector** object. It is accessed by the data link layer bound by its Contained Connection Termination Points attribute.

The polling interval for each of the four “Thresholds” attributes is marked as Not Applicable (N/A) because it does not originate from the modeled NE. Instead, it is taken from the TCA system of the VNE.


Note

The following attributes are configured in the registry and not retrieved from the device.

Table 37-1 **Physical Layer (IPhysicalLayer)**

Attribute Name	Attribute Description	Scheme	Polling Interval
Media Type	Physical media type (<i>Null, Thin Coax, Thick Coax, Fiber Optic, Multi Mode Fiber Optic, Single Mode Fiber Optic, Short Single Mode Fiber Optic, Long Single Mode Fiber Optic, UTP, STP, FTP, EIA/TIA-232, EIA/TIA-449, V.35, X.21, EIA/TIA-530, EIA/TIA-530A, Generic Serial, EIA/TIA-612/613, Other</i>)	Any	Configuration
Clocking Source	Clocking source (<i>Unknown, Other, Network, Internal, Loop Timed, External, None, Line, Back Plane, Adaptive Timing</i>)	Any	Configuration
Maximum Speed	Maximum supported speed with units specification	Any	System
Is Internal Port	Indicates an internal port, such as between module and backplane (<i>True, False</i>)	Any	Configuration
Maximum and Minimum Discarded Thresholds	Maximum and minimum discarded input bandwidth thresholds	Any	N/A
Discarded Bandwidth	Current discarded input bandwidth	Any	Configuration
Maximum and Minimum Dropped Thresholds	Maximum and minimum dropped output bandwidth thresholds	Any	N/A
Dropped Bandwidth	Current dropped output bandwidth	Any	Configuration
Maximum and Minimum Input Thresholds	Maximum and minimum utilized input bandwidth thresholds	Any	N/A
Input Bandwidth	Current utilized input bandwidth	Any	Configuration
Maximum and Minimum Output Thresholds	Maximum and minimum utilized output bandwidth thresholds	Any	N/A
Output Bandwidth	Current utilized output bandwidth	Any	Configuration
Discarded and Received Input Data Counters	Discarded and received input octets and packets counters	Any	Topology L1
Dropped and Forwarded Output Data Counters	Dropped and forwarded output octets and packets counters	Any	Topology L1
Administrative Status	Administrative status (<i>Unknown, Up, Down, Testing</i>)	Any	Status
Operational Status	Operational status (<i>Unknown, Up, Down, Testing, Dormant, Not Present</i>)	Any	Status
Operational Status Last Change	Date of last operational status change	Any	Configuration

Table 37-1 *Physical Layer (IPhysicalLayer) (continued)*

Attribute Name	Attribute Description	Scheme	Polling Interval
IANA Type	Internet Assigned Numbers Authority (IANA) type of the sublayer	N/A	N/A
Containing Termination Points	Underlying termination points (connection or physical)	Any	N/A
Contained Connection Termination Points	Bound connection termination points	Any	N/A

Bridging Entity

The [Bridging Entity](#) object describes the IEEE 802-based protocol- independent forwarding component of an IEEE 802 bridge or switch. It is bound by its Logical Sons attribute to all the data link layer objects (such as [Ethernet Interface](#)) among which this Bridging Entity is bridging or switching IEEE 802-based data link frames.

Table 37-2 *Bridging Entity (IBridge)*

Attribute Name	Attribute Description	Scheme	Polling Interval
Bridge Table	Array of Bridging Entries	Any	Configuration
Type	Bridge type (<i>Null, Automatic, Regular, Bridge Route</i>)	Any	Configuration
MAC Address	Bridge internal MAC address used either for running Spanning Tree Protocol (STP) or for bridge network management	Any	Configuration
IP Interface	OID of the IP interface used mainly for routing traffic from that bridge	Any	Configuration
Name	Bridging entity name	Any	Configuration
Logical Sons	Array of all IEEE 802-based data link interfaces among which this Bridging Entity is bridging or switching IEEE 802-based data link frames	Any	Configuration
VLAN Type	The type of VLAN	Any	Configuration

Bridging Entry

The [Bridging Entry](#) object describes a domain-wide bridge table entry within a [Bridging Entity](#).

Table 37-3 *Bridging Entry (IBridgeEntry)*

Attribute Name	Attribute Description	Scheme	Polling Interval
Destination MAC Address	Destination station MAC address	Any	Configuration
Outgoing Interface	Underlying outgoing interface (Cisco Ethernet Channels , Ethernet Interfaces , Virtual LAN Interfaces or Virtual LAN Multiplexers)	Any	Configuration

VC Multiplexer

The **VC Multiplexer** object is bound by its Containing Termination Points attribute to either an **ATM Interface** or a **Frame Relay Interface** object. It is accessed primarily by the data link layer **VC Encapsulations** bound by its Contained Connection Termination Points attribute.

Table 37-4 *VC Multiplexer (EncapMux)*

Attribute Name	Attribute Description	Scheme	Polling Interval
Virtual Connection Count	Bound virtual connection count	Any	Configuration
IANA Type	Internet Assigned Numbers Authority (IANA) type of the sublayer	N/A	N/A
Containing Termination Points	Underlying termination points (ATM Interface or Frame Relay Interface)	Any	N/A
Contained Connection Termination Points	Bound connection termination points (VC Encapsulations)	Any	N/A

VC Encapsulation

The data link layer **VC Encapsulation** object is bound by its Containing Termination Points attribute to an ATM or Frame Relay **VC Multiplexer** object. It is accessed primarily by a network layer object (such as an **IP Interface**), and also by the data link layer object (such as an **Ethernet Interface** or **PPP Encapsulation**) bound by its Contained Connection Termination Points attribute.

Table 37-5 *VC Encapsulation (IVcBasedEncapsulation)*

Attribute Name	Attribute Description	Scheme	Polling Interval
Virtual Connection	Virtual connection (ATM Virtual Connection or Frame Relay Virtual Connection)	Any	Configuration
Binding Information	Binding information (<i>User Name, ...</i>)	Any	Configuration
Binding Status	Binding status (<i>Not Bound, Bound</i>)	Any	Configuration
IANA Type	Internet Assigned Numbers Authority (IANA) type of the sublayer	N/A	N/A
Containing Termination Points	Underlying termination points (connection or physical)	Any	N/A
Contained Connection Termination Points	Bound connection termination points	Any	N/A

Virtual Cross Connection

The [Virtual Cross Connection](#) object describes either a [Virtual Connection Switching Entity](#)-wide or an [ATM Interface](#)-specific Cross Connect table's entry.

Table 37-6 *Virtual Cross Connection (IVcCrossConnect)*

Attribute Name	Attribute Description	Scheme	Polling Interval
Ingress and Egress Virtual Connection	Ingress and egress virtual connections (ATM Virtual Connection or Frame Relay Virtual Connection)	Any	Configuration
Ingress and Egress Port	Ingress and egress ports (<i>Port Connectors</i>)	Any	Configuration

Forwarding Component Container

The [Forwarding Component Container](#) object aggregates a single type of Forwarding Component, such as a [Routing Entry](#), [Bridging Entity](#) or [Virtual Connection Switching Entity](#).

Table 37-7 *Forwarding Component Container (IFWComponentContainer)*

Attribute Name	Attribute Description	Scheme	Polling Interval
Forwarding Components	Array of a single type of forwarding component	Any	Configuration
Type	Forwarding component (<i>Null, Routing Entities, Bridges, VRFs, LSEs, VC Switching Entities, L2TP Peers, MPBGPs, IMA Groups</i>)	Any	Configuration

Traffic Descriptor Container

The [Traffic Descriptor Container](#) object is basically a container of any table's entries. It aggregates a single type of Traffic Descriptor.

Table 37-8 *Traffic Descriptor Container (ITrafficDescriptorContainer)*

Attribute Name	Attribute Description	Scheme	Polling Interval
Traffic Descriptors	Array of a single type of traffic descriptor	Any	Configuration
Type	Descriptor type (<i>Null, ATM Traffic Profiles, ADSL Traffic Descriptors, SDSL Traffic Descriptors, IDSL Traffic Descriptors, SHDSL Traffic Descriptors, MPLS Properties, CAC Profiles, ATM Access Profiles, OSPF Networks, BGP Neighbor, Access Lists, Tunnel Traffic Descriptors, QoS Policies, QoS Classes, IS-IS Database, QoS WRED, ATM Traffic Shaping Profile, Frame Relay Traffic Profiles, Rate Limit, Filter, Policer, IP Pools, ISAKMP Policies, IPsec Maps, Process List, Installed Software, L2TP Peer Group, L2TP Domain Group, QoS Object Table, QoS Class Map, QoS Policy Map, QoS Match Statements Table, QoS Queueing Config Table, QoS Service Policy Table, ADSL 2 Traffic Descriptors, ADSL 2 Spectrum Descriptors</i>)	Any	Configuration

Tunnel Container

The [Tunnel Container](#) object aggregates instances of a single type of tunnel interface (either [MPLS TE Tunnel Interfaces](#) or [PTP Layer 2 MPLS Tunnel Interfaces](#)).

Table 37-9 *Tunnel Container (ITunnelContainer)*

Attribute Name	Attribute Description	Scheme	Polling Interval
Tunnel Edges	Array of either PTP Layer 2 MPLS Tunnel Interfaces or MPLS TE Tunnel Interfaces	Any	Configuration

Network Topology

The Cisco Discovery Protocol (CDP), although proprietary, plays a major role in discovery of all Cisco network equipment. Cisco ANA uses it as part of the data link topology discovery for all Cisco network elements. It uses CDP by searching for the existence of local CDP neighbor signatures, gathered from the CDP process, in any remote side port of the same type.

LLDP, which is a standard discovery protocol for the data link layer, is also used for link discovery on the Cisco devices which support this protocol. Cisco ANA uses LLDP by searching for the existence of local LLDP neighbor signatures, gathered from the LLDP process, in any remote side port of the same type.

Service Alarms

The following alarms are supported for this technology:

- [Cloud Problem, page 41-22](#)
- [Discard Packets, page 41-26](#)
- [Dropped Packets, page 41-27](#)
- [Link Down, page 41-42](#)
- [Port Down, page 41-51](#)
- [Rx Utilization, page 41-53](#)
- [Tx Utilization, page 41-57](#)



CHAPTER 38

Cisco ANA VNE Topology

This chapter describes the Cisco ANA VNE Topology, as follows:

- [Specifications, page 38-1](#)
- [Topology Types, page 38-7](#)

Specifications

[Table 38-1](#) describes the types of topologies Cisco ANA supports and how Cisco ANA discovers and displays them. Discovery takes place in two phases:

1. Discovery of existing links.
2. For discovered links, verification that the links still exist.

The Topology Type column identifies the type of technology to which each Link Type is related.

The Link Type column displays the link type as exposed by Cisco ANA.

Table 38-1 *Types of Topologies Supported by Cisco ANA*

Topology Type	Link Type	Discovery Technique	Verification Technique	Description
ATM	ATM	ATM VC Counters: 1. Same Active VCs 2. VC traffic signature; see Traffic Signature .	Physical layer counters. See physical layer counters in Physical Layer .	Active VCs—Each side identifies a set of active 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. VC Traffic Signatures—Based on the VCs counters; see Traffic Signature .
		CDP	CDP. See CDP (Cisco Discovery Protocol) .	
		Static	Static	

Table 38-1 *Types of Topologies Supported by Cisco ANA (continued)*

Topology Type	Link Type	Discovery Technique	Verification Technique	Description
ATM	PNNI	PNNI Information	None	PNNI Information—In this technique, each port in the ATM switch is identified with two values: 1. Node ID. 2. Port ID.
BFD	BFD	BFD session's source and destination addresses	BFD session's source and destination addresses	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	BGP	BGP Info	BGP Info	BGP Info—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.
Business	Business	N/A	N/A	Business links are not discovered at the VNE level; they are created in the gateway. These links represent a relationship between any two objects in the model, which can be business or network related.
LAG	LAG	STP	STP. See STP (Spanning Tree Protocol) .	
		MAC	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	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	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).

Table 38-1 *Types of Topologies Supported by Cisco ANA (continued)*

Topology Type	Link Type	Discovery Technique	Verification Technique	Description
Ethernet	Ethernet	MAC	Ethernet counters and physical layer counters; see physical layer counters in Physical Layer .	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). Ethernet Counters—Based on the Unicast Packets traffic signature, see Traffic Signature .
		CDP	CDP	See CDP (Cisco Discovery Protocol) .
		LLDP	LLDP	See LLDP (Link Layer Discovery Protocol) .
		STP	STP	See STP (Spanning Tree Protocol) .
		REP	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.
		Static	Static	
Frame Relay	Frame Relay	Not Supported	Physical layer counters. See physical layer counters in Physical Layer .	Frame Relay links can be discovered dynamically only between Cisco devices with CDP enabled, or by using static or manual configuration (physical link discovery).
		CDP	CDP. See CDP (Cisco Discovery Protocol) .	
		Static	Static	
MLPPP	MLPPP	MLPPP End Point Identifier	MLPPP End Point 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.
MPLS	MPLS	IP Information	IP Information	IP Information—In this technique, the IP addresses of the multiple MPLS interfaces are checked to see if they are in the same subnet (includes the generic VNE). For more information, see IPv4 IP Topology Testing .

Table 38-1 *Types of Topologies Supported by Cisco ANA (continued)*

Topology Type	Link Type	Discovery Technique	Verification Technique	Description
PPP or HDLC	PPP or HDLC	IP Information	IP Information and physical layer counters. See physical layer counters in Physical Layer .	IP Information—In this technique, the IP addresses of the multiple PPP or HDLC interfaces are checked to see if they are in the same subnet (includes the generic VNE). For more information, see IPv4 IP Topology Testing .
		CDP	CDP. See CDP (Cisco Discovery Protocol) .	
		Static	Static	
Physical Layer	Physical Layer	A physical link is not discovered independently. Physical links are created as a result of the discovery of Layer 2 links, such as ATM and Ethernet.	Physical Layer Counters	By default, the physical layer does not have specific techniques for discovery. Special cases are: - Ports from the same device will not be connected. - Static topology may be used in the physical layer. For more information, see Physical Layer .
		Static	Static	Physical Layer Counters—Based on the port traffic signature, using octet-based, or octet- and packet-based traffic; see Traffic Signature . Note In the discovery phase of physical topology, use the Same Device test. In this technique, the port is checked to see if it is in separate VNEs depending on the type of managed equipment.
PWE3	Tunnel	PWE3 Information	PWE3 Information	PWE3 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.

Table 38-1 *Types of Topologies Supported by Cisco ANA (continued)*

Topology Type	Link Type	Discovery Technique	Verification Technique	Description
GRE Tunnel	Tunnel GRE	GRE Tunnel Information	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.
VLAN	VLAN	VLAN ID matching	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.
VPN (VRF)	VPN	Route Targets	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).
	VPNv6	Route Targets for IPv6 Address Family	Route Targets for IPv6 Address Family	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

In Cisco ANA'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.

In addition, 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.

IPv4 IP Topology Testing

Cisco ANA uses IP testing 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.

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.

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.

STP (Spanning Tree Protocol)

If STP is enabled between switches, it has the highest priority and its information will be used for discovery and verification. In this technique 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.

**Note**

This STP discovery technique will work correctly only when the same STP protocol is running on both ports.

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.

Topology Types

The following topology types are described in this section:

- [ATM](#)
- [BFD](#)
- [BGP](#)
- [Business](#)
- [Ethernet](#)
- [LAG](#)
- [Frame Relay](#)
- [MPLS](#)
- [PPP or HDLC](#)
- [Physical Layer](#)
- [PWE3](#)
- [GRE Tunnel](#)
- [VPN](#)

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.

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.

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.

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 a business object or network objects. These links are created in the Cisco ANA 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.

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.

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.

MPLS

MPLS topology represents adjacent MPLS interfaces in the network. This adjacency represents that 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.

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.

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.

PWE3

PWE3 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.

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.

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.



PART 3

Alarms and Events



CHAPTER 39

System Events

This section describes the Cisco ANA system events. System events appear in the Cisco ANA EventVision System tab. They include a variety of events pertaining to the system activities, from alarm thresholds to disk space and AVMs. Cisco ANA system events and system event messages are listed in the following tables:

- System events—[Table 39-1 on page 39-2](#)
- System event messages—[Table 39-2 on page 39-9](#)

For definitions of system event terms and acronyms, see [Table 39-3 on page 39-9](#). For information about Cisco ANA EventVision, see the [Cisco Active Network Abstraction 3.7.1 User Guide](#).

Table 39-1 Cisco ANA System Events

Source OID	Message	Severity	Cause	Action
Category: MCReachability				
IMC	Agent <i>vne_name</i> , <i>agent_ip</i> is reachable: DNA Unit = <i>unit_ip</i> AVM = <i>avm_id</i>	CLEARED	The VNE is reachable.	None needed.
IMC	Agent <i>vne_name</i> , <i>agent_ip</i> is unreachable: DNA Unit = <i>unit_ip</i> AVM = <i>avm_id</i>	MINOR	Various causes; system or network failure.	Contact Cisco Support.
IAvm	AVM <i>unit_ip</i> : <i>avm_id</i> (<i>avm_key</i>) is reachable	CLEARED	The AVM is reachable.	None needed.
IAvm	AVM <i>unit_ip</i> : <i>avm_id</i> (<i>avm_key</i>) is unreachable	MINOR	Network or machine failure.	Contact Cisco Support.
IMC	Unit <i>unit_ip</i> reachable	CLEARED	The MC is reachable.	None needed.
IMC	Unit <i>unit_ip</i> unreachable	MINOR	System, network, or machine failure.	Contact Cisco Support.
Category: alarm threshold				
IAvm	Violet threshold reached, alarms must be deleted	CRITICAL	There are too many alarms open in the system.	Remove alarms.
IAvm	Red threshold reached, deleting alarms!	CRITICAL	There are too many alarms open in the system and the user has not removed them.	The system is deleting some of the alarms.
Category: backup				
IAvm	Unable to backup 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: <i>path</i>	MAJOR	Permission problems.	Check the directory permissions.
IAvm	Unable to delete file: <i>name</i>	MAJOR	Permission problems.	Check the file permissions.
IAvm	Error deleting files from: <i>path</i>	MAJOR	Permission problems.	Check the permissions of the directory containing the files and the permissions on the files.
IAvm	Error deleting files from: <i>path</i>	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 <i>count</i> alarms.	MINOR	Element removed without first removing its alarms.	The system is removing the relevant alarms.

Table 39-1 Cisco ANA System Events (continued)

Source OID	Message	Severity	Cause	Action
Category: bad oid				
IAvm	<i>count</i> bad oids found in table <i>businessObject</i>	CRITICAL	Bad business objects were inserted into the database.	The system is removing them.
Category: bos misconfiguration				
IElementManagement	<i>duplicate_value</i> is configured as <i>existing_element</i> in Unit <i>unit_ip</i> AVM <i>avm_id</i> and also as <i>new_element</i> in Unit <i>new_unit_ip</i> AVM <i>new_avm_id</i>	MAJOR	XML files were edited manually and incorrectly. Note: The existing element is a VNE. The duplicate value is either the VNE's name or its IP address.	Fix XML file. Remove conflicting entry.
Category: drop affected				
IAvm	Dropping affected Message of size: <i>size</i> the total affected waiting to be saved is: <i>count</i>	CRITICAL	The system was shut down while removing affected messages.	The system removes the remaining affected messages.
Category: event-rate-limiter				
IAvm	Dropped Events Report Long Description List of dropped events, with the total number of events dropped for each type of event. For example: Count type (ID) ----- 282 dot1qBridge trap (dot1qBridge trap 601 generic trap (generic trap)	CRITICAL	There is an event burst in the network. The number of events received exceeded the Cisco ANA threshold. Cisco ANA dropped the excess events.	Check the network for the root cause of the event burst.
IAvm	<i>number_of_seconds</i> sec limiter for default event type reached CLEARED threshold	CLEARED	The rate of events received has now dropped below the threshold and is normal.	None needed.
IAvm	<i>number_of_seconds</i> sec limiter for default event type reached WARNING threshold	WARNING	The rate at which events are being received is very close to the defined threshold value. There may be an event burst in the network.	Check the network for the root cause of the event burst.
Category: free space				
IAvm	No room for tablespace <i>tablespace_name</i> 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 <i>object_name</i> in tablespace <i>tablespace_name</i>	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.

Table 39-1 Cisco ANA System Events (continued)

Source OID	Message	Severity	Cause	Action
Category: license				
MCNetwork	No license file exists (Evaluation system).	WARNING	Cisco ANA 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.
Category: no stacktrace				
IAvm	Session discard a msg due to an exception <i>exception_msg</i>	MAJOR	An exception occurred while handling an internal message.	If this event recurs frequently, check the logs for the exception type.
Category: partitioning				
IAvm	Unable to split partition <i>partition_name</i> on <i>table_name</i> because it contains data!	CRITICAL	The system did not split the partition before the system started inserting data into it.	Contact Cisco Support.
Category: queue-size-limiter				
IAvm	Queue Size Limiter Report	CRITICAL	There was an event burst in the network. The number of events received exceeded the Cisco ANA threshold. Cisco ANA dropped the excess events.	Check the network for the root cause of the event burst.
Category: session timeout				
IAvm	Session creator <i>creator</i> has timed out (session <i>XID=session_xid</i>)	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: severity				
IAvm	Found Integrity problem on <i>problems</i> elements	CRITICAL	There was a problem calculating the severity.	The system will fix the inaccuracy.

Table 39-1 Cisco ANA System Events (continued)

Source OID	Message	Severity	Cause	Action
Category: tickets capacity				
IAvm	Tickets capacity back to normal.	CLEARED	The number of tickets Cisco ANA is generating has dropped below the defined threshold value.	None needed.
IAvm	Tickets capacity overflow, red threshold reached.	CRITICAL	The number of new tickets Cisco ANA is generating has reached the defined threshold value.	Check the network for the root cause of the event burst.
Category: user disabled				
IAvm	Too many failed login, user disabled <i>username</i>	MINOR	Too many failed login attempts caused Cisco ANA 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 <i>agent_ip</i> is not loading because of incorrect polling group. BOS Unit = <i>unit_ip</i> AVM = <i>avm_id</i>	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.
IElement Management	Configuration Error - Duplicate IP [<i>existing_ip</i>]. 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 [<i>existing_key</i>]. Will unload device.	CRITICAL	Cisco ANA found a duplicate device key and will unload the device.	Assign a unique key to the device, then reload it.
IElement Management	Agent <i>agent_ip</i> is starting. BOS Unit = <i>unit_ip</i> AVM = <i>avm_id</i>	MINOR	The specified VNE is starting.	None needed.
IElement Management	Agent <i>agent_ip</i> is shutting down. BOS Unit = <i>unit_ip</i> AVM = <i>avm_id</i>	MINOR	The specified VNE is shutting down.	None needed.
IElement Management	Agent <i>agent_ip</i> not responding: BOS Unit = <i>unit_ip</i> AVM = <i>avm_id</i>	MAJOR	The specified VNE is not responding.	Check AVM logs for any errors or memory issues.

Table 39-1 Cisco ANA System Events (continued)

Source OID	Message	Severity	Cause	Action
IElement Management	Agent <i>agent_ip</i> suppressed: BOS Unit = <i>unit_ip</i> AVM = <i>avm_id</i>	MAJOR	The specified VNE is not responding. Efforts to restart the VNE have failed, so Cisco ANA 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 <i>avm_id</i> is starting. BOS Unit = <i>unit_ip</i>	MINOR	The specified AVM is starting.	None needed.
IAvm	AVM <i>avm_id</i> is shutting down. BOS Unit = <i>unit_ip</i>	MINOR	The specified AVM is shutting down.	None needed.
IAvm	AVM <i>avm_id</i> suppressed: BOS Unit = <i>unit_ip</i> AVM = <i>avm_id</i>	MINOR	The specified AVM is not responding and Cisco ANA's efforts to restart it have failed multiple times. Cisco ANA is now permanently suppressing the AVM.	Check AVM logs for any evident errors, rectify those errors, and restart manually.
IAvm	AVM <i>avm_id</i> not responding: BOS Unit = <i>unit_ip</i> AVM = <i>avm_id</i>	MAJOR	The specified AVM is not responding.	Check AVM logs for any evident errors, rectify those errors, and restart manually.
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 <i>avm_id</i> started. BOS Unit = <i>unit_ip</i>	MINOR	The specified AVM has started.	None needed.
IAvm	AVM <i>avm_id</i> shut down. BOS Unit = <i>unit_ip</i>	MINOR	The specified AVM has shut down.	None needed.
IAvm	An outgoing <i>frame_type</i> frame to <i>port_peer_description</i> was dropped	MAJOR	There is insufficient buffer space for outgoing transport frames.	Note the machine's CPU usage and then contact Cisco Support.
IAvm	<i>repeat_count_frames</i> were dropped in the last <i>time</i> seconds - for example an outgoing <i>frame_type</i> frame to <i>port_peer_description</i>	MAJOR	There is insufficient buffer space. Repeated events were suppressed to avoid an event storm.	Note the machine's CPU usage and then contact Cisco Support.

Table 39-1 Cisco ANA System Events (continued)

Source OID	Message	Severity	Cause	Action
IAvm	A deserialization error occurred: class version error while deserializing a <i>frame_type_name</i> frame from <i>transport_string</i> to <i>transport_string:class_name</i>	MAJOR	Code incompatibility exists between the source's AVM and the target's AVM.	Contact Cisco Support.
IAvm	<i>deserialization_error_repeat_count</i> deserialization errors occurred in the last <i>time</i> seconds - for example: class version error while deserializing a <i>frame_type_name</i> frame from <i>transport_string</i> to <i>transport_string:class_name</i>	MAJOR	A code incompatibility exists; repeated events were suppressed.	Contact Cisco Support.
Category: Unit System Events				
IMC	Server <i>unit_ip</i> manual failover initiated. Raising Redundant machine = <i>redundant_unit_ip</i>	MAJOR	A manual failover was requested for unit <i>unit_ip</i> . Cisco ANA is attempting to start the specified standby machine.	None needed.
IMC	Server <i>unit_ip</i> not responding. Raising Redundant machine = <i>redundant_unit_ip</i>	MAJOR	A manual failover was requested for unit <i>unit_ip</i> . Cisco ANA is attempting to start the specified standby machine.	None needed.
IMC	Server <i>unit_ip</i> manual failover initiated. No Redundant machine available.	MAJOR	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.
IMC	Server <i>unit_ip</i> not responding. No Redundant machine available.	MAJOR	The High Availability service cannot service the failover request because the assigned standby machine <i>unit_ip</i> 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 <i>unit_ip</i> is starting.	MINOR	The specified unit is starting.	None needed.
IMC	BOS Unit <i>unit_ip</i> is shutting down.	MINOR	The specified unit is shutting down.	None needed.
IMC	Uplink to <i>peer_host_address/peer_AVM_id</i> disabled	MINOR	The administrator disabled the uplink to the specified host or peer AVM.	None needed.
IMC	Uplink to <i>peer_host_address/peer_AVM_id</i> enabled	MINOR	The administrator disabled the uplink to the specified host or peer AVM.	None needed.

Table 39-1 Cisco ANA System Events (continued)

Source OID	Message	Severity	Cause	Action
IMC	Uplink to <i>peer_host_address/peer_AVM_id</i> connected	MINOR	The uplink connection with the specified host or peer AVM was established.	None needed.
IMC	Uplink to <i>peer_host_address/peer_AVM_id</i> 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 <i>ipPort</i> using <i>connectTechnology</i> information conflicts with verification based on <i>disconnectTechnology</i> information. You are strongly recommended to wait until the link disappears and then create a static link from Port <i>ipPort</i> 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: Others				
IManaged Element	VNE definitions did not load properly Long Description VNE definitions did not load properly. Reason: <i>reason</i>	CRITICAL	Cisco ANA was unable to load VNEs.	Check the AVM logs for any evident errors, rectify those errors, and restart manually.

Table 39-2 Error and Event Messages

Description	Cause	Action
The key of AVM <i>unit_ip:avmid</i> (<i>avmeap</i>) was changed to <i>newkey</i>	The Administrator changed the AVM key.	None needed.
Full GC max time exceeded (reached <i>seconds</i> 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: <i>unit_ip</i> , AVM: <i>avm_id</i>	The High Availability service determined that the AVM <i>avm_id</i> on unit <i>unit_ip</i> is not responding.	None needed.
AVM suppressed, DNA Unit: <i>unit_ip</i> , AVM: <i>avm_id</i>	The High Availability service has suppressed AVM <i>avm_id</i> on unit <i>unit_ip</i> . 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: <i>unit_ip</i> , AVM: <i>avm_id</i>	The specified AVM exceeded its allocated memory.	Assign more memory to the AVM, then restart the AVM.
A message was dropped from <i>vne_xid</i> 's mailbox: <i>message_class</i> from <i>XID</i> to <i>XID</i>	There is insufficient buffer space in the specified VNE's message queue.	Contact Cisco Support.
<i>number</i> messages were dropped in the last <i>number</i> seconds – for example this message from <i>vne_xid</i> 's mailbox: <i>message_class</i> from <i>XID</i> to <i>XID</i>	There has been insufficient buffer space in the specified VNE's message queue for the specified time, and repeated events are being suppressed.	Contact Cisco Support.
Dropped events report: <i>event type:number</i> <i>event type:number</i>	The event type reached its rate limit and events of this type were dropped.	Contact Cisco Support.
<i>period_in_seconds</i> sec period limiter for <i>event_type</i> event type reached WARNING threshold	The event type reached its warning threshold.	Contact Cisco Support.
<i>period_in_seconds</i> sec period limiter for <i>event_type</i> event type reached CLEARED threshold	The event type reached its cleared threshold.	None needed.

Table 39-3 defines some common security event acronyms.

Table 39-3 System Event Terms and Acronyms

Term	Definition
AVM	A Cisco ANA Java process that provides the necessary distribution support platform for executing and monitoring multiple VNEs.
<i>avm_id</i>	AVM identifier
<i>avm_key</i>	AVM key
BOS	Cisco ANA
DNA	Cisco ANA

Table 39-3 **System Event Terms and Acronyms (continued)**

Term	Definition
MC	Cisco ANA unit
VNE	Virtual Network Element



CHAPTER 40

Security Events

This section describes the Cisco ANA security events. Security events are related to client logins and user activities when managing Cisco ANA and the Cisco ANA environment. [Table 40-1](#) lists Cisco ANA security events. Security events are displayed in the Security tab in Cisco ANA EventVision.

For definitions of terms and acronyms used in [Table 40-1](#), see [Table 40-2 on page 40-7](#). For information about Cisco ANA EventVision, see the [Cisco Active Network Abstraction 3.7.1 User Guide](#).

Table 40-1 Cisco ANA 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 40-1 Cisco ANA 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 40-1 Cisco ANA 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 40-1 Cisco ANA 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 40-1 Cisco ANA 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.
Category: Insufficient Permissions					
execute command	IAvm	User <username> doesn't have required permission to run command <command name> .	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.
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.

Table 40-1 Cisco ANA Security Events (continued)

Event Name	Source OID	Short Description	Severity	Cause	Action
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.
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.

Table 40-1 Cisco ANA Security Events (continued)

Event Name	Source OID	Short Description	Severity	Cause	Action
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.

Table 40-2 defines terms and acronyms that appear in the security events table.

Table 40-2 Security Event Terms and Acronyms

Term	Definition
avmid	AVM identifier
avmkey	AVM key
BOS	Cisco ANA
DNA	Cisco ANA
MC	Cisco ANA unit
VNE	Virtual Network Element





CHAPTER 41

Service Alarms

This section describes the Cisco ANA service alarms (events). Service alarms appear in the Cisco ANA EventVision Service tab. For information about Cisco ANA EventVision, see the [Cisco Active Network Abstraction 3.7.1 User Guide](#). These topics describe the Cisco ANA 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 (Cisco ANA) state that caused the alarm. The short description of the service alarm is what appears in the ticket, in the Service tab of Cisco ANA EventVision. 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 Cisco ANA:

- [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](#)
- [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](#)
- [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
- Members Changed
- Memory Utilization
- MLPPP Bundle
- MPLS Black Hole Found
- MPLS Interface Removed
- MPLS TE FRR State Changed
- MPLS TE Tunnel Down
- OSPF Neighbor State Change
- Port Down
- 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 41-1 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 Maintenance Mode Due to CPU High Usage	Issued when the VNE polling rate is lower but the CPU stays high for several samplings (configurable, default=10). The VNE is automatically moved to the maintenance state, which means it stops polling the device. This state cannot be automatically cleared when the CPU usage decreases; the user must manually change the VNE state from the maintenance state to Start (as described in Cisco Active Network Abstraction 3.7.1 Administrator Guide).

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 41-2 *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 41-3 *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 41-4 **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 mechanism 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 correlate to alarms that are found up to 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 41-5 **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 mechanism 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 correlate up to 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 41-6 **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 41-7 **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 41-7 **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 Cisco ANA 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 41-8 **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, Cisco ANA 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).

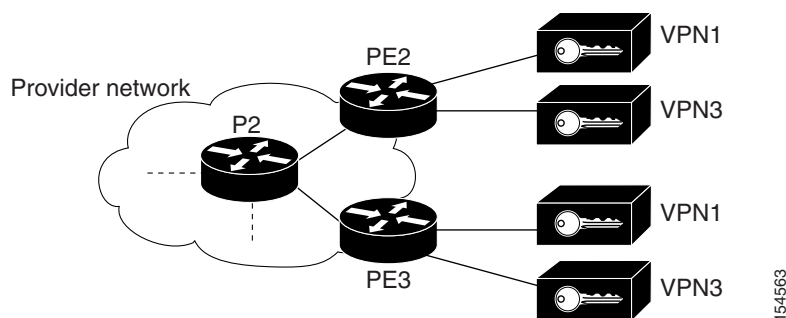
This information is used in the impact analysis process to identify the relevant affected pairs (services).

In the network described in [Figure 41-1](#), 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 41-1 Example of an MPLS Black Hole Scenario



In this case, Cisco ANA 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 41-9 **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 41-10 **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, Cisco ANA NetworkVision 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 Cisco ANA NetworkVision so that you can identify which network element is generating the alarm.

Table 41-11 **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 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 41-12 **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 Cisco ANA 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 41-13 **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 41-14 *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 41-15 **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 41-16 *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 41-17 *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 41-17 *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 41-18 *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 41-19 *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 \(ICgnServiceOid\)](#).

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, Cisco ANA 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 41-20 **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 Cisco ANA), 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 41-21 *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 Cisco ANA 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 41-22 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 Cisco ANA 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.
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 Cisco ANA 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 <code>Enter</code> via the open session and expects to get a prompt back.	General polling is suspended, and a VNE Unreachable event is sent to the Cisco ANA 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, Cisco ANA starts to poll the device using the dedicated reachability command (see [Table 41-22](#)). 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 41-23 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 41-24 *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 41-25 *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 41-26 *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 41-27 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 41-28 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 41-29 **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 41-30 **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.

Table 41-30 DS3 Path Link Down—Subtype Events

Subtype Event Name	Description
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 41-31 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 41-32 *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 41-33 *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 41-34 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 41-35 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 \(IEFPOID\)](#).

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 41-36 **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 41-37 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 41-38 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.

Table 41-38 *HSRP Group Status Changed—Subtype Events (continued)*

Subtype Event Name	Description
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 41-38](#).

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 41-39](#).

Table 41-39 **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 41-39](#).

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 41-40 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 41-41 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 41-42 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 41-43 *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 41-44 *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 Up	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 41-45 **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 \(ITopologicalLinkId\)](#) (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 41-46 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 41-47 **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 Cisco ANA EventVision, 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 41-48 **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 \(IPhysicalLayerOid\)](#).

Local Switching Down

The Local Switching Entry Down Alarm is issued when the status of the local switching entry changes.

Table 41-49 **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 mechanism 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 Cisco ANA 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 41-50 **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 \(ILogicalPortOid\)](#).

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 41-51 **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 41-52 **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 41-53 **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.
MLPPP Down Due To Admin Down	Generated when MLPPP is administratively shut down on either side.

Table 41-53 MLPPP Bundle Service Alarm

Subtype Event Name	Description
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 \(ITopologicalLinkId\)](#), 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.

Table 41-54 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 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 41-55 **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 41-56 *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 Cisco ANA correlation engine 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, Cisco ANA supports the following subalarms for the MPLS 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. Cisco ANA 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 41-57 MPLS TE Tunnel Down—Subtype Events

Subtype Event Name	Description
MPLS TE Tunnel Rerouted	Issued when the tunnel changes its 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 Cisco ANA EventVision, 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. Cisco ANA maps the bit to a high priority alarm.
Medium Priority MPLS TE Tunnel Down	This alarm is issued if the EXP bit is set to denote medium priority. Cisco ANA 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. Cisco ANA maps the bit to a 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.

Impact Analysis

No impact analysis is performed for this alarm.

Source OID

See [MPLS TE Tunnel OID \(IMplsTETunnelOid\)](#).

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 41-58 *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 41-59 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.
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 \(IPhysicalLayerOid\)](#).

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 41-60 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 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 41-61 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 41-62 ***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 41-63 ***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 41-64 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 41-65 Subinterface Down—Subtype Events

Subtype Event Name	Description
Subinterface Down	Issued when the operational status of the subinterface changes from up to down.
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 41-66 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 41-67 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 41-68 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
- 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 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
- Members Changed
- Memory Utilization
- MLPPP Bundle
- MPLS Black Hole Found
- MPLS Interface Removed

- MPLS TE FRR State Changed
- MPLS TE Tunnel Down
- OSPF Neighbor State Change
- Port Down
- 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 41-69 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
	gw-correlation-timeout=1200000
	is-ticketable=true
	send-to-gw=true
	short-description=VNE switched to low polling rate due to CPU high usage

Table 41-70 VNE Switched to Maintenance Mode Due to CPU High 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
	gw-correlation-timeout=1200000
	is-ticketable=true
	send-to-gw=true
	short-description=VNE switched to maintenance mode due to CPU high usage

Table 41-71 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
	gw-correlation-timeout=1200000
	is-ticketable=false
	send-to-gw=true
	short-description=VNE switched back to regular polling rate

All IP Interfaces Down

Table 41-72 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
	gw-correlation-timeout=1200000
	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 41-73 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 41-73 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
	gw-correlation-timeout=1200000
	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 41-74 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 41-74 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
	gw-correlation-timeout=1200000
	is-ticketable=true
	priority=0
	reduction-counter=1
	send-to-gw=true
	severity=CRITICAL
	short-description=ima administratively down

Table 41-75 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
	gw-correlation-timeout=1200000
	is-ticketable=true
	priority=0
	reduction-counter=1
	send-to-gw=true
	severity=MAJOR
	short-description=ima operationally down

Table 41-76 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
	gw-correlation-timeout=1200000
	is-ticketable=true
	priority=0
	reduction-counter=1
	send-to-gw=true
	severity=CRITICAL
	short-description=high priority ima down

Table 41-77 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 41-77 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
	gw-correlation-timeout=1200000
	is-ticketable=true
	priority=0
	reduction-counter=1
	send-to-gw=true
	severity=MAJOR
	short-description=medium priority ima down

Table 41-78 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
	gw-correlation-timeout=1200000
	is-ticketable=true
	priority=0
	reduction-counter=1
	send-to-gw=true
	severity=MINOR
	short-description=low priority ima down

BFD Connectivity Down

Table 41-79 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
	gw-correlation-timeout=1200000
	is-ticketable=true
	send-to-gw=true
	short-description=BFD connectivity down

Table 41-80 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
	gw-correlation-timeout=1200000
	is-ticketable=false
	send-to-gw=true
	short-description=BFD connectivity up

BFD Neighbor Loss

Table 41-81 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
	gw-correlation-timeout=1200000
	is-ticketable=true
	send-to-gw=true
	short-description=BFD neighbor loss

Table 41-82 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
	gw-correlation-timeout=1200000
	is-ticketable=false
	send-to-gw=true
	short-description=BFD neighbor found

BGP Link Down

Table 41-83 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
	gw-correlation-timeout=1200000
	is-ticketable=true
	send-to-gw=true
	short-description=BGP link down due to admin

Table 41-84 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
	gw-correlation-timeout=1200000
	is-ticketable=true
	send-to-gw=true
	short-description=BGP link down due to oper

Table 41-85 *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
	gw-correlation-timeout=1200000
	is-ticketable=true
	send-to-gw=true
	short-description=BGP link down vrf due to admin

Table 41-86 *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
	gw-correlation-timeout=1200000
	is-ticketable=true
	send-to-gw=true
	short-description=BGP link down vrf due to oper

Table 41-87 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
	gw-correlation-timeout=1200000
	is-ticketable=false
	send-to-gw=true
	short-description=BGP link up

BGP Neighbor Loss

Table 41-88 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
	gw-correlation-timeout=1200000
	is-ticketable=false
	send-to-gw=true
	short-description=BGP neighbor found

Table 41-89 *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
	gw-correlation-timeout=1200000
	is-ticketable=true
	send-to-gw=true
	short-description=BGP neighbor loss due to admin

Table 41-90 *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
	gw-correlation-timeout=1200000
	is-ticketable=true
	send-to-gw=true
	short-description=BGP neighbor loss due to oper

Table 41-91 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
	gw-correlation-timeout=1200000
	is-ticketable=true
	send-to-gw=true
	short-description=BGP neighbor loss vrf due to admin

Table 41-92 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
	gw-correlation-timeout=1200000
	is-ticketable=true
	send-to-gw=true
	short-description=BGP neighbor loss vrf due to oper

BGP Process Down

Table 41-93 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
	gw-correlation-timeout=1200000
	is-ticketable=true
	send-to-gw=true
	short-description=BGP process down

Table 41-94 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
	gw-correlation-timeout=1200000
	is-ticketable=false
	send-to-gw=true
	short-description=BGP process up

Broken LSP Discovered

Table 41-95 *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
	gw-correlation-timeout=1200000
	is-ticketable=true
	send-to-gw=true
	short-description=Broken LSP discovered

Card Down

Table 41-96 *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

Table 41-96 Card Down (continued)

Event Setting	Registry Parameter
Northbound metadata	alarm-type=11
	auto-cleared=false
	auto-removed=true
	functionality-type=SERVICE
	severity=MAJOR
	gw-correlation-timeout=1200000
	is-ticketable=true
	send-to-gw=true
	short-description=Card down

Table 41-97 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
	gw-correlation-timeout=1200000
	is-ticketable=false
	send-to-gw=true
	short-description=Card up

Card Out

Table 41-98 Card In

Event Setting	Registry Parameter
Type	card out
Subtype	card in

Table 41-98 *Card In (continued)*

Event Setting	Registry Parameter
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
	gw-correlation-timeout=1200000
	is-ticketable=false
	send-to-gw=true
	short-description=Card in

Table 41-99 *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
	gw-correlation-timeout=1200000
	is-ticketable=true
	send-to-gw=true
	short-description=Card out

Table 41-100 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
	gw-correlation-timeout=1200000
	is-ticketable=true
	send-to-gw=true
	short-description=Card out

Carrier Grade NAT Translations Create Rate

Table 41-101 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

Table 41-101 Carrier Grade NAT Translations Create Rate Higher Threshold Exceeded (continued)

Event Setting	Registry Parameter
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 41-102 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
	gw-correlation-timeout=1200000
	is-ticketable=true
	send-to-gw=true
	short-description=cgn statistics translationsCreate lower threshold exceeded

Table 41-103 Carrier Grade NAT Translations Create Rate Threshold Normal

Event Setting	Registry Parameter
Type	cgn statistics translationsCreate
Subtype	cgn statistics translationsCreate threshold normal

Table 41-103 Carrier Grade NAT Translations Create Rate Threshold Normal (continued)

Event Setting	Registry Parameter
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
	gw-correlation-timeout=1200000
	is-ticketable=false
	send-to-gw=true
	short-description=cgn statistics translationsCreate threshold normal

Carrier Grade NAT Translations Delete Rate

Table 41-104 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
	gw-correlation-timeout=1200000
	is-ticketable=true
	send-to-gw=true
	short-description=cgn statistics translationsDelete higher threshold exceeded

Table 41-105 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
	gw-correlation-timeout=1200000
	is-ticketable=true
	send-to-gw=true
	short-description=cgn statistics translationsDelete lower threshold exceeded

Table 41-106 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
	gw-correlation-timeout=1200000
	is-ticketable=false
	send-to-gw=true
	short-description=cgn statistics translationsDelete threshold normal

Carrier Grade NAT Inside-to-Outside Forward Rate

Table 41-107 Carrier Grade NAT Inside-to-Outside Forward Rate Higher Threshold Exceeded

Event Setting	Registry Parameter
Type	cg_n_statistics_fwdIn2Out
Subtype	cg_n_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
	gw-correlation-timeout=1200000
	is-ticketable=true
	send-to-gw=true
	short-description=cg_n_statistics_fwdIn2Out_higher_threshold_exceeded

Table 41-108 Carrier Grade NAT Inside-to-Outside Forward Rate Lower Threshold Exceeded

Event Setting	Registry Parameter
Type	cg_n_statistics_fwdIn2Out
Subtype	cg_n_statistics_fwdIn2Out_lower_threshold_exceeded
Correlation information	activate-flow=false
	correlate=false
	is-correlation-allowed=false
	weight=0

Table 41-108 Carrier Grade NAT Inside-to-Outside Forward Rate Lower Threshold Exceeded (continued)

Event Setting	Registry Parameter
Northbound metadata	alarm-type=5003
	auto-cleared=false
	auto-removed=true
	functionality-type=SERVICE
	severity=MINOR
	gw-correlation-timeout=1200000
	is-ticketable=true
	send-to-gw=true
	short-description=cgn statistics fwdIn2Out lower threshold exceeded

Table 41-109 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
	gw-correlation-timeout=1200000
	is-ticketable=false
	send-to-gw=true
	short-description=cgn statistics fwdIn2Out threshold normal

Carrier Grade NAT Outside-to-Inside Forward Rate

Table 41-110 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

Table 41-110 Carrier Grade NAT Outside-to-Inside Forward Rate Higher Threshold Exceeded

Event Setting	Registry Parameter
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
	gw-correlation-timeout=1200000
	is-ticketable=true
	send-to-gw=true
	short-description=cgn statistics fwdOut2In higher threshold exceeded

Table 41-111 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
	gw-correlation-timeout=1200000
	is-ticketable=true
	send-to-gw=true
	short-description=cgn statistics fwdOut2In lower threshold exceeded

Table 41-112 *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
	gw-correlation-timeout=1200000
	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 41-113 *Carrier Grade NAT Inside-to-Outside Drops Port Limit Higher Threshold Exceeded*

Event Setting	Registry Parameter
Type	cgn statistics dropsPortLimitIn2Out
Subtype	cgn statistics dropsPortLimitIn2Out higher threshold exceeded
Correlation information	activate-flow=false
	correlate=false
	is-correlation-allowed=false
	weight=0

Table 41-113 Carrier Grade NAT Inside-to-Outside Drops Port Limit Higher Threshold Exceeded

Event Setting	Registry Parameter
Northbound metadata	alarm-type=5005
	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 dropsPortLimitIn2Out higher threshold exceeded

Table 41-114 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
	gw-correlation-timeout=1200000
	is-ticketable=true
	send-to-gw=true
	short-description=cgn statistics dropsPortLimitIn2Out lower threshold exceeded

Table 41-115 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

Table 41-115 Carrier Grade NAT Inside-to-Outside Drops Port Limit Threshold Normal (continued)

Event Setting	Registry Parameter
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
	gw-correlation-timeout=1200000
	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 41-116 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
	gw-correlation-timeout=1200000
	is-ticketable=true
	send-to-gw=true
	short-description=cgn statistics dropsSystemLimitIn2Out higher threshold exceeded

Table 41-117 *Carrier Grade NAT Inside-to-Outside Drops System Limit Reached Lower Threshold Exceeded*

Event Setting	Registry Parameter
Type	cgnsystemstatistics dropsSystemLimitIn2Out
Subtype	cgnsystemstatistics 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
	gw-correlation-timeout=1200000
	is-ticketable=true
	send-to-gw=true
	short-description=cgnsystemstatistics dropsSystemLimitIn2Out lower threshold exceeded

Table 41-118 *Carrier Grade NAT Inside-to-Outside Drops System Limit Reached Threshold Normal*

Event Setting	Registry Parameter
Type	cgnsystemstatistics dropsSystemLimitIn2Out
Subtype	cgnsystemstatistics 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
	gw-correlation-timeout=1200000
	is-ticketable=false
	send-to-gw=true
	short-description=cgnsystemstatistics dropsSystemLimitIn2Out threshold normal

Carrier Grade NAT Inside-to-Outside Drops Resource Depletion

Table 41-119 *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
	gw-correlation-timeout=1200000
	is-ticketable=true
	send-to-gw=true
	short-description=cgn statistics dropsResourceDepletionIn2Out higher threshold exceeded

Table 41-120 *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 41-120 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
	gw-correlation-timeout=1200000
	is-ticketable=true
	send-to-gw=true
	short-description=cgn statistics dropsResourceDepletionIn2Out lower threshold exceeded

Table 41-121 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
	gw-correlation-timeout=1200000
	is-ticketable=false
	send-to-gw=true
	short-description=cgn statistics dropsResourceDepletionIn2Out threshold normal

CFM Domain Fault

Table 41-122 CFM Domain Aggregation Down

Event Setting	Registry Parameter
Type	CFM Domain Fault
Subtype	CFM Domain Aggregation Down
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
	gw-correlation-timeout=9223372036854775807
	is-ticketable=true
	priority=0
	reduction-counter=1
	send-to-gw=true
	severity=INFO
	short-description=CFM Domain fault

Table 41-123 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 41-123 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
	gw-correlation-timeout=1200000
	is-ticketable=false
	priority=0
	reduction-counter=1
	send-to-gw=true
	severity=CLEARED
	short-description=CFM Domain fault cleared

Cloud Problem

Table 41-124 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
	gw-correlation-timeout=1200000
	is-ticketable=true
	send-to-gw=true
	short-description=cloud problem

Table 41-125 *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
	gw-correlation-timeout=1200000
	is-ticketable=false
	send-to-gw=true
	short-description=cloud problem fixed

Component Unreachable

Table 41-126 *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
	gw-correlation-timeout=1200000
	is-ticketable=false
	send-to-gw=true
	short-description=Device Reachable

Table 41-127 *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
	gw-correlation-timeout=1200000
	is-ticketable=true
	send-to-gw=true
	short-description=Device Unreachable

Table 41-128 *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
	gw-correlation-timeout=1200000
	is-ticketable=true
	send-to-gw=true
	short-description=Device Partially Reachable

CPU Utilization

Table 41-129 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
	gw-correlation-timeout=1200000
	is-ticketable=false
	send-to-gw=true
	short-description=CPU utilization less than lower threshold

Table 41-130 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
	gw-correlation-timeout=1200000
	is-ticketable=true
	send-to-gw=true
	short-description=CPU utilization exceeded lower threshold

Device Unsupported

Table 41-131 *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 41-132 *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
	gw-correlation-timeout=1200000
	is-ticketable=true
	send-to-gw=true
	short-description=Device unsupported

Discard Packets

Table 41-133 *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
	gw-correlation-timeout=1200000
	is-ticketable=true
	send-to-gw=true
	short-description=Discarded packet rate exceeded upper threshold

Table 41-134 *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
	gw-correlation-timeout=1200000
	is-ticketable=false
	send-to-gw=true
	short-description=Discarded packet rate is below lower threshold

Dropped Packets

Table 41-135 *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
	gw-correlation-timeout=1200000
	is-ticketable=true
	send-to-gw=true
	short-description=Dropped packet rate exceeded upper threshold

Table 41-136 *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
	gw-correlation-timeout=1200000
	is-ticketable=false
	send-to-gw=true
	short-description=Dropped packet rate is below lower threshold

DS0 Bundle

Table 41-137 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
Northbound metadata	alarm-type=660
	auto-cleared=false
	auto-removed=true
	auto-removed-timeout=5000000
	duplication-counter=1
	functionality-type=SERVICE
	gw-correlation-timeout=1200000
	is-ticketable=true
	priority=0
	reduction-counter=1
	send-to-gw=true
	severity=MAJOR
	short-description=ds0 bundle admin down

Table 41-138 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

Table 41-138 DS0 Bundle Oper 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
	gw-correlation-timeout=1200000
	is-ticketable=true
	priority=0
	reduction-counter=1
	send-to-gw=true
	severity=MAJOR
	short-description=ds0 bundle oper down

Table 41-139 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

Table 41-139 DS0 Bundle Up (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
	gw-correlation-timeout=1200000
	is-ticketable=false
	priority=0
	reduction-counter=1
	send-to-gw=true
	severity=CLEARED
	short-description=ds0 bundle up

DS1 Path Link Down

Table 41-140 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 41-140 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
	gw-correlation-timeout=1200000
	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 41-141 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

Table 41-141 DS1 Path Link Down Due to Oper 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
	gw-correlation-timeout=1200000
	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 41-142 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

Table 41-142 DS1 Path Link Down Due to Card (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
	gw-correlation-timeout=1200000
	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 41-143 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 41-143 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
	gw-correlation-timeout=1200000
	is-ticketable=true
	priority=0
	reduction-counter=1
	send-to-gw=true
	severity=CRITICAL
	short-description=DS1 Path Link down on unreachable

Table 41-144 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

Table 41-144 *DS1 Path Link Up (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
	gw-correlation-timeout=1200000
	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 41-145 *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

Table 41-145 DS1 Path Port Down Due to Admin (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
	gw-correlation-timeout=1200000
	is-ticketable=true
	priority=0
	reduction-counter=1
	send-to-gw=true
	severity=MAJOR
	short-description=DS1 Path down due to Admin

Table 41-146 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 41-146 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
	gw-correlation-timeout=1200000
	is-ticketable=true
	priority=0
	reduction-counter=1
	send-to-gw=true
	severity=MAJOR
	short-description=DS1 Path down due to Oper

Table 41-147 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

Table 41-147 DS1 Path Port Down Due to Card (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
	gw-correlation-timeout=1200000
	is-ticketable=true
	priority=0
	reduction-counter=1
	send-to-gw=true
	severity=MAJOR
	short-description=DS1 Path down due to Card

Table 41-148 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

Table 41-148 DS1 Path Port Up (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
	gw-correlation-timeout=1200000
	is-ticketable=false
	priority=0
	reduction-counter=1
	send-to-gw=true
	severity=CLEARED
	short-description=DS1 Path up

DS3 Path Link Down

Table 41-149 DS3 Path Link Down Due to Admin Down

Event Setting	Registry Parameter
Type	ds3path link down
Subtype	ds3path link down due to admin down
Correlation information	activate-flow=false
	correlate=false
	is-correlation-allowed=true
	root-cause-timeout=420000
	weight=825

Table 41-149 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
	gw-correlation-timeout=1200000
	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 41-150 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

Table 41-150 DS3 Path Link Down Due to Oper 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
	gw-correlation-timeout=1200000
	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 41-151 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

Table 41-151 DS3 Path Link Down Due to Card (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
	gw-correlation-timeout=1200000
	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 41-152 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 41-152 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
	gw-correlation-timeout=1200000
	is-ticketable=true
	priority=0
	reduction-counter=1
	send-to-gw=true
	severity=CRITICAL
	short-description=DS3 Path Link down on unreachable

Table 41-153 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

Table 41-153 DS3 Path Link Up (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
	gw-correlation-timeout=1200000
	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 41-154 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

Table 41-154 DS3 Path Port Down Due to Admin (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
	gw-correlation-timeout=1200000
	is-ticketable=true
	priority=0
	reduction-counter=1
	send-to-gw=true
	severity=MAJOR
	short-description=DS3 Path Down due to Admin

Table 41-155 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 41-155 *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
	gw-correlation-timeout=1200000
	is-ticketable=true
	priority=0
	reduction-counter=1
	send-to-gw=true
	severity=MAJOR
	short-description=DS3 Path Down due to Oper

Table 41-156 *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

Table 41-156 DS3 Path Port Down Due to Card (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
	gw-correlation-timeout=1200000
	is-ticketable=true
	priority=0
	reduction-counter=1
	send-to-gw=true
	severity=MAJOR
	short-description=DS3 Path down due to Card

Table 41-157 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

Table 41-157 DS3 Path Port Up (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
	gw-correlation-timeout=1200000
	is-ticketable=false
	priority=0
	reduction-counter=1
	send-to-gw=true
	severity=MAJOR
	short-description=DS3 Path up

Dual Stack IP Changed

Table 41-158 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 41-158 *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
	gw-correlation-timeout=1200000
	is-ticketable=true
	priority=0
	reduction-counter=1
	send-to-gw=true
	severity=MINOR
	short-description=Dual stack IP removed

Table 41-159 *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

Table 41-159 *Dual Stack IP Added (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
	gw-correlation-timeout=1200000
	is-ticketable=false
	priority=0
	reduction-counter=1
	send-to-gw=true
	severity=CLEARED
	short-description=Dual stack IP added

DWDM Controller

Table 41-160 *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

Table 41-160 DWDM Controller Down (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
	gw-correlation-timeout=1200000
	is-ticketable=true
	priority=0
	reduction-counter=1
	send-to-gw=true
	severity=MAJOR
	short-description=dwdm controller down

Table 41-161 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 41-161 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
	gw-correlation-timeout=1200000
	is-ticketable=false
	priority=0
	reduction-counter=1
	send-to-gw=true
	severity=CLEARED
	short-description=dwdm controller up

DWDM G709 Status

Table 41-162 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 41-162 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
	gw-correlation-timeout=1200000
	is-ticketable=true
	priority=0
	reduction-counter=1
	send-to-gw=true
	severity=MINOR
	short-description=dwdm g709 status down

Table 41-163 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

Table 41-163 DWDM G709 Status Up (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
	gw-correlation-timeout=1200000
	is-ticketable=false
	priority=0
	reduction-counter=1
	send-to-gw=true
	severity=CLEARED
	short-description=dwdm g709 status up

EFP Down

Table 41-164 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
	gw-correlation-timeout=1200000
	is-ticketable=true
	send-to-gw=true
	short-description=EFP admin down

Table 41-165 *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
	gw-correlation-timeout=1200000
	is-ticketable=true
	send-to-gw=true
	short-description=EFP down due to error disabled

Table 41-166 *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
	gw-correlation-timeout=1200000
	is-ticketable=true
	send-to-gw=true
	short-description=EFP oper down

Table 41-167 *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
	gw-correlation-timeout=1200000
	is-ticketable=false
	send-to-gw=true
	short-description=EFP up

GRE Keepalive

Table 41-168 *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

Table 41-168 *Keepalive Not 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
	gw-correlation-timeout=1200000
	is-ticketable=true
	priority=0
	reduction-counter=1
	send-to-gw=true
	severity=MINOR
	short-description=keepalive not configured

Table 41-169 *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
Northbound metadata	alarm-type=915
	auto-cleared=false
	auto-removed=true
	auto-removed-timeout=5000000
	duplication-counter=1
	functionality-type=SERVICE
	gw-correlation-timeout=1200000
	is-ticketable=false
	priority=0
	reduction-counter=1
	send-to-gw=true
	severity=CLEARED
	short-description=keepalive configured

GRE Tunnel Down

Table 41-170 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
	gw-correlation-timeout=1200000
	is-ticketable=true
	send-to-gw=true
	short-description=GRE tunnel down

Table 41-171 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
	gw-correlation-timeout=1200000
	is-ticketable=false
	send-to-gw=true
	short-description=GRE tunnel up

HSRP Group Status Changed

Table 41-172 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
	gw-correlation-timeout=1200000
	is-ticketable=false
	send-to-gw=true
	short-description=Primary HSRP interface is active

Table 41-173 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
	gw-correlation-timeout=1200000
	is-ticketable=true
	send-to-gw=true
	short-description=Primary HSRP interface is not active

Table 41-174 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
	gw-correlation-timeout=1200000
	is-ticketable=true
	send-to-gw=true
	short-description=Secondary HSRP interface is active

Table 41-175 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
	gw-correlation-timeout=1200000
	is-ticketable=false
	send-to-gw=true
	short-description=Secondary HSRP interface is not active

Interface Status

Table 41-176 *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
	gw-correlation-timeout=1200000
	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 41-177 *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

Table 41-177 *Interface Status Down Connection (continued)*

Event Setting	Registry Parameter
Northbound metadata	alarm-type=700
	auto-cleared=false
	auto-removed=true
	functionality-type=SERVICE
	severity=MAJOR
	gw-correlation-timeout=1200000
	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 41-178 *Interface Status Down Nonconnection*

Event Setting	Registry Parameter
Type	interface status
Subtype	interface status down non connection
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
	gw-correlation-timeout=1200000
	is-ticketable=true
	send-to-gw=true
	short-description=Interface status down

Table 41-178 *Interface Status Down Nonconnection (continued)*

Event Setting	Registry Parameter
Flapping information	clear-interval=240000
	flapping-interval=60000
	flapping-threshold=5
	update-interval=200000
	update-threshold=20

Table 41-179 *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
	gw-correlation-timeout=1200000
	is-ticketable=false
	send-to-gw=true
	short-description=Interface status up
Flapping information	clear-interval=240000
	flapping-interval=60000
	flapping-threshold=5
	update-interval=200000
	update-threshold=20

Investigation State

Table 41-180 *Investigation State*

Event Setting	Registry Parameter
Type	investigation state
Subtype	investigation state module unsupported

Table 41-180 Investigation State (continued)

Event Setting	Registry Parameter
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
	gw-correlation-timeout=1200000
	is-ticketable=true
	send-to-gw=true
	short-description=Module unsupported

L2TP Peer Not Established

Table 41-181 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
Northbound metadata	alarm-type=185
	auto-cleared=false
	auto-removed=true
	functionality-type=SERVICE
	severity=CLEARED
	gw-correlation-timeout=1200000
	is-ticketable=false
	send-to-gw=true
	short-description=l2tp peer established

Table 41-181 L2TP Peer Established (continued)

Event Setting	Registry Parameter
Flapping information	clear-interval=240000
	flapping-interval=60000
	flapping-threshold=5
	update-interval=200000
	update-threshold=20

Table 41-182 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
	gw-correlation-timeout=1200000
	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 41-183 L2TP Peer Not Established

Event Setting	Registry Parameter
Type	l2tp peer not established
Subtype	l2tp peer not established

Table 41-183 L2TP Peer Not Established (continued)

Event Setting	Registry Parameter
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
	gw-correlation-timeout=1200000
	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 41-184 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 41-184 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
	gw-correlation-timeout=1200000
	is-ticketable=true
	send-to-gw=true
	short-description=l2tp sessions count exceeds max threshold

Table 41-185 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
	gw-correlation-timeout=1200000
	is-ticketable=false
	send-to-gw=true
	short-description=l2tp sessions count has returned to normal

Lag Down

Table 41-186 Lag Admin Down

Event Setting	Registry Parameter
Type	lag down
Subtype	lag admin down

Table 41-186 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
	gw-correlation-timeout=1200000
	is-ticketable=true
	send-to-gw=true
	short-description=Lag down due to admin down

Table 41-187 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
	gw-correlation-timeout=1200000
	is-ticketable=true
	send-to-gw=true
	short-description=Lag down due to oper down

Table 41-188 *Lag Up*

Event Setting	Registry Parameter
Type	lag down
Subtype	lag up
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
	gw-correlation-timeout=1200000
	is-ticketable=false
	send-to-gw=true
	short-description=Lag up

Lag Link Down

Table 41-189 *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
	gw-correlation-timeout=1200000
	is-ticketable=true
	send-to-gw=true
	short-description=Lag link down due to admin down

Table 41-190 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
	gw-correlation-timeout=1200000
	is-ticketable=true
	send-to-gw=true
	short-description=Lag link down due to oper down

Table 41-191 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
	gw-correlation-timeout=1200000
	is-ticketable=false
	send-to-gw=true
	short-description=Lag link up

Layer 2 Tunnel Down

Table 41-192 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
	gw-correlation-timeout=1200000
	is-ticketable=true
	send-to-gw=true
	short-description=Layer 2 tunnel down

Table 41-193 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
	gw-correlation-timeout=1200000
	is-ticketable=false
	send-to-gw=true
	short-description=Layer 2 tunnel up

LDP Neighbor Loss

Table 41-194 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
	gw-correlation-timeout=1200000
	is-ticketable=true
	send-to-gw=true
	short-description=LDP neighbor down

Table 41-195 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
	gw-correlation-timeout=1200000
	is-ticketable=false
	send-to-gw=true
	short-description=LDP neighbor up

Link Down

Table 41-196 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
	gw-correlation-timeout=1200000
	is-ticketable=true
	send-to-gw=true
	short-description=Link down due to admin down
Flapping information	clear-interval=360000
	flapping-interval=150000
	flapping-threshold=5
	update-interval=200000
	update-threshold=20

Table 41-197 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

Table 41-197 Link Down Due to Card Event (continued)

Event Setting	Registry Parameter
Northbound metadata	alarm-type=1
	auto-cleared=false
	auto-removed=true
	functionality-type=SERVICE
	severity=CRITICAL
	gw-correlation-timeout=1200000
	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 41-198 Link Down Due to Oper Down

Event Setting	Registry Parameter
Type	link down
Subtype	link down due to oper down
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
	gw-correlation-timeout=1200000
	is-ticketable=true
	send-to-gw=true
	short-description=Link down due to oper down

Table 41-198 *Link 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 41-199 *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
	gw-correlation-timeout=1200000
	is-ticketable=true
	send-to-gw=true
	short-description=Link down on unreachable
Flapping information	clear-interval=360000
	flapping-interval=150000
	flapping-threshold=5
	update-interval=200000
	update-threshold=20

Table 41-200 *Link Up*

Event Setting	Registry Parameter
Type	link down
Subtype	link up

Table 41-200 *Link Up (continued)*

Event Setting	Registry Parameter
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
	gw-correlation-timeout=1200000
	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 41-201 *Link Overutilized*

Event Setting	Registry Parameter
Type	link utilization
Subtype	link over Utilized
Correlation information	activate-flow=false
	correlate=true
	is-correlation-allowed=true
	weight=0

Table 41-201 *Link Overutilized (continued)*

Event Setting	Registry Parameter
Northbound metadata	alarm-type=642
	auto-cleared=false
	auto-removed=true
	functionality-type=SERVICE
	severity=MINOR
	gw-correlation-timeout=1200000
	is-ticketable=true
	send-to-gw=true
	short-description=Link over utilized

Table 41-202 *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
	gw-correlation-timeout=1200000
	is-ticketable=false
	send-to-gw=true
	short-description=Link utilization normal

Local Switching Down

Table 41-203 *Local Switching Entry Down*

Event Setting	Registry Parameter
Type	local switching down
Subtype	local switching down

Table 41-203 Local Switching Entry Down (continued)

Event Setting	Registry Parameter
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
	gw-correlation-timeout=1200000
	is-ticketable=true
	send-to-gw=true
	short-description=Local switching entry down

Table 41-204 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
	gw-correlation-timeout=1200000
	is-ticketable=false
	send-to-gw=true
	short-description=Local switching entry up

Logical Port Down

Table 41-205 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
	gw-correlation-timeout=1200000
	is-ticketable=true
	send-to-gw=true
	short-description=Logical port down

Table 41-206 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
	gw-correlation-timeout=1200000
	is-ticketable=false
	send-to-gw=true
	short-description=Logical port up

Members Changed

Table 41-207 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
	gw-correlation-timeout=1200000
	is-ticketable=true
	send-to-gw=true
	short-description=High priority member down

Table 41-208 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
	gw-correlation-timeout=1200000
	is-ticketable=true
	send-to-gw=true
	short-description=Medium priority member down

Table 41-209 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
	gw-correlation-timeout=1200000
	is-ticketable=true
	send-to-gw=true
	short-description=Low priority member down

Table 41-210 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
	gw-correlation-timeout=1200000
	is-ticketable=false
	send-to-gw=true
	short-description=All members operationally up

Memory Utilization

Table 41-211 *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
	gw-correlation-timeout=1200000
	is-ticketable=false
	send-to-gw=true
	short-description=Memory utilization less than normal threshold

Table 41-212 *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
	gw-correlation-timeout=1200000
	is-ticketable=true
	send-to-gw=true
	short-description=Memory utilization exceeded upper threshold

MLPPP Bundle

Table 41-213 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
	gw-correlation-timeout=1200000
	is-ticketable=true
	priority=0
	reduction-counter=1
	send-to-gw=true
	severity=MAJOR
	short-description=mlppp down flapping

Table 41-214 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 41-214 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
	gw-correlation-timeout=1200000
	is-ticketable=true
	priority=0
	reduction-counter=1
	send-to-gw=true
	severity=MAJOR
	short-description=mlppp down flapping update

Table 41-215 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
	gw-correlation-timeout=1200000
	is-ticketable=true
	priority=0
	reduction-counter=1
	send-to-gw=true
	severity=CRITICAL
	short-description=mlppp administratively down

Table 41-216 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
	gw-correlation-timeout=1200000
	is-ticketable=false
	priority=0
	reduction-counter=1
	send-to-gw=false
	severity=INFO
	short-description=mlppp down flapping proxy

Table 41-217 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 41-217 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
	gw-correlation-timeout=1200000
	is-ticketable=true
	priority=0
	reduction-counter=1
	send-to-gw=true
	severity=MAJOR
	short-description=mlppp operationally down

Table 41-218 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
	gw-correlation-timeout=1200000
	is-ticketable=false
	priority=0
	reduction-counter=1
	send-to-gw=true
	severity=CLEARED
	short-description=mlppp up

MPLS Black Hole Found

An MPLS black hole is defined as an abnormal termination of an MPLS path (LSP) inside an MPLS network. An MPLS black hole exists when on a specific interface there are untagged entries destined for a known PE router. It is assumed that a router functions as a PE router if services, such as L3 VPNs or pseudowire (L2 VPN) MPLS tunnels, are using the MPLS network. Note that the untagged interfaces may exist in the network in normal situations; for example, where the boundary of the MPLS cloud has untagged interfaces.

An MPLS black hole causes the loss of all MPLS labels on a packet, including the VPN information that lies in the inner MPLS label. If a packet goes through an untagged interface, the VPN information is lost. The VPN information loss causes VPN sites to lose connectivity.

MPLS Black Hole Found alarms are actively detected. Service alarms are generated whenever Cisco ANA discovers an MPLS interface with at least one untagged LSP leading to a known PE router.

Black hole alarms are detected either:

- When the system is loaded for the first time and performs the initial discovery of the network.
- Through the ongoing discovery process, which identifies changes in the network.



Note

MPLS black hole discovery is supported only when the PEs are managed by Cisco ANA.

Table 41-219 *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
	gw-correlation-timeout=1200000
	is-ticketable=false
	send-to-gw=true
	short-description=MPLS Black hole cleared

Table 41-220 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
	gw-correlation-timeout=1200000
	is-ticketable=true
	send-to-gw=true
	short-description=MPLS Black hole found

MPLS Interface Removed

Table 41-221 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
Northbound metadata	alarm-type=972
	auto-cleared=false
	auto-removed=true
	functionality-type=SERVICE
	severity=CLEARED
	gw-correlation-timeout=1200000
	is-ticketable=false
	send-to-gw=true
	short-description=MPLS interface added

Table 41-222 *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
	gw-correlation-timeout=1200000
	is-ticketable=true
	send-to-gw=true
	short-description=MPLS interface removed

MPLS TE FRR State Changed

Table 41-223 *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
Correlation information	activate-flow=true
	correlate=true
	is-correlation-allowed=true
	root-cause-timeout=420000
	weight=700

Table 41-223 MPLS TE FRR State Changed to Active (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
	gw-correlation-timeout=1200000
	is-ticketable=true
	priority=0
	reduction-counter=1
	send-to-gw=true
	severity=MAJOR
	short-description=MPLS TE FRR State Changed to Active

Table 41-224 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 41-224 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
	gw-correlation-timeout=1200000
	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 41-225 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
	gw-correlation-timeout=1200000
	is-ticketable=true
	send-to-gw=true
	short-description=MPLS TE tunnel down

Table 41-225 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 41-226 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
	gw-correlation-timeout=1200000
	is-ticketable=true
	send-to-gw=true
Flapping information	short-description=High Priority MPLS-TE tunnel down
	clear-interval=240000
	flapping-interval=60000
	flapping-threshold=5
	update-interval=200000
	update-threshold=20

Table 41-227 Medium Priority MPLS TE Tunnel Down

Event Setting	Registry Parameter
Type	mpls te tunnel down
Subtype	Medium Priority mpls te tunnel down

Table 41-227 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
	gw-correlation-timeout=1200000
	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 41-228 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

Table 41-228 Low Priority MPLS TE Tunnel Down (continued)

Event Setting	Registry Parameter
Northbound metadata	alarm-type=555
	auto-cleared=false
	auto-removed=true
	functionality-type=SERVICE
	severity=MINOR
	gw-correlation-timeout=1200000
	is-ticketable=true
	send-to-gw=true
	short-description=Low Priority MPLS-TE tunnel down
Flapping information	clear-interval=240000
	flapping-interval=60000
	flapping-threshold=5
	update-interval=200000
	update-threshold=20

Table 41-229 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
	gw-correlation-timeout=1200000
	is-ticketable=true
	send-to-gw=true
	short-description=MPLS-TE tunnel reoptimized

Table 41-229 MPLS TE Tunnel Reoptimized (continued)

Event Setting	Registry Parameter
Flapping information	clear-interval=240000
	flapping-interval=60000
	flapping-threshold=5
	update-interval=200000
	update-threshold=20

Table 41-230 MPLS TE Tunnel Rerouted

Event Setting	Registry Parameter
Type	mpls te tunnel down
Subtype	mpls te tunnel rerouted
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
	gw-correlation-timeout=1200000
	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 41-231 MPLS TE Tunnel Up

Event Setting	Registry Parameter
Type	mpls te tunnel down
Subtype	mpls te tunnel up

Table 41-231 MPLS TE Tunnel Up (continued)

Event Setting	Registry Parameter
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
	gw-correlation-timeout=1200000
	is-ticketable=false
	send-to-gw=true
	short-description=MPLS-TE tunnel up
Flapping information	clear-interval=240000
	flapping-interval=60000
	flapping-threshold=5
	update-interval=200000
	update-threshold=20

OSPF Neighbor State Change

Table 41-232 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

Table 41-232 *OSPF Neighbor Down (continued)*

Event Setting	Registry Parameter
Northbound metadata	alarm-type=1350
	auto-cleared=false
	auto-removed=true
	functionality-type=SERVICE
	severity=MAJOR
	gw-correlation-timeout=1200000
	is-ticketable=true
	send-to-gw=true
	short-description=OSPF Neighbor Down

Table 41-233 *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
	gw-correlation-timeout=1200000
	is-ticketable=false
	send-to-gw=true
	short-description=OSPF Neighbor Up

Port Down

Table 41-234 *Port Down Due to Admin*

Event Setting	Registry Parameter
Type	port down
Subtype	port down due to admin

Table 41-234 Port Down Due to Admin (continued)

Event Setting	Registry Parameter
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
	gw-correlation-timeout=1200000
	is-ticketable=true
	send-to-gw=true
	short-description=Port down due to admin
Flapping information	clear-interval=360000
	flapping-interval=150000
	flapping-threshold=5
	update-interval=200000
	update-threshold=20

Table 41-235 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

Table 41-235 Port Down Due to Oper (continued)

Event Setting	Registry Parameter
Northbound metadata	alarm-type=2
	auto-cleared=false
	auto-removed=true
	functionality-type=SERVICE
	severity=MAJOR
	gw-correlation-timeout=1200000
	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 41-236 Port Down Due to Card Event

Event Setting	Registry Parameter
Type	port down
Subtype	port down due to card
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
	gw-correlation-timeout=1200000
	is-ticketable=true
	send-to-gw=true
	short-description=Port down due to Card event

Table 41-236 Port Down Due to Card Event (continued)

Event Setting	Registry Parameter
Flapping information	clear-interval=360000
	flapping-interval=150000
	flapping-threshold=5
	update-interval=200000
	update-threshold=20

Table 41-237 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
	gw-correlation-timeout=1200000
	is-ticketable=false
	send-to-gw=true
Flapping information	short-description=Port up
	clear-interval=360000
	flapping-interval=150000
	flapping-threshold=5
	update-interval=200000
	update-threshold=20

Rx Dormant

Table 41-238 Rx Dormant

Event Setting	Registry Parameter
Type	rx dormant
Subtype	rx dormant

Table 41-238 Rx Dormant (continued)

Event Setting	Registry Parameter
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
	gw-correlation-timeout=1200000
	is-ticketable=true
	send-to-gw=true
	short-description=rx dormant

Table 41-239 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
	gw-correlation-timeout=1200000
	is-ticketable=false
	send-to-gw=true
	short-description=rx dormant normal

Rx Utilization

Table 41-240 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
	gw-correlation-timeout=1200000
	is-ticketable=true
	send-to-gw=true
	short-description=Rx utilization exceeded upper threshold

Table 41-241 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
	gw-correlation-timeout=1200000
	is-ticketable=false
	send-to-gw=true
	short-description=Rx utilization is below lower threshold

Shelf Out

Table 41-242 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
	gw-correlation-timeout=1200000
	is-ticketable=false
	send-to-gw=true
	short-description=Shelf in

Table 41-243 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
	gw-correlation-timeout=1200000
	is-ticketable=true
	send-to-gw=true
	short-description=Shelf out

SONET Path Link Down

Table 41-244 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
	gw-correlation-timeout=1200000
	is-ticketable=true
	send-to-gw=true
	short-description=SONET Path Link down due to admin down
Flapping information	clear-interval=360000
	flapping-interval=150000
	flapping-threshold=5
	update-interval=200000
	update-threshold=20

Table 41-245 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

Table 41-245 SONET Path Link Down Due to Oper Down (continued)

Event Setting	Registry Parameter
Northbound metadata	alarm-type=1345
	auto-cleared=false
	auto-removed=true
	functionality-type=SERVICE
	severity=CRITICAL
	gw-correlation-timeout=1200000
	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 41-246 SONET Path Link Down Due to Card

Event Setting	Registry Parameter
Type	sonetpath link down
Subtype	sonetpath link down due to card
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
	gw-correlation-timeout=1200000
	is-ticketable=true
	send-to-gw=true
	short-description=SONET Path Link down due to Card event

Table 41-246 SONET Path Link Down Due to Card (continued)

Event Setting	Registry Parameter
Flapping information	clear-interval=360000
	flapping-interval=150000
	flapping-threshold=5
	update-interval=200000
	update-threshold=20

Table 41-247 SONET Path Link Down on Unreachable

Event Setting	Registry Parameter
Type	sonetpath link down
Subtype	sonetpath link down 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
	gw-correlation-timeout=1200000
	is-ticketable=true
	send-to-gw=true
Flapping information	short-description=SONET Path Link down on unreachable
	clear-interval=360000
	flapping-interval=150000
	flapping-threshold=5
	update-interval=200000
	update-threshold=20

Table 41-248 SONET Path Link Up

Event Setting	Registry Parameter
Type	sonetpath link down
Subtype	sonetpath link up

Table 41-248 *SONET Path Link Up (continued)*

Event Setting	Registry Parameter
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
	gw-correlation-timeout=1200000
	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 41-249 *SONET Path Port Down Due to Admin Down*

Event Setting	Registry Parameter
Type	sonetpath port down
Subtype	sonetpath port down due to admin
Correlation information	activate-flow=true
	correlate=true
	is-correlation-allowed=true
	weight=840

Table 41-249 SONET Path Port Down Due to Admin Down (continued)

Event Setting	Registry Parameter
Northbound metadata	alarm-type=1333
	auto-cleared=false
	auto-removed=true
	functionality-type=SERVICE
	severity=MAJOR
	gw-correlation-timeout=1200000
	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 41-250 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
	gw-correlation-timeout=1200000
	is-ticketable=true
	send-to-gw=true
	short-description=SONET Path down due to Oper

Table 41-250 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 41-251 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
	gw-correlation-timeout=1200000
	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 41-252 SONET Path Port Up

Event Setting	Registry Parameter
Type	sonetpath port down
Subtype	sonetpath port up

Table 41-252 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
	gw-correlation-timeout=1200000
	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 41-253 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 41-253 Subinterface Down (continued)

Event Setting	Registry Parameter
Northbound metadata	alarm-type=917
	auto-cleared=false
	auto-removed=true
	functionality-type=SERVICE
	severity=MAJOR
	gw-correlation-timeout=1200000
	is-ticketable=true
	send-to-gw=true
	short-description=VLAN Sub Interface oper down

Table 41-254 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
	gw-correlation-timeout=1200000
	is-ticketable=true
	send-to-gw=true
	short-description=VLAN Sub Interface admin down

Table 41-255 Subinterface Up

Event Setting	Registry Parameter
Type	sub-interface down
Subtype	sub-interface up

Table 41-255 Subinterface Up (continued)

Event Setting	Registry Parameter
Correlation information	activate-flow=false
	correlate=false
	is-correlation-allowed=false
	weight=0
Northbound metadata	alarm-type=917
	auto-cleared=false
	auto-removed=true
	functionality-type=SERVICE
	severity=CLEARED
	gw-correlation-timeout=1200000
	is-ticketable=false
	send-to-gw=true
	short-description=VLAN Sub Interface up

Tx Dormant

Table 41-256 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
	gw-correlation-timeout=1200000
	is-ticketable=true
	send-to-gw=true
	short-description=tx dormant

Table 41-257 Tx Dormant Normal

Event Setting	Registry Parameter
Type	tx dormant
Subtype	tx dormant normal
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
	gw-correlation-timeout=1200000
	is-ticketable=false
	send-to-gw=true
	short-description=tx dormant normal

Tx Utilization

Table 41-258 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
	gw-correlation-timeout=1200000
	is-ticketable=true
	send-to-gw=true
	short-description=Tx utilization exceeded upper threshold

Table 41-259 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
	gw-correlation-timeout=1200000
	is-ticketable=false
	send-to-gw=true
	short-description=Tx utilization is below lower threshold

VSI Down

Table 41-260 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
	gw-correlation-timeout=1200000
	is-ticketable=true
	send-to-gw=true
	short-description=VSI oper down

Table 41-261 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
	gw-correlation-timeout=1200000
	is-ticketable=true
	send-to-gw=true
	short-description=VSI admin down

Table 41-262 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
	gw-correlation-timeout=1200000
	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 Cisco ANA. 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 \(ICgnServiceOid\)](#)
- [DS0 Bundle OID \(IDS0BundleOid\)](#)
- [DS1 Path OID \(IDS1PathOid\)](#)
- [DS3 Path OID \(IDS3PathOid\)](#)
- [DWDM Controller OID \(IDWDMOid\)](#)
- [EFP OID \(IEFPOID\)](#)
- [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 \(IMplsTETunnelOid\)](#)
- [OSPF Neighbor State Change 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=Default context)] [BfdService] }) (LinkType=14) (TunnelID=-1) (ZEndPoint={ [ManagedElement (Key=c3-npe1-76)] [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] [BgpNeighborEntry (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)] }
```


DS0 Bundle OID (IDS0BundleOid)

The DS0 Bundle OID is the source OID for any alarms related to DS0 Bundle.

The alarm supported by Cisco ANA 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_SdhHo
p(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_SdhHo
p(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 (IDWDM0id)

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] [BgpNeighbourEntry (PeerIdentifier=10.0.7.4) (VrfName=Red)] }
```

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 (Type=type)] [IMAGroup (Id=IMAGroupID)] }
```

Example

```
{ [ManagedElement (Key=vne-146)] [LogicalRoot] [PhysicalLayerAggregationContainer (Type=1)] [IMAGroup (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 Cisco ANA 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)][RoutingEntity][IpInterface(IpInterfaceName=ifName)]}
```
- IP interface under a VRF:

```
{[ManagedElement(Key=deviceName)][LogicalRoot][FWComponentContainer(Type=3)][Vrf(VrfName=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=vrfA)][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 similar to Lag Down OID.

L2TP Peer OID (IL2tpPeerOid)

Layer 2 Tunneling Protocol (L2TP) modeling in Cisco ANA 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 Cisco ANA 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)] [FWComponentContainer(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 Cisco ANA.

The Logical Port OID is the source OID for any alarms related to logical ports.

The alarm supported by Cisco ANA 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)] }
```

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 Cisco ANA 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 Cisco ANA 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] [ServiceEvent (DiffObject=MPLS on interface FastEthernet0/1)] }
```

```
{ [ManagedElement (Key=PE4-NY-7200)] [LogicalRoot] [FWComponentContainer (Type=4)] [Lse] [ServiceEvent (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] [ServiceEvent (DiffObject=172.255.0.1:0)] }
```

```
{ [ManagedElement (Key=CORE2-NY-GSR)] [LogicalRoot] [FWComponentContainer (Type=4)] [Lse] [ServiceEvent (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 Cisco ANA 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 Cisco ANA 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 41-191).

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)][OspfProcess(OspfVersion=v2)(ProcessId=1)][OspfNeighbor(AreaId=0)(IfName=TenGigabitEthernet2/4)(OspfNeighborId=10.10.20.3)]}
```

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 similar 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 Cisco ANA 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 41-198](#).



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 41-199](#).
- 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 41-199](#).
- 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 41-199](#).
- DS1 Path Link Down—See [DS1 Path Link Down, page 41-28](#).
- DS3 Path Link Down—See [DS3 Path Link Down, page 41-29](#).
- MLPPP Down Due to Admin Down—See [MLPPP Bundle, page 41-46](#).
- MLPPP Down Due to Oper Down—See [MLPPP Bundle, page 41-46](#).

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) (ZEndPoint={ [ManagedElement (Key=PE1-NY-GSR) ] [PhysicalRoot] [Chassis] [Slot (SlotNum=1) ] [Module] [Slot (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)] [PhysicalLayer] }) (TunnelID=-1) (ZEndPoint={ [ManagedElement (Key=NPE1-NY-7600)] [PhysicalRoot] [Chassis] [Slot (SlotNum=4)] [Module] [Port (PortNumber=FastEthernet4/48)] [PhysicalLayer] }) ] }
```

See also, [DS3 Path OID \(IDS3PathOid\)](#), page 41-189, [DS3 Path OID \(IDS3PathOid\)](#), page 41-189, [MLPPP OID \(IMLPPPOid\)](#), page 41-195.

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 (ContextName=Default context)] [TunnelContainer (TunnelType=4)] [TunnelGre (TunnelName=Tunnel1)] }) (TunnelID=-1) (ZEndPoint={ [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 (ContextName=Default context)] [TunnelContainer (TunnelType=1)] [PTPLayer2MplsTunnel (PeerRouterIp=172.255.1.5) (TunnelId=100)] }) (TunnelID=) (ZEndPoint={ [ManagedElement (Key=PE4-NY-7200)] [LogicalRoot] [Context (ContextName=Default context)] [TunnelContainer (TunnelType=1)] [PTPLayer2MplsTunnel (PeerRouterIp=172.255.1.3) (TunnelId=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] [FWComponentContainer (Type=7)] [MpBgp] }) (TunnelID=-1) (ZEndPoint={ [ManagedElement (Key=RR2-IOU-159)] [LogicalRoot] [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] [VlanEncapMux] [VLANTaggedInterface (InterfaceName=Gi4/0/2.1)] }
```

VSI OID (IVSI OID)

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 42

Traps

This section describes the Cisco ANA traps. Traps appear in the Cisco ANA EventVision V1 Trap, V2 Trap, and V3 Trap tabs. (For information about Cisco ANA EventVision, see the [Cisco Active Network Abstraction 3.7.1 User Guide](#).) Trap information is presented in two forms:

- **Trap Tables**—A section devoted to the supported traps 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 Cisco ANA-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 Cisco ANA EventVision. 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 Cisco ANA 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 Cisco ANA 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. Cisco ANA natively supports SNMP informs and SNMP V3 AuthNoPriv and AuthPriv options.

Cisco ANA 3.7.1 users can enable an additional IP in the device for traps and syslogs. This new feature is called Multisource Events. When Cisco ANA 3.7.1 receives a trap or syslog from that device (from the new IP) it will still recognize the device. For more details on multisource events see [Cisco ANA 3.7.1 Release notes](#).

This chapter includes the following sections:

- [Cisco ASR 9000 V1 Traps, page 42-3](#)
- [Cisco ASR 9000 V2/V3 Traps, page 42-4](#)
- [Cisco IOS V1 Traps, page 42-6](#)
- [Cisco IOS V2/V3 Traps, page 42-62](#)
- [Cisco IOX V1 Traps, page 42-90](#)
- [Cisco IOX V2/V3 Traps, page 42-103](#)
- [Cisco MIB2 V1 Traps, page 42-119](#)
- [Cisco MIB2 V2/V3 Traps, page 42-129](#)
- [Cisco ACE V1 Traps, page 42-139](#)
- [Cisco ACE V2/V3 Traps, page 42-140](#)

- [Cisco Nexus V1 Traps, page 42-141](#)
- [Cisco Nexus V2/V3 Traps, page 42-154](#)
- [Cisco ASR 9000 V1 Trap Registry Parameters, page 42-161](#)
- [Cisco ASR 9000 V2/V3 Registry Parameters, page 42-162](#)
- [Cisco IOS V1 Trap Registry Parameters, page 42-163](#)
- [Cisco IOS V2/V3 Trap Registry Parameters, page 42-188](#)
- [Cisco IOX V1 Trap Registry Parameters, page 42-209](#)
- [Cisco IOX V2/V3 Trap Registry Parameters, page 42-218](#)
- [Cisco MIB2 V1 Trap Registry Parameters, page 42-229](#)
- [Cisco MIB2 V2/V3 Trap Registry Parameters, page 42-237](#)
- [Cisco ACE V1 Trap Registry Parameters, page 42-245](#)
- [Cisco ACE V2/V3 Trap Registry Parameters, page 42-246](#)
- [Cisco Nexus V1 Trap Registry Parameters, page 42-247](#)
- [Cisco Nexus V2/V3 Trap Registry Parameters, page 42-251](#)

**Note**

Cisco IOS devices, Cisco XR 12000 Series and the Cisco CRS-1 Carrier Routing System must be configured to send traps in SNMP V2.

Cisco ASR 9000 V1 Traps

Table 42-1 lists the Cisco ASR 9000 SNMP V1 traps supported in Cisco ANA. For associated event types, event subtypes, and Cisco ANA registry parameters, use the link under Short Description or see Table 42-13.

Table 42-1 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	1.0.8802.1.1.3.1.3.1.1.2.802.1.1.8	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	1.0.8802.1.1.3.1.3.1.1.2.802.1.1.8	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 42-2 lists the Cisco ASR 9000 SNMP V2/V3 traps supported in Cisco ANA. For associated event types, event subtypes, and Cisco ANA registry parameters, use the link in the Short Description column or see Table 42-14.

Table 42-2 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 42-2 Cisco ASR 9000 V2 Traps (continued)

Trap Name	Trap OID	Subtype Varbind OID	Subtype Varbind Value	Description	Short Description
dot1agCfmFaultAlarm	1.0.8802.1.1.3.0.11.3.11.2.802.1.1.8.0.1	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	1.0.8802.1.1.3.0.11.3.11.2.802.1.1.8.0.1	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 42-3 lists the Cisco IOS SNMP V1 traps supported in Cisco ANA. For associated event types, event subtypes, and Cisco ANA registry parameters, use the link under Short Description or see Table 42-15.

Table 42-3 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 Temperature
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 Temperature
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 Temperature - 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.	Temperature 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 42-3 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 42-3 Cisco IOS V1 Traps (continued)

Trap Name	Generic Type	Specific Type	Enterprise OID	Subtype Varbind OID	Subtype Varbind Value	Description	Short Description
cEtherCfmCcMep Up	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
cEtherCfmCcMep Down	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 agent's configuration or the protocol entity implementation may be altered.	Cold start trap

Table 42-3 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 42-3 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 any of the status : 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 any of the status : acceptable, warning, overloaded.	IPRAN Backhaul Received Util Overloaded Trap

Table 42-3 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 froto any of the status : 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 froto any of the status : 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 froto any of the status : 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 42-3 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 42-3 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	1.3.6.1.4.1.9.1.0.98	N/A	N/A	TE FRR trigger notification v1	FRR Protected Trap
cmplsFrrUnProtected	6	2	1.3.6.1.4.1.9.1.0.98	N/A	N/A	TE FRR trigger notification v1	FRR Unprotected Trap

Table 42-3 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	1.3.6.1.4.1.9.1.0.106.2	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	1.3.6.1.4.1.9.1.0.106.2	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 42-3 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 42-3 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 42-3 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 managementDomainVersionInUse). 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 managementDomainLocalMode 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 managementDomainVersionInUse is changed.	vtp VersionInUse Changed trap

Table 42-3 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 42-3 Cisco IOS V1 Traps (continued)

Trap Name	Generic Type	Specific Type	Enterprise OID	Subtype Varbind OID	Subtype Varbind Value	Description	Short Description
cEtherCfmCcCross connect	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
cEtherCfmCcMep Down	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
cEtherCfmCcMep Down	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
cEtherCfmCcMep Down	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
cEtherCfmXCheck Missing	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
cEtherCfmXCheck Unknown	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
cEtherCfmCcMep Down	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
cEtherCfmXCheck ServiceUp	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	1.3.6.1.4.1.9.1.0.136	1.3.6.1.4.1.9.1.0.136.1.6.1.4	256	Local or remote non-threshold crossing event is detected.	OAM Non-threshold crossing link fault trap

Table 42-3 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	1.3.6.1.4.1.9.1.0.136	1.3.6.1.4.1.9.1.0.136.1.6.1.4	257	Local or remote non-threshold crossing event is detected.	OAM Non-threshold crossing dying gasp trap
cdot3OamNonThresholdEvent	6	2	1.3.6.1.4.1.9.1.0.136	1.3.6.1.4.1.9.1.0.136.1.6.1.4	258	Local or remote non-threshold crossing event is detected.	OAM Non-threshold crossing critical Link trap
cdot3OamThresholdEvent	6	1	1.3.6.1.4.1.9.1.0.136	1.3.6.1.4.1.9.1.0.136.1.6.1.4	1	Local or remote threshold crossing event is detected.	OAM threshold errored Symbol trap
cdot3OamThresholdEvent	6	1	1.3.6.1.4.1.9.1.0.136	1.3.6.1.4.1.9.1.0.136.1.6.1.4	2	Local or remote threshold crossing event is detected.	OAM threshold errored Frame Period trap
cdot3OamThresholdEvent	6	1	1.3.6.1.4.1.9.1.0.136	1.3.6.1.4.1.9.1.0.136.1.6.1.4	3	Local or remote threshold crossing event is detected.	OAM threshold errored Frame trap
cdot3OamThresholdEvent	6	1	1.3.6.1.4.1.9.1.0.136	1.3.6.1.4.1.9.1.0.136.1.6.1.4	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 42-3 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 42-3 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 bgpPeerRemoteAddress, bgpPeerAddressFamilyAfi and cbgpPeerAddressFamilySafi values are attached to the notification object ID.	Cisco BGP prefix threshold clear
ciscoConfigManagementEvent	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 42-3 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 cefcFRUInserted 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 42-3 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 cefcFRUPowerStatus Change 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 cefcFRUPowerStatus Change 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 entSensorThresholdTable. 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 42-3 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 42-3 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 deprecates 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 deprecates ciscoFlashDeviceRemovedNotif since it uses ciscoFlashDeviceName as a varbind which is deprecated.	Cisco Flash device removed

Table 42-3 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 42-3 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	1.3.6.1.4.1.9.1.0.119	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 42-3 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 'mplsLdpEntityPVLimitMismatchTrapEnable' 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 except 'nonexistent(1)' to 'operational'.	MPLS LDP session up Trap

Table 42-3 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 mplsTunnelOperStat us 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 mplsTunnelOperStat us.	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 mplsTunnelOperStat us 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 mplsTunnelOperStat us.	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 42-3 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	1.3.6.1.4.1.9.1.0.2.3.1	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 42-3 Cisco IOS V1 Traps (continued)

Trap Name	Generic Type	Specific Type	Enterprise OID	Subtype Varbind OID	Subtype Varbind Value	Description	Short Description
cEtherCfmCcMep Up	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 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
cEtherCfmCcMep Down	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 42-3 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 42-3 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 42-3 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 42-3 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 42-3 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 42-3 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 42-3 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 42-3 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
stpInconsistencyUpdate	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 stpPortInconsistencyUpdate notification is sent by a bridge when an instance of stpInconsistentState 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 stpInconsistentState value indicates the type of inconsistency which now exists/no longer exists for the relevant VLAN on the relevant port.	stp port inconsistency discovered

Table 42-3 Cisco IOS V1 Traps (continued)

Trap Name	Generic Type	Specific Type	Enterprise OID	Subtype Varbind OID	Subtype Varbind Value	Description	Short Description
stpInconsistencyUpdate	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 stpPortInconsistencyUpdate notification is sent by a bridge when an instance of stpInconsistentState 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 stpInconsistentState value indicates the type of inconsistency which now exists/no longer exists for the relevant VLAN on the relevant port.	stp port inconsistency resolved

Table 42-3 Cisco IOS V1 Traps (continued)

Trap Name	Generic Type	Specific Type	Enterprise OID	Subtype Varbind OID	Subtype Varbind Value	Description	Short Description
stpLoopInconsistencyUpdate	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 stpLoopInconsistencyUpdate notification is sent by a bridge when an instance of stpLoopInconsistencyState is created or destroyed. That is, when a 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 stpLoopInconsistencyState in the notification is true(1); for deletion, the value is false(2). The object value of stpSpanningTreeType indicates which Spanning Tree protocol is running when an instance of stpLoopInconsistencyState is created or destroyed.	stp loop inconsistency discovered

Table 42-3 Cisco IOS V1 Traps (continued)

Trap Name	Generic Type	Specific Type	Enterprise OID	Subtype Varbind OID	Subtype Varbind Value	Description	Short Description
stpLoopInconsistencyUpdate	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 stpLoopInconsistencyUpdate notification is sent by a bridge when an instance of stpLoopInconsistencyState 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 stpLoopInconsistencyState in the notification is true(1); for deletion, the value is false(2). The object value of stpSpanningTreeType indicates which Spanning Tree protocol is running when an instance of stpLoopInconsistencyState is created or destroyed.	stp loop inconsistency resolved

Table 42-3 Cisco IOS V1 Traps (continued)

Trap Name	Generic Type	Specific Type	Enterprise OID	Subtype Varbind OID	Subtype Varbind Value	Description	Short Description
stpRootInconsistencyUpdate	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 stpRootInconsistencyUpdate notification is sent by bridge when an instance of stpRootInconsistencyState is created or destroyed. That is, when a root-inconsistency is discovered in the VLAN's or instance's Spanning Tree for a particular port, or when such a root-inconsistency disappears. For creation, the value of stpRootInconsistencyState in the notification is true(1); for deletion, the value is false(2). The object value of stpSpanningTreeType indicates which Spanning Tree protocol is running when an instance of stpRootInconsistencyState is created or destroyed.	stp root inconsistency discovered

Table 42-3 Cisco IOS V1 Traps (continued)

Trap Name	Generic Type	Specific Type	Enterprise OID	Subtype Varbind OID	Subtype Varbind Value	Description	Short Description
stpRootInconsistencyUpdate	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 stpRootInconsistencyUpdate notification is sent by a bridge when an instance of stpRootInconsistencyState 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 stpRootInconsistencyState in the notification is true(1); for deletion, the value is false(2). The object value of stpSpanningTreeType indicates which Spanning Tree protocol is running when an instance of stpRootInconsistencyState is created or destroyed.	stp root inconsistency resolved

Table 42-3 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 42-3 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 42-3 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 42-3 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 42-3 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 cmnHistTrapContent 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 42-3 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 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	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 managementDomainLocalMode 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 42-3 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 42-3 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 (clcVlanMacLimit) 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 42-3 Cisco IOS V1 Traps (continued)

Trap Name	Generic Type	Specific Type	Enterprise OID	Subtype Varbind OID	Subtype Varbind Value	Description	Short Description
clcIfMacLimitHighNotif	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
clcIfVlanMacLimitLowNotif	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 (clcIfVlanMacLimitLow) either rising above or falling below it.	cisco L2 Control IfVlanMacLimit Low Notif Trap
clcIfVlanMacLimitHighNotif	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 (clcIfVlanMacLimitHigh) either rising above or falling below it.	cisco L2 Control IfVlanMacLimit High Notif Trap

Table 42-3 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 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

Table 42-3 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 42-3 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://lbg.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 42-3 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 42-3 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 42-3 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 42-3 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 42-4 lists the Cisco IOS SNMP V2/V3 traps supported in Cisco ANA. For associated event types, event subtypes, and Cisco ANA registry parameters, use the link under Short Description or see Table 42-16.

Table 42-4 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	!= (1 or 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 cbgpPrfexixMaxThresholdExceeded 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 42-4 Cisco IOS V2/V3 Traps (continued)

Trap Name	Trap OID	Subtype Varbind OID	Subtype Varbind Value	Description	Short Description
ccCopyCompletion	1.3.6.1.4.1.9.9.6.2.1.1	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	1.3.6.1.4.1.9.9.4.3.2.0.1	N/A	N/A	Notification of a configuration management event as recorded in ccmHistoryEventTable.	Cisco Configuration management event notification
cefcFanTrayStatusChange	1.3.6.1.4.1.9.9.17.2.0.6	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	1.3.6.1.4.1.9.9.17.2.0.6	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	1.3.6.1.4.1.9.9.17.2.0.3	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	1.3.6.1.4.1.9.9.17.2.0.4	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	1.3.6.1.4.1.9.9.17.2.0.1	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	1.3.6.1.4.1.9.9.17.2.0.1	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	1.3.6.1.4.1.9.9.17.2.0.2	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

Table 42-4 Cisco IOS V2/V3 Traps (continued)

Trap Name	Trap OID	Subtype Varbind OID	Subtype Varbind Value	Description	Short Description
cefcPowerStatusChange	1.3.6.1.4.1.9.9.1 17.2.0.2	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	1.3.6.1.4.1.9.9.9 1.2.0.1	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
ciscoFlashCopyCompletionTrap	1.3.6.1.4.1.9.9.1 0.1.3.0.1	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	1.3.6.1.4.1.9.9.1 0.1.3.0.1	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	1.3.6.1.4.1.9.9.1 0.1.3.0.1	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
ciscoFlashDeviceChangeTrap	1.3.6.1.4.1.9.9.1 0.1.3.0.4	N/A	N/A	A ciscoFlashDeviceChangeTrap is sent whenever a removable Flash device is inserted or removed.	Cisco Flash device changed
ciscoFlashDeviceInsertedNotification	1.3.6.1.4.1.9.9.1 0.1.3.0.5	N/A	N/A	A ciscoFlashDeviceInsertedNotification is sent whenever a removable Flash device is inserted.	Cisco Flash device inserted
ciscoFlashDeviceRemovedNotification	1.3.6.1.4.1.9.9.1 0.1.3.0.6	N/A	N/A	A ciscoFlashDeviceRemovedNotification is sent whenever a removable Flash device is removed.	Cisco Flash device removed
ciscoFlashDeviceInsertedNotificationRev1	1.3.6.1.4.1.9.9.1 0.1.3.0.7	N/A	N/A	A ciscoFlashDeviceInsertedNotificationRev1 notification is sent whenever a removable Flash device is inserted. The ciscoFlashDeviceInsertedNotificationRev1 deprecates ciscoFlashDeviceInsertedNotification since it uses ciscoFlashDeviceName as a varbind which is deprecated.	Cisco Flash device inserted

Table 42-4 Cisco IOS V2/V3 Traps (continued)

Trap Name	Trap OID	Subtype Varbind OID	Subtype Varbind Value	Description	Short Description
ciscoFlashDeviceRemovedNotifRev1	1.3.6.1.4.1.9.9.1.0.1.3.0.8	N/A	N/A	A ciscoFlashDeviceRemovedNotifRev1 notification is sent whenever a removable Flash device is removed. The ciscoFlashDeviceRemovedNotifRev1 deprecates ciscoFlashDeviceRemovedNotif since it uses ciscoFlashDeviceName as a varbind which is deprecated.	Cisco Flash device removed
ciscoFlashMiscOpCompletionTrap	1.3.6.1.4.1.9.9.1.0.1.3.0.3	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	1.3.6.1.4.1.9.9.1.0.1.3.0.3	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	1.3.6.1.4.1.9.9.1.0.1.3.0.3	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
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	1.3.6.1.4.1.9.9.1.6.2.0.1	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	1.3.6.1.4.1.9.9.1.26.0.1	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

Table 42-4 Cisco IOS V2/V3 Traps (continued)

Trap Name	Trap OID	Subtype Varbind OID	Subtype Varbind Value	Description	Short Description
ciscoSonetSectionStatusChange	1.3.6.1.4.1.9.9.1 26.0.1	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	1.3.6.1.4.1.9.9.1 26.0.2	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	1.3.6.1.4.1.9.9.1 26.0.2	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	1.3.6.1.4.1.9.9.1 26.0.3	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	1.3.6.1.4.1.9.9.1 26.0.3	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
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 except '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

Table 42-4 Cisco IOS V2/V3 Traps (continued)

Trap Name	Trap OID	Subtype Varbind OID	Subtype Varbind Value	Description	Short Description
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
ciscoIpMRoutMissingHeartBeats	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
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

Table 42-4 Cisco IOS V2/V3 Traps (continued)

Trap Name	Trap OID	Subtype Varbind OID	Subtype Varbind Value	Description	Short Description
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
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	1.3.6.1.4.1.9.9.106.2.1.1.15	= 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	1.3.6.1.4.1.9.9.106.2.1.1.15	= 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	1.3.6.1.4.1.9.9.106.2.1.1.15	= 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 42-4 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	= 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
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

Table 42-4 Cisco IOS V2/V3 Traps (continued)

Trap Name	Trap OID	Subtype Varbind OID	Subtype Varbind Value	Description	Short Description
ciscoEnvMonRedundantSupplyNotification	1.3.6.1.4.1.9.9.1.3.3.0.5	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	1.3.6.1.4.1.9.9.1.3.3.0.5	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
ciscoEnvMonRedundantSupplyNotification	1.3.6.1.4.1.9.9.1.3.3.0.5	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	1.3.6.1.4.1.9.9.1.3.3.0.5	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 sent than does the ciscoEnvMonShutdownNotification.	Redundant Supply State - Not Present
ciscoEnvMonRedundantSupplyNotification	1.3.6.1.4.1.9.9.1.3.3.0.5	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

Table 42-4 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	= 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
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	= 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
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	= 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
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	= 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

Table 42-4 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	= 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
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
stpInconsistencyUpdate	1.3.6.1.4.1.9.9.82.2.2.0.1	1.3.6.1.4.1.9.9.82.1.1.3	=1	A stpPortInconsistencyUpdate notification is sent by a bridge when an instance of stpInconsistentState 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 stpInconsistentState value indicates the type of inconsistency which now exists/no longer exists for the relevant VLAN on the relevant port.	stp port inconsistency discovered

Table 42-4 Cisco IOS V2/V3 Traps (continued)

Trap Name	Trap OID	Subtype Varbind OID	Subtype Varbind Value	Description	Short Description
stpInconsistencyUpdate	1.3.6.1.4.1.9.9.82.1.3.1.1.4	1.3.6.1.4.1.9.9.82.1.3.1.1.4	=2	A stpPortInconsistencyUpdate notification is sent by a bridge when an instance of stpInconsistentState 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 stpInconsistentState value indicates the type of inconsistency which now exists/no longer exists for the relevant VLAN on the relevant port.	stp port inconsistency resolved
stpLoopInconsistencyUpdate	1.3.6.1.4.1.9.9.82.1.3.2.1.3	1.3.6.1.4.1.9.9.82.1.3.2.1.3	= 1	A stpLoopInconsistencyUpdate notification is sent by a bridge when an instance of stpLoopInconsistencyState is created or destroyed. That is, when a 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 stpLoopInconsistencyState in the notification is true(1); for deletion, the value is false(2). The object value of stpSpanningTreeType indicates which Spanning Tree protocol is running when an instance of stpLoopInconsistencyState is created or destroyed.	stp loop inconsistency discovered
stpLoopInconsistencyUpdate	1.3.6.1.4.1.9.9.82.1.3.2.1.3	1.3.6.1.4.1.9.9.82.1.3.2.1.3	= 2	A stpLoopInconsistencyUpdate notification is sent by a bridge when an instance of stpLoopInconsistencyState is created or destroyed. That is, when a 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 stpLoopInconsistencyState in the notification is true(1); for deletion, the value is false(2). The object value of stpSpanningTreeType indicates which Spanning Tree protocol is running when an instance of stpLoopInconsistencyState is created or destroyed.	stp loop inconsistency resolved

Table 42-4 Cisco IOS V2/V3 Traps (continued)

Trap Name	Trap OID	Subtype Varbind OID	Subtype Varbind Value	Description	Short Description
stpRootInconsistencyUpdate	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 stpRootInconsistencyUpdate notification is sent by a bridge when an instance of stpRootInconsistencyState 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 stpRootInconsistencyState in the notification is true(1); for deletion, the value is false(2). The object value of stpSpanningTreeType indicates which Spanning Tree protocol is running when an instance of stpRootInconsistencyState is created or destroyed.	stp root inconsistency discovered
stpRootInconsistencyUpdate	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 stpRootInconsistencyUpdate notification is sent by a bridge when an instance of stpRootInconsistencyState 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 stpRootInconsistencyState in the notification is true(1); for deletion, the value is false(2). The object value of stpSpanningTreeType indicates which Spanning Tree protocol is running when an instance of stpRootInconsistencyState is created or destroyed.	stp 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

Table 42-4 Cisco IOS V2/V3 Traps (continued)

Trap Name	Trap OID	Subtype Varbind OID	Subtype Varbind Value	Description	Short Description
vtpConfigDigestError	1.3.6.1.4.1.9.9.4.6.2.0.2	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
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	1.3.6.1.4.1.9.9.6.1.2.0.1	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	1.3.6.1.4.1.9.9.6.1.2.0.2	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

Table 42-4 Cisco IOS V2/V3 Traps (continued)

Trap Name	Trap OID	Subtype Varbind OID	Subtype Varbind Value	Description	Short Description
cmnMacChangedNotification	1.3.6.1.4.1.9.9.2 15.2.0.1	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	1.3.6.1.4.1.9.9.2 15.2.0.2	N/A	N/A	cmnMacMoveNotification is generated when a MAC address is moved between two interfaces.	cmn Mac Move Notification Trap
vtpVersionOneDeviceDetected	1.3.6.1.4.1.9.9.4 6.2.0.6	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	1.3.6.1.4.1.9.9.4 6.2.0.8	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	1.3.6.1.4.1.9.9.4 6.2.0.9	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	1.3.6.1.4.1.9.9.4 6.2.0.7	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	1.3.6.1.4.1.9.9.4 6.2.0.7	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

Table 42-4 Cisco IOS V2/V3 Traps (continued)

Trap Name	Trap OID	Subtype Varbind OID	Subtype Varbind Value	Description	Short Description
cpsSecureMacAddrViolation	1.3.6.1.4.1.9.9.3 15.0.0.1	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	1.3.6.1.4.1.9.9.3 15.0.0.3	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	1.3.6.1.4.1.9.9.3 13.0.1	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 (clcVlanMacMaxMacLimit) either rising above or falling below it.	cisco L2 Control VlanMacLimit Notif Trap
clcVlanMacLimitHighNotif	1.3.6.1.4.1.9.9.3 13.0.2	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	1.3.6.1.4.1.9.9.3 13.0.3	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	1.3.6.1.4.1.9.9.3 13.0.4	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	1.3.6.1.4.1.9.9.3 13.0.5	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

Table 42-4 Cisco IOS V2/V3 Traps (continued)

Trap Name	Trap OID	Subtype Varbind OID	Subtype Varbind Value	Description	Short Description
clcIfVlanMacLimitHighNotification	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
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

Table 42-4 Cisco IOS V2/V3 Traps (continued)

Trap Name	Trap OID	Subtype Varbind OID	Subtype Varbind Value	Description	Short Description
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/t/d/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
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

Table 42-4 Cisco IOS V2/V3 Traps (continued)

Trap Name	Trap OID	Subtype Varbind OID	Subtype Varbind Value	Description	Short Description
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
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

Table 42-4 Cisco IOS V2/V3 Traps (continued)

Trap Name	Trap OID	Subtype Varbind OID	Subtype Varbind Value	Description	Short Description
csbH248Cont rollerStatus	1.3.6.1.4.1.9.9.6 58.0.9	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
rttMonConne ctionChange Notification	1.3.6.1.4.1.9.9.4 2.2.0.1	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
rttMonTimeo utNotification	1.3.6.1.4.1.9.9.4 2.2.0.2	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
rttMonThresh oldNotificatio n	1.3.6.1.4.1.9.9.4 2.2.0.3	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
rttMonVerify ErrorNotificat ion	1.3.6.1.4.1.9.9.4 2.2.0.4	N/A	N/A	A rttMonVerifyErrorNotification indicates the occurrence of a data corruption in an RTT operation.	RTT Verify Error
rttMonNotific ation	1.3.6.1.4.1.9.9.4 2.2.0.5	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

Table 42-4 Cisco IOS V2/V3 Traps (continued)

Trap Name	Trap OID	Subtype Varbind OID	Subtype Varbind Value	Description	Short Description
rttMonLpdDiscoveryNotification	1.3.6.1.4.1.9.9.4.2.2.0.6	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	1.3.6.1.4.1.9.9.4.2.2.0.7	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
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

Table 42-4 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	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 froto any of the status : acceptable, warning, overloaded.	IPRAN Backhaul Received Util Acceptable 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	2	When Rcvd. util changes froto any of the status : 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 froto any of the status : 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 froto any of the status : 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 froto any of the status : 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 froto any of the status : acceptable, warning, overloaded.	IPRAN Backhaul Sent Util Warning Trap
rttMonConnectionChange Notification	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

Table 42-4 Cisco IOS V2/V3 Traps (continued)

Trap Name	Trap OID	Subtype Varbind OID	Subtype Varbind Value	Description	Short Description
rttMonConnectionChangeNotification	1.3.6.1.4.1.9.9.4.2.2.0.1	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	1.3.6.1.4.1.9.9.4.2.2.0.2	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	1.3.6.1.4.1.9.9.4.2.2.0.2	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	1.3.6.1.4.1.9.9.4.2.2.0.3	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	1.3.6.1.4.1.9.9.4.2.2.0.3	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	1.3.6.1.4.1.9.9.4.2.2.0.4	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	1.3.6.1.4.1.9.9.4.2.2.0.4	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	1.3.6.1.4.1.9.9.4.2.2.0.5	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	1.3.6.1.4.1.9.9.4.2.2.0.5	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

Table 42-4 Cisco IOS V2/V3 Traps (continued)

Trap Name	Trap OID	Subtype Varbind OID	Subtype Varbind Value	Description	Short Description
rttMonNotification	1.3.6.1.4.1.9.9.4.2.2.0.5	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	1.3.6.1.4.1.9.9.4.2.2.0.5	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
rttMonNotification	1.3.6.1.4.1.9.9.4.2.2.0.5	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	1.3.6.1.4.1.9.9.4.2.2.0.5	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

Table 42-4 Cisco IOS V2/V3 Traps (continued)

Trap Name	Trap OID	Subtype Varbind OID	Subtype Varbind Value	Description	Short Description
rttMonNotification	1.3.6.1.4.1.9.9.4.2.2.0.5	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	1.3.6.1.4.1.9.9.4.2.2.0.5	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	1.3.6.1.4.1.9.9.4.2.2.0.5	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
rttMonNotification	1.3.6.1.4.1.9.9.4.2.2.0.5	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	1.3.6.1.4.1.9.9.4.2.2.0.6	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	1.3.6.1.4.1.9.9.4.2.2.0.6	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
rttMonLpdGroupStatusNotification	1.3.6.1.4.1.9.9.4.2.2.0.7	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
rttMonLpdGroupStatusNotification	1.3.6.1.4.1.9.9.4.2.2.0.7	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

Table 42-4 Cisco IOS V2/V3 Traps (continued)

Trap Name	Trap OID	Subtype Varbind OID	Subtype Varbind Value	Description	Short Description
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
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 clear 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
cEtherCfmCcMepUp	1.3.6.1.4.1.9.9.461.0.0.1			mep up	CFM cc mep up trap
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	5	timeout	CFM cc mep down due to timeout trap
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	4	lastgasp	CFM cc mep down due to last gasp trap

Table 42-4 Cisco IOS V2/V3 Traps (continued)

Trap Name	Trap OID	Subtype Varbind OID	Subtype Varbind Value	Description	Short Description
cEtherCfmCc Crossconnect	.1.3.6.1.4.1.9.9.4 61.0.0.3	N/A	N/A	cross-connected service error trap	CFM cc cross-connected service error trap
cEtherCfmCc MepDown	.1.3.6.1.4.1.9.9.4 61.0.0.2	.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	.1.3.6.1.4.1.9.9.4 61.0.0.4	N/A	N/A	loop trap	CFM cc loop trap
cEtherCfmCc MepDown	.1.3.6.1.4.1.9.9.4 61.0.0.2	.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	.1.3.6.1.4.1.9.9.4 61.0.0.5	N/A	N/A	config error trap	CFM cc config error trap
cEtherCfmCc MepDown	.1.3.6.1.4.1.9.9.4 61.0.0.2	.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	.1.3.6.1.4.1.9.9.4 61.0.0.6	N/A	N/A	mep missing trap	CFMcrossconnect mep missing trap
cEtherCfmXC heckUnknow n	.1.3.6.1.4.1.9.9.4 61.0.0.7	N/A	N/A	mep unknown trap	CFMcrossconnect mep unknown trap
cEtherCfmCc MepDown	.1.3.6.1.4.1.9.9.4 61.0.0.2	.1.3.6.1.4. 1.9.9.461. 1.1.2.1.16	9	mep unknown trap clear	CFMcrossconnect mep unknown trap clear
cEtherCfmXC heckServiceU p	.1.3.6.1.4.1.9.9.4 61.0.0.8	N/A	N/A	mep service up trap	CFMcrossconnect mep service up trap
vrrpTrapAuth Failure	1.3.6.1.2.1.68.0. 2			vrrp trap auth failure trap	Vrrp trap auth failure trap
vrrpTrapNew Master	1.3.6.1.2.1.68.0. 1			vrrp trap new master trap	Vrrp trap new master trap
cdot3OamNo nThresholdEv ent	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
cdot3OamNo nThresholdEv ent	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

Table 42-4 Cisco IOS V2/V3 Traps (continued)

Trap Name	Trap OID	Subtype Varbind OID	Subtype Varbind Value	Description	Short Description
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
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 42-5 lists the Cisco IOX SNMP V1 traps supported in Cisco ANA. For associated event types, event subtypes, and Cisco ANA registry parameters, use the link under Short Description or see Table 42-17.

Table 42-5 Cisco IOX V1 Traps

Trap Name	Generic Type	Specific Type	Enterprise OID	Subtype Varbind OID	Subtype Varbind Value	Description	Short Description
cpwVcUp	6	2	1.3.6.1.4.1.9.10.10.6.2	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	1.3.6.1.4.1.9.10.10.6.2	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
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

Table 42-5 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 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
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 42-5 Cisco IOX 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

Table 42-5 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	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
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

Table 42-5 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, 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	1.3.6.1.2.1.10.18.1.5	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	1.3.6.1.2.1.10.18.1.5	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	1.3.6.1.2.1.10.18.1.5	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	1.3.6.1.2.1.10.18.1.5	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	1.3.6.1.2.1.10.18.1.5	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 42-5 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	1.3.6.1.2.1.10.18.1.5	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	1.3.6.1.2.1.10.18.1.5	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	1.3.6.1.2.1.10.18.1.5	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	1.3.6.1.2.1.10.18.1.5	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	1.3.6.1.2.1.10.18.1.5	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	1.3.6.1.2.1.10.18.1.5	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	1.3.6.1.2.1.10.18.1.5	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	1.3.6.1.2.1.10.18.1.5	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	1.3.6.1.2.1.10.18.1.5	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	1.3.6.1.2.1.10.18.1.5	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	1.3.6.1.2.1.10.18.1.5	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 42-5 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	1.3.6.1.2.1.10.18.1.5	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	1.3.6.1.2.1.10.18.1.5	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	1.3.6.1.2.1.10.30.1.5	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	1.3.6.1.2.1.10.30.1.5	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	1.3.6.1.2.1.10.30.1.5	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	1.3.6.1.2.1.10.30.1.5	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	1.3.6.1.2.1.10.30.1.5	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	1.3.6.1.2.1.10.30.1.5	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	1.3.6.1.2.1.10.30.1.5	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 42-5 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	.1.3.6.1.2.1.10.30.1.5	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	.1.3.6.1.2.1.10.30.1.5	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	.1.3.6.1.2.1.10.30.1.5	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	.1.3.6.1.2.1.10.30.1.5	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	.1.3.6.1.2.1.10.30.1.5	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	.1.3.6.1.2.1.10.30.1.5	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 42-5 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
ciscoBfdSessionDown	6	2	1.3.6.1.4.1.9.10.137	N/A	N/A	Cisco-BFD-session-change-trap	Cisco bfd session down trap
ciscoBfdSessionUp	6	1	1.3.6.1.4.1.9.10.137	N/A	N/A	Cisco-BFD-session-change-trap	Cisco bfd session up trap
cbgpBackwardTransition	6	2	1.3.6.1.4.1.9.9.187	1.3.6.1.4.1.9.9.187.0.2	!= (1 or 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

Table 42-5 Cisco IOX V1 Traps (continued)

Trap Name	Generic Type	Specific Type	Enterprise OID	Subtype Varbind OID	Subtype Varbind Value	Description	Short Description
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
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

Table 42-5 Cisco IOX V1 Traps (continued)

Trap Name	Generic Type	Specific Type	Enterprise OID	Subtype Varbind OID	Subtype Varbind Value	Description	Short Description
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	1.3.6.1.4.1.9.10.10.6.2	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	1.3.6.1.4.1.9.10.10.6.2	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
ciscoRFSwactNotification	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

Table 42-5 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 - 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
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

Table 42-5 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 - 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
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

Cisco IOX V2/V3 Traps

Table 42-6 lists the Cisco IOX SNMP V2/V3 traps supported in Cisco ANA. For associated event types, event subtypes, and Cisco ANA registry parameters, use the link under Short Description or see Table 42-18.

Table 42-6 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 cbgpPrfexMaxThresholdExceeded 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 42-6 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	!=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	=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 cefcFRUInserted 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	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	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	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	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 42-6 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 nonzero 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 nonzero 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
ciscoConfigManagementEvent	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 42-6 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	1.3.6.1.2.1.1.0.39.1.2.1.1.1	!=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	1.3.6.1.2.1.1.0.39.1.2.1.1.1	=1	This notification is generated whenever the value of sonetSectionCurrentStatus changes to value 1.	Cisco Sonet section status changed to clear

Table 42-6 Cisco IOX V2/V3 Traps (continued)

Trap Name	Trap OID	Subtype Varbind OID	Subtype Varbind Value	Description	Short Description
ciscoSonetLineStatusChange	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
ciscoSonetLineStatusChange	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
ciscoSonetPathStatusChange	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
ciscoSonetPathStatusChange	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
clogMessageGenerated	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
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 entSensorThreshold Table
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
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 42-6 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
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	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
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	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
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	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
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	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 42-6 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 42-6 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 42-6 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 42-6 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	!= (1 or 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 42-6 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 42-6 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 42-6 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 42-6 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 42-6 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 42-6 *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	1.3.6.1.2.1.1 0.32.2.1.3	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	1.3.6.1.2.1.1 0.32.2.1.3	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
ciscoSonetVTS tatusChange	.1.3.6.1.4.1 .9.9.126.0.4	1.3.6.1.2.1.1 0.39.3.1.1.1. 2	!=1	VT Status is down	Cisco Sonet vt status changed to error
ciscoSonetVTS tatusChange	.1.3.6.1.4.1 .9.9.126.0.4	1.3.6.1.2.1.1 0.39.3.1.1.1. 2	1	VT Status is down	Cisco Sonet vt status changed to clear
vrrpTrapAuthF ailure	1.3.6.1.2.1. 68.0.2	N/A	N/A	vrrp trap auth failure trap	Vrrp trap auth failure trap
vrrpTrapNewM aster	1.3.6.1.2.1. 68.0.1	N/A	N/A	vrrp trap new master trap	Vrrp trap new master trap
ciscoBfdSessD own	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
ciscoBfdSessU p	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

Cisco MIB2 V1 Traps

Table 42-7 lists the Cisco MIB2 SNMP V1 traps supported in Cisco ANA. For associated event types, event subtypes, and Cisco ANA registry parameters, use the link under Short Description or see Table 42-19.

Table 42-7 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 42-7 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 42-7 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 42-7 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 42-7 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-virtual OSPF 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 42-7 Cisco MIB2 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-virtual OSPF 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	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
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

Table 42-7 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 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
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 42-7 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 that 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 that 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 42-7 Cisco MIB2 V1 Traps (continued)

Trap Name	Generic Type	Specific Type	Enterprise OID	Subtype Varbind OID	Subtype Varbind Value	Description	Short Description
ipv6IfStateChange	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
mplsL3VpnNumVrfRouteMaxThresholdCleared	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
mplsL3VpnVrfDown	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
mplsL3VpnVrfNumVrfRouteMaxThresholdExceeded	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
mplsL3VpnVrfRouteMidThresholdExceeded	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 42-7 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 42-7 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 notPresent 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 42-8 lists the Cisco MIB2 SNMP V2/V3 traps supported in Cisco ANA. For associated event types, event subtypes, and Cisco ANA registry parameters, use the link under Short Description or see Table 42-20.

Table 42-8 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	1.3.6.1.2.1.15.3.1.2	= 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 42-8 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 configuration is 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 42-8 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 virtual OSPF 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 virtual OSPF 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 42-8 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 42-8 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 that 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 that 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 42-8 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
mplsL3VpnVrfNumVrfRouteMaxThresholdExceeded	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
mplsL3VpnVrfRouteMidThresholdExceeded	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 42-8 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 notPresent 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 42-8 Cisco MIB2 V2/V3 Traps (continued)

Trap Name	Trap OID	Subtype Varbind OID	Subtype Varbind Value	Description	Short Description
DSX1 V1 Line Status Change	1.3.6.1.2.1.10.18.1.5.0.1	1.3.6.1.2.1.1.0.18.6.1.10.1.7	8	Indicates the line status of dsx1 interface	DSX1 Far end sending AIS
DSX1 V1 Line Status Change	1.3.6.1.2.1.10.18.1.5.0.1	1.3.6.1.2.1.1.0.18.6.1.10.1.7	16	Indicates the line status of dsx1 interface	DSX1 Near end sending AIS
DSX1 V1 Line Status Change	1.3.6.1.2.1.10.18.1.5.0.1	1.3.6.1.2.1.1.0.18.6.1.10.1.7	32	Indicates the line status of dsx1 interface	DSX1 Near end LOF
DSX1 V1 Line Status Change	1.3.6.1.2.1.10.18.1.5.0.1	1.3.6.1.2.1.1.0.18.6.1.10.1.7	64	Indicates the line status of dsx1 interface	DSX1 Near end Loss of Signal
DSX1 V1 Line Status Change	1.3.6.1.2.1.10.18.1.5.0.1	1.3.6.1.2.1.1.0.18.6.1.10.1.7	128	Indicates the line status of dsx1 interface	DSX1 Near end is looped
DSX1 V1 Line Status Change	1.3.6.1.2.1.10.18.1.5.0.1	1.3.6.1.2.1.1.0.18.6.1.10.1.7	256	Indicates the line status of dsx1 interface	DSX1 E1 TS16 AIS
DSX1 V1 Line Status Change	1.3.6.1.2.1.10.18.1.5.0.1	1.3.6.1.2.1.1.0.18.6.1.10.1.7	512	Indicates the line status of dsx1 interface	DSX1 Far End Sending TS16 LOMF
DSX1 V1 Line Status Change	1.3.6.1.2.1.10.18.1.5.0.1	1.3.6.1.2.1.1.0.18.6.1.10.1.7	1024	Indicates the line status of dsx1 interface	DSX1 Near End Sending TS16 LOMF
DSX1 V1 Line Status Change	1.3.6.1.2.1.10.18.1.5.0.1	1.3.6.1.2.1.1.0.18.6.1.10.1.7	2048	Indicates the line status of dsx1 interface	DSX1 Near End detects a test code
DSX1 V1 Line Status Change	1.3.6.1.2.1.10.18.1.5.0.1	1.3.6.1.2.1.1.0.18.6.1.10.1.7	4096	Indicates the line status of dsx1 interface	DSX1 any line status not defined here
DSX1 V1 Line Status Change	1.3.6.1.2.1.10.18.1.5.0.1	1.3.6.1.2.1.1.0.18.6.1.10.1.7	8192	Indicates the line status of dsx1 interface	DSX1 Near End in Unavailable Signal State
DSX1 V1 Line Status Change	1.3.6.1.2.1.10.18.1.5.0.1	1.3.6.1.2.1.1.0.18.6.1.10.1.7	16384	Indicates the line status of dsx1 interface	DSX1 Carrier Equipment Out of Service
DSX1 V1 Line Status Change	1.3.6.1.2.1.10.18.1.5.0.1	1.3.6.1.2.1.1.0.18.6.1.10.1.7	32768	Indicates the line status of dsx1 interface	DSX1 DS2 Payload AIS
DSX1 V1 Line Status Change	1.3.6.1.2.1.10.18.1.5.0.1	1.3.6.1.2.1.1.0.18.6.1.10.1.7	65536	Indicates the line status of dsx1 interface	DSX1 DS2 Performance Threshold Exceeded

Table 42-8 Cisco MIB2 V2/V3 Traps (continued)

Trap Name	Trap OID	Subtype Varbind OID	Subtype Varbind Value	Description	Short Description
DSX1 V1 Line Status Change	1.3.6.1.2.1.10.18.1.5.0.1	1.3.6.1.2.1.1.0.18.6.1.10.1.7	!=(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	1.3.6.1.2.1.10.18.1.5.0.1	1.3.6.1.2.1.1.0.18.6.1.10.1.7	1	Indicates the line status of dsx1 interface	DSX1 No alarm present
DSX3 V1 Line Status Change	1.3.6.1.2.1.10.30.1.5.0.1	1.3.6.1.2.1.1.0.30.5.1.10.1.7	2	Indicates the line status of dsx3 interface	DSX3 Receiving Yellow/Remote Alarm Indication
DSX3 V1 Line Status Change	1.3.6.1.2.1.10.30.1.5.0.1	1.3.6.1.2.1.1.0.30.5.1.10.1.7	4	Indicates the line status of dsx3 interface	DSX3 Transmitting Yellow/Remote Alarm Indication
DSX3 V1 Line Status Change	1.3.6.1.2.1.10.30.1.5.0.1	1.3.6.1.2.1.1.0.30.5.1.10.1.7	8	Indicates the line status of dsx3 interface	DSX3 Receiving AIS failure state
DSX3 V1 Line Status Change	1.3.6.1.2.1.10.30.1.5.0.1	1.3.6.1.2.1.1.0.30.5.1.10.1.7	16	Indicates the line status of dsx3 interface	DSX3 Transmitting AIS
DSX3 V1 Line Status Change	1.3.6.1.2.1.10.30.1.5.0.1	1.3.6.1.2.1.1.0.30.5.1.10.1.7	32	Indicates the line status of dsx3 interface	DSX3 Receiving LOF failure state
DSX3 V1 Line Status Change	1.3.6.1.2.1.10.30.1.5.0.1	1.3.6.1.2.1.1.0.30.5.1.10.1.7	64	Indicates the line status of dsx3 interface	DSX3 Receiving LOS failure state
DSX3 V1 Line Status Change	1.3.6.1.2.1.10.30.1.5.0.1	1.3.6.1.2.1.1.0.30.5.1.10.1.7	128	Indicates the line status of dsx3 interface	DSX3 Looping the received signal
DSX3 V1 Line Status Change	1.3.6.1.2.1.10.30.1.5.0.1	1.3.6.1.2.1.1.0.30.5.1.10.1.7	256	Indicates the line status of dsx3 interface	DSX3 Receiving a Test Pattern
DSX3 V1 Line Status Change	1.3.6.1.2.1.10.30.1.5.0.1	1.3.6.1.2.1.1.0.30.5.1.10.1.7	512	Indicates the line status of dsx3 interface	DSX3 any line status not defined here
DSX3 V1 Line Status Change	1.3.6.1.2.1.10.30.1.5.0.1	1.3.6.1.2.1.1.0.30.5.1.10.1.7	1024	Indicates the line status of dsx3 interface	DSX3 Near End in Unavailable Signal State

Table 42-8 Cisco MIB2 V2/V3 Traps (continued)

Trap Name	Trap OID	Subtype Varbind OID	Subtype Varbind Value	Description	Short Description
DSX3 V1 Line Status Change	1.3.6.1.2.1.10.30.1.5.0.1	1.3.6.1.2.1.1.0.30.5.1.10.1.7	2048	Indicates the line status of dsx3 interface	DSX3 Carrier Equipment Out of Service
DSX3 V1 Line Status Change	1.3.6.1.2.1.10.30.1.5.0.1	1.3.6.1.2.1.1.0.30.5.1.10.1.7	!=(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	1.3.6.1.2.1.10.30.1.5.0.1	1.3.6.1.2.1.1.0.30.5.1.10.1.7	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	1.3.6.1.2.1.1.0.32.2.1.3	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	1.3.6.1.2.1.1.0.32.2.1.3	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	1.3.6.1.2.1.1.0.32.2.1.3	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 42-9 lists the Cisco ACE SNMP V1 traps supported in Cisco ANA. For associated event types, event subtypes, and Cisco ANA registry parameters, use the link under Short Description or Table 42-21.

Table 42-9 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
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 42-10 lists the Cisco ACE SNMP V2/V3 traps supported in Cisco ANA. For associated event types, event subtypes, and Cisco ANA registry parameters, use the link in the Short Description column or see Table 42-22.

Table 42-10 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
ciscoSibVServerVIPStateChange	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
ciscoSibVServerStateChange	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 42-11 lists the Cisco NEXUS SNMP V1 traps supported in Cisco ANA. For associated event types, event subtypes, and Cisco ANA registry parameters, use the link under Short Description or Table 42-23.

Table 42-11 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 42-11 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	1.3.6.1.4.1.9.9.117.1.1.2.1.1.2	!=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	1.3.6.1.4.1.9.9.117.1.1.2.1.1.2	=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 cefcFRUInserted 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 42-11 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 42-11 Cisco Nexus V1 Traps (continued)

Trap Name	Generic Type	Specific Type	Enterprise OID	Subtype Varbind OID	Subtype Varbind Value	Description	Short Description
stpInconsistencyUpdate	6	1	1.3.6.1.4.1.9.9.82.2	1.3.6.1.4.1.9.9.82.1.3	=1	A stpPortInconsistencyUpdate notification is sent by a bridge when an instance of stpInconsistentState 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 stpInconsistentState value indicates the type of inconsistency which now exists/no longer exists for the relevant VLAN on the relevant port.	Stpx Pvid Inconsistency Trap
stpInconsistencyUpdate	6	1	1.3.6.1.4.1.9.9.82.2	1.3.6.1.4.1.9.9.82.1.3	=0	A stpPortInconsistencyUpdate notification is sent by a bridge when an instance of stpInconsistentState 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 stpInconsistentState 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 42-11 Cisco Nexus V1 Traps (continued)

Trap Name	Generic Type	Specific Type	Enterprise OID	Subtype Varbind OID	Subtype Varbind Value	Description	Short Description
stpLoopInconsistencyUpdate	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 stpLoopInconsistencyUpdate notification is sent by a bridge when an instance of stpLoopInconsistencyState 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 stpLoopInconsistencyState in the notification is true(1); for deletion, the value is false(2).The object value of stpSpanningTreeType indicates which Spanning Tree protocol is running when an instance of stpLoopInconsistencyState is created or destroyed.	stp loop inconsistency discovered

Table 42-11 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 indicates which Spanning Tree protocol is running when an instance of stpxLoopInconsistencyState is created or destroyed.	stpx loop inconsistency resolved

Table 42-11 Cisco Nexus V1 Traps (continued)

Trap Name	Generic Type	Specific Type	Enterprise OID	Subtype Varbind OID	Subtype Varbind Value	Description	Short Description
stpRootInconsistencyUpdate	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 stpRootInconsistencyUpdate notification is sent by a bridge when an instance of stpRootInconsistencyState is created or destroyed. That is, when a root-inconsistency is discovered in the VLAN's or instance's Spanning Tree for a particular port, or when such a root-inconsistency disappears. For creation, the value of stpRootInconsistencyState in the notification is true(1); for deletion, the value is false(2).The object value of stpSpanningTreeType indicates which Spanning Tree protocol is running when an instance of stpRootInconsistencyState is created or destroyed.	stp root inconsistency discovered

Table 42-11 Cisco Nexus V1 Traps (continued)

Trap Name	Generic Type	Specific Type	Enterprise OID	Subtype Varbind OID	Subtype Varbind Value	Description	Short Description
stpRootInconsistencyUpdate	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 stpRootInconsistencyUpdate notification is sent by a bridge when an instance of stpRootInconsistencyState 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 stpRootInconsistencyState in the notification is true(1); for deletion, the value is false(2). The object value of stpSpanningTreeType indicates which Spanning Tree protocol is running when an instance of stpRootInconsistencyState is created or destroyed.	stp 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 42-11 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 42-11 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	1.3.6.1.2.1.14.1.6.2	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	1.3.6.1.2.1.14.1.6.2	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
ospfVirtNbrState Change	6	3	1.3.6.1.2.1.14.1.6.2	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
ospfVirtNbrState Change	6	3	1.3.6.1.2.1.14.1.6.2	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 42-11 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	1.3.6.1.2.1.14.1.6.2	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	1.3.6.1.2.1.14.1.6.2	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	1.3.6.1.2.1.14.1.6.2	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	1.3.6.1.2.1.14.1.6.2	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	1.3.6.1.2.1.14.1.6.2	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 42-11 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	1.3.6.1.2.1.14.1.6.2	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	1.3.6.1.2.1.14.1.6.2	N/A	N/A	An ospfTxRetransmit trap signifies that an OSPF packet has been retransmitted on a non-virtual interface.	OSPF packet retransmitted
ospfVirtIfTxRetransmit	6	11	1.3.6.1.2.1.14.1.6.2	N/A	N/A	An ospfTxRetransmit trap signifies that an OSPF packet has been retransmitted on a virtual interface.	OSPF packet retransmitted on virtual interface
ospfOriginateLsa	6	12	1.3.6.1.2.1.14.1.6.2	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	1.3.6.1.2.1.14.1.6.2	N/A	N/A	An ospfMaxAgeLsa trap signifies that one of the LSAs in the router's link-state database has aged to MaxAge.	OSPF LSA aged to MaxAge
ospfLsdbOverflow	6	14	1.3.6.1.2.1.14.1.6.2	N/A	N/A	OSPF lsdb overflow trap	OSPF lsdb overflow trap
ospfLsdbApproachingOverflow	6	15	1.3.6.1.2.1.14.1.6.2	N/A	N/A	OSPF lsdb approaching overflow trap	OSPF lsdb approaching overflow trap

Table 42-11 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	1.3.6.1.2.1.14.1.6.2	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-virtual OSPF 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	1.3.6.1.2.1.14.1.6.2	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-virtual OSPF 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	1.3.6.1.2.1.14.1.6.2	N/A	N/A	OSPF NSSA translator status change trap	OSPF NSSA translator status change trap
ospfRestartStatusChange	6	18	1.3.6.1.2.1.14.1.6.2	N/A	N/A	OSPF restart status change trap	OSPF restart status change trap
ospfNbrRestartHelperStatusChange	6	19	1.3.6.1.2.1.14.1.6.2	N/A	N/A	OSPF neighbor restart helper status change trap	OSPF neighbor restart helper status change trap
ospfVirtNbrRestartHelperStatusChange	6	20	1.3.6.1.2.1.14.1.6.2	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 42-12 lists the Cisco Nexus SNMP V2/V3 traps supported in Cisco ANA. For associated event types, event subtypes, and Cisco ANA registry parameters, use the link in the Short Description column or see Table 42-24.

Table 42-12 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
bgpBackward Transition	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	1.3.6.1.4.1.9.9.17.2.1	1.3.6.1.4.1.9.9.17.1.2.1.1.2	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	1.3.6.1.4.1.9.9.17.2.1	1.3.6.1.4.1.9.9.17.1.2.1.1.2	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	1.3.6.1.4.1.9.9.17.2.2	1.3.6.1.4.1.9.9.17.1.2.1.1.2	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 42-12 Cisco Nexus V2/V3 Traps (continued)

Trap Name	Trap OID	Subtype Varbind OID	Subtype Varbind Value	Description	Short Description
cefcPowerStatusChange	1.3.6.1.4.1.9.9.17.2.2	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	1.3.6.1.4.1.9.9.17.2.3	N/A	N/A	The cefcFRUInserted 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	1.3.6.1.4.1.9.9.17.2.4	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	1.3.6.1.4.1.9.9.12.0.1	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 42-12 Cisco Nexus V2/V3 Traps (continued)

Trap Name	Trap OID	Subtype Varbind OID	Subtype Varbind Value	Description	Short Description
stpInconsistencyUpdate	1.3.6.1.4.1.9.9.82.1.3.2.2.1	1.3.6.1.4.1.9.9.82.1.3.1.1.3	N/A	A stpPortInconsistencyUpdate notification is sent by a bridge when an instance of stpInconsistentState 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 stpInconsistentState value indicates the type of inconsistency which now exists/no longer exists for the relevant VLAN on the relevant port.	Stpx Type Inconsistency Trap
stpLoopInconsistencyUpdate	1.3.6.1.4.1.9.9.82.1.3.2.2.3	1.3.6.1.4.1.9.9.82.1.8.2.1.3	N/A	A stpLoopInconsistencyUpdate notification is sent by a bridge when an instance of stpLoopInconsistencyState is created or destroyed. That is, when a 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 stpLoopInconsistencyState in the notification is true(1); for deletion, the value is false(2). The object value of stpSpanningTreeType indicates which Spanning Tree protocol is running when an instance of stpLoopInconsistencyState is created or destroyed.	stp loop inconsistency discovered
stpLoopInconsistencyUpdate	1.3.6.1.4.1.9.9.82.1.3.2.2.3	1.3.6.1.4.1.9.9.82.1.8.2.1.3	N/A	A stpLoopInconsistencyUpdate notification is sent by a bridge when an instance of stpLoopInconsistencyState is created or destroyed. That is, when a 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 stpLoopInconsistencyState in the notification is true(1); for deletion, the value is false(2). The object value of stpSpanningTreeType indicates which Spanning Tree protocol is running when an instance of stpLoopInconsistencyState is created or destroyed.	stp loop inconsistency resolved

Table 42-12 Cisco Nexus V2/V3 Traps (continued)

Trap Name	Trap OID	Subtype Varbind OID	Subtype Varbind Value	Description	Short Description
stpRootInconsistencyUpdate	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 stpRootInconsistencyUpdate notification is sent by a bridge when an instance of stpRootInconsistencyState 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 stpRootInconsistencyState in the notification is true(1); for deletion, the value is false(2). The object value of stpSpanningTreeType indicates which Spanning Tree protocol is running when an instance of stpRootInconsistencyState is created or destroyed.	stp root inconsistency discovered
stpRootInconsistencyUpdate	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 stpRootInconsistencyUpdate notification is sent by a bridge when an instance of stpRootInconsistencyState 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 stpRootInconsistencyState in the notification is true(1); for deletion, the value is false(2). The object value of stpSpanningTreeType indicates which Spanning Tree protocol is running when an instance of stpRootInconsistencyState is created or destroyed.	stp 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 42-12 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 42-12 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 that 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 that 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 42-12 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-virtual OSPF 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-virtual OSPF 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 ASR 9000 V1 Trap Registry Parameters

Table 42-13 lists the associated event types, event subtypes, and Cisco ANA registry parameters for the ASR 9000 SNMP V1 traps shown in Table 42-1.

Table 42-13 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	ICFMServ	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	ICFMServ	F	F	F	0	F	clr	F	T	F

Cisco ASR 9000 V2/V3 Registry Parameters

Table 42-14 lists the associated event types, event subtypes, and Cisco ANA registry parameters for the Cisco ASR 9000 SNMP V2/V3 traps shown in Table 42-2.

Table 42-14 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
dot1ag CFM Fault Alarm	dot1ag cfm fault alarm trap	dot1ag cfm fault alarm trap	N	ICFMServ ice	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	ICFMServ ice	F	F	F	0	F	clr	F	T	F

Cisco IOS V1 Trap Registry Parameters

Table 42-15 lists the associated event types, event subtypes, and Cisco ANA registry parameters for the Cisco IOS SNMP V1 traps shown in Table 42-3.

Table 42-15 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 Temperature	cisco-Environment-Monitoring-Temperature-Notification	critical	N	IManaged Element	F	F	F	0	T	cri	F	T	F
Normal Temperature	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 Temperature - Device Shutdown	cisco-Environment-Monitoring-Temperature-Notification	shutdown	N	IManaged Element	F	F	F	0	T	cri	F	T	F
Temperature Rising	cisco-Environment-Monitoring-Temperature-Notification	warning	N	IManaged Element	F	F	F	0	T	wrn	F	T	F
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

Table 42-15 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 - 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 42-15 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-mlppbundle-status-telnet/mtop-ima-group-state-telnet/mtop-cem-group-status/bundle-status/mpls traffic engineering tunnel information/basetech-ll dp-neighbors-s nmp/basetech-c dp-neighbors-s nmp/port-status/ip interface oper status	IPhysical Layer	F	T	F	0	T	min		F	T	T

Table 42-15 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-mlppbundle-status-telnet/mtop-ima-group-state-telnet/mtop-cem-group-status/bundle-status/mps traffic engineering tunnel information/basetech-ll dp-neighbors-s nmp/basetech-c dp-neighbors-s nmp/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 42-15 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	ImaGroupOid	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	ImaGroupOid	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	ImaGroupOid	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	ImaGroupOid	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	ImaGroupOid	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	ImaGroupOid	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	ImaGroupOid	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	ImaGroupOid	F	F	F	0	F	CLEARED	F	T	T

Table 42-15 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 Warning Trap	N/A	PortLayer1Oid	F	F	F	0	T	maj	F	T	F

Table 42-15 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	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	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 42-15 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	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	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	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	Managed Element	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	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 42-15 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	maj	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	maj	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 42-15 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	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

Table 42-15 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 clear	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 clear	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 clear	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 clear	mep unknown trap clear	N/A	ICfmServiceOid	F	F	F	0	F	clr	F	T	F

Table 42-15 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	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
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

Table 42-15 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 42-15 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
cefcmodule oper status down	cefc module oper status changed	cefc module oper down	physical -command	IModule	F	T	T	0	T	maj	F	T	T
cefcmodule 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	IManaged Element	F	F	F	0	F	maj	T	T	T
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
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 device inserted	cisco flash device removed	cisco flash device inserted	N	IManaged Element	F	F	F	0	F	clr	F	T	T

Table 42-15 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 42-15 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 42-15 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 42-15 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	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
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 42-15 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 42-15 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 42-15 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
stp loop inconsistency resolved	stp loop inconsistency update	stp loop inconsistency resolved	N	IStpService	F	F	F	0	F	clr	T	T	F
stp root inconsistency discovered	stp root inconsistency update	stp root inconsistency discovered	N	IStpService	F	T	F	0	F	maj	T	T	F
stp root inconsistency resolved	stp root inconsistency update	stp 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	IManaged Element	F	F	F	0	F	info	F	T	F
caem Temperature Notification Trap	caem-MIB-Notifications-Trap	caem Temperature Notification	N	IManaged Element	F	F	F	0	F	min	F	T	F
caem Voltage Notification Trap	caem-MIB-Notifications-Trap	caem Voltage Notification	N	IManaged Element	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	IManaged Element	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	IManaged Element + identifier index	F	F	F	0	F	min	F	T	F

Table 42-15 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	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
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

Table 42-15 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 42-15 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 42-15 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 42-16 lists the associated event types, event subtypes, and Cisco ANA registry parameters for the Cisco IOS SNMP V2/V3 traps shown in Table 42-4.

Table 42-16 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

Table 42-16 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 down	cefc module oper status changed	cefc module oper down	physical-c ommand	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-c ommand	IModule	F	F	F	0	F	clr	F	T	T
cefc power status down	cefc power status changed	cefc power status down	physical-c ommand	IModule	F	T	T	0	T	maj	F	T	T
cefc power status up	cefc power status changed	cefc power status up	physical-c ommand	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

Table 42-16 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 failed	cisco flash operation completed	cisco flash operation failed	N	IManagedElement	F	F	F	0	F	info	F	T	F
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

Table 42-16 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 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
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-com mand	IShelf	F	F	F	110000	F	info	T	T	F

Table 42-16 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 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-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

Table 42-16 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 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
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

Table 42-16 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 - Shutdown	cisco-Environment-Monitoring-Fan-Notification	shutdown	N	IManagedElement + identifier index	F	F	F	0	F	cri	T	T	F
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

Table 42-16 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
Critical Temperature	cisco-Environment-Monitoring-Temperature-Notification	critical	N	IManagedElement + identifier index	F	F	F	0	F	cri	T	T	F
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

Table 42-16 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 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	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-Notification-Trap	caem Temperature Notification	N	IManagedElement	F	F	F	0	F	min	F	T	F
caem Voltage Notification Trap	caem-MIB-Notification-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	min	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

Table 42-16 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
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	IPortLayer 1	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	IPortLayer 1	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	IPortLayer 1	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	IPortLayer 1	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	IPortLayer 1	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	IPortLayer 1	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	IPortLayer 1	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	IPortLayer 1	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	IPortLayer 1	F	F	F	0	F	info	F	T	F

Table 42-16 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 L2 Control IfVlanMacLimit High Notif Trap	cisco-L2-Control-IfVlanMacLimit-Notifs-Trip	clc IfVlanMacLimit High Notif	N	IPortLayer 1	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
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

Table 42-16 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 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
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

Table 42-16 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 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
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	ImaGroupOid	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	ImaGroupOid	F	F	F	0	T	maj	F	T	T

Table 42-16 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 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
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

Table 42-16 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 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 Warning Trap	N/A	PortLayer1Oid	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

Table 42-16 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 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	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

Table 42-16 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
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	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

Table 42-16 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
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-snmpp, 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-snmpp, 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	IREPServic	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	IREPServic	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	IREPServic	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	IREPServic	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

Table 42-16 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 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
CFM cc cross-connected service error trap clear	cisco cfm cc cross-connected service error trap clear	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 clear	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 clear	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 clear	mep unknown trap clear	N/A	ICfmServiceOid	F	F	F	0	F	clr	F	T	F

Table 42-16 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 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
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

Table 42-16 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 - 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
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 42-17 lists the associated event types, event subtypes, and Cisco ANA registry parameters for the Cisco IOX SNMP V1 traps shown in Table 42-5.

Table 42-17 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	IPPhysicalLayer	F	T	F	0	T	min	F	T	T
SNMP Link up	snmp link down	snmp link up	Y	IPPhysicalLayer	F	T	F	0	F	clr	F	T	T
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

Table 42-17 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
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
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

Table 42-17 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 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
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

Table 42-17 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 down	pseudo wire tunnel traps	Pseudo wire tunnel down	ce-pw-tunnels-status-trap	IP/MPLS Tunnel	F	T	F	0	T	min	F	T	T
DSX1 Far end LOF	dsx1 line status change	RcvFarEndLOF	Y	IPPhysicalLayer	F	T	F	0	T	maj	F	T	F
DSX1 Near end sending LOF Indication	dsx1 line status change	XmtFarEndLOF	Y	IPPhysicalLayer	F	T	F	0	T	maj	F	T	F
DSX1 Far end sending AIS	dsx1 line status change	RcvAIS	Y	IPPhysicalLayer	F	T	F	0	T	wrn	F	T	F
DSX1 Near end sending AIS	dsx1 line status change	XmtAIS	Y	IPPhysicalLayer	F	T	F	0	T	wrn	F	T	F
DSX1 Near end LOF	dsx1 line status change	LossOfFrame	Y	IPPhysicalLayer	F	T	F	0	T	maj	F	T	F
DSX1 Near end Loss of Signal	dsx1 line status change	LossOfSignal	Y	IPPhysicalLayer	F	T	F	0	T	maj	F	T	F
DSX1 Near end is looped	dsx1 line status change	LoopbackState	Y	IPPhysicalLayer	F	T	F	0	T	maj	F	T	F
DSX1 E1 TS16 AIS	dsx1 line status change	T16AIS	Y	IPPhysicalLayer	F	T	F	0	T	wrn	F	T	F
DSX1 Far End Sending TS16 LOMF	dsx1 line status change	RcvFarEndLOMF	Y	IPPhysicalLayer	F	T	F	0	T	maj	F	T	F
DSX1 Near End Sending TS16 LOMF	dsx1 line status change	XmtFarEndLOMF	Y	IPPhysicalLayer	F	T	F	0	T	maj	F	T	F
DSX1 Near End detects a test code	dsx1 line status change	RcvTestCode	Y	IPPhysicalLayer	F	T	F	0	T	maj	F	T	F
DSX1 any line status not defined here	dsx1 line status change	OtherFailure	Y	IPPhysicalLayer	F	T	F	0	T	min	F	T	F

Table 42-17 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 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
DSX3 Looping the received signal	dsx3 line status change	LoopbackState	Y	IPhysicalLayer	F	T	F	0	T	maj	F	T	F

Table 42-17 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 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

Table 42-17 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
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
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
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

Table 42-17 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
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
Pseudo wire tunnel up	pseudo wire tunnel traps	Pseudo wire tunnel up	ce-pw-tunnel-status-snmpp, ce-vfi-status-telnet	IP/MPLS Layer 2 MplsTunnel	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-snmpp, ce-vfi-status-telnet	IP/MPLS Layer 2 MplsTunnel	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

Table 42-17 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 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

Cisco IOX V2/V3 Trap Registry Parameters

Table 42-18 lists the associated event types, event subtypes, and Cisco ANA registry parameters for the Cisco IOX SNMP V2/V3 traps shown in Table 42-6.

Table 42-18 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	IBgpNeigh borEntry	F	T	F	0	T	info	F	T	T
Cisco BGP down trap	cisco bgp trap	cisco bgp down trap	N	IBgpNeigh borEntry	F	T	T	0	T	maj	F	T	T
Cisco BGP established trap	cisco bgp trap	cisco bgp established trap	N	IBgpNeigh borEntry	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	IProfileCo ntainer (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	IProfileCo ntainer (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 -comma nd	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 -comma nd	IModule	F	F	F	0	T	clr	F	T	T
cefc FRU inserted	cefc fru removed	cefc fru inserted	physical -comma nd	IModule	F	F	F	0	T	clr	F	T	T
cefc FRU removed	cefc fru removed	cefc fru removed	physical -comma nd	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 -comma nd	IModule	F	T	T	0	T	maj	F	F	T

Table 42-18 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 42-18 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 42-18 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-snmptelnet	IP/MPLS Tunnel	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-snmptelnet	IP/MPLS Tunnel	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 42-18 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 42-18 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 42-18 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 42-18 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-snmptelnet	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-snmptelnet	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 42-18 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 42-18 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	IManaged Element	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	IPortLayer 1	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	IPortLayer 1	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	IPortLayer 1	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	IPortLayer 1	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	IPortLayer 1	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	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	minor	F	T	F

Table 42-18 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	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

Cisco MIB2 V1 Trap Registry Parameters

Table 42-19 lists the associated event types, event subtypes, and Cisco ANA registry parameters for the Cisco MIB2 SNMP V1 traps shown in Table 42-7.

Table 42-19 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
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

Table 42-19 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 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

Table 42-19 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 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
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

Table 42-19 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 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	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	190000	F	info	T	T	F
BGP down trap	bgp trap	bgp down trap	N	IBgpNeighborEntry	F	T	T	0	T	maj	F	T	T

Table 42-19 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
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	info	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	T	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
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	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

Table 42-19 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 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
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

Table 42-19 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
ipv6 interface state changed	ipv6-if-state-change-d	ipv6-if-state-c-hanged	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	F	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	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	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

Table 42-19 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-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 42-20 lists the associated event types, event subtypes, and Cisco ANA registry parameters for the Cisco MIB2 SNMP V2/V3 traps shown in Table 42-8.

Table 42-20 Cisco MIB2 V2/V3 Trap Registry Parameters

Short Description	Event Type	Event Subtype	Expedited 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 42-20 Cisco MIB2 V2/V3 Trap Registry Parameters (continued)

Short Description	Event Type	Event Subtype	Expedited 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-mlp ppbundle-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	IPPhysicalLayer	F	T	T	0	T	min	F	T	T

Table 42-20 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-stat us-telnet/ mtop-mlp ppbundle- status-teln et/mtop-i ma-group- state-telne t/mtop-ce m-group-s tatus/bund le-status/ mpls traffic engineerin g tunnel informatio n/basetech -lldp-neig hbors-snm p/basetech -cdp-neig hbors-snm p/port-stat us/ip interface oper status	IPPhysicalL ayer	F	F	F	0	F	clr	F	T	T
ipv6 interface state changed	ipv6-if-state-changed	ipv6-if-state-changed	N	IManagedE lement	F	F	F	0	T	min	F	T	F
OSPF interface state changed to Down	ospf if state down	ospf if state down	N	IIPInterfac e	F	T	T	0	F	info	F	T	T
OSPF interface state changed to Up	ospf if state down	ospf if state up	N	IIPInterfac e	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	IProfileCon tainer (OSPF)	F	T	T	0	F	min	F	T	T
OSPF neighbor state down	ospf neighbor state down	ospf neighbor state down	N	IIPInterfac e	T	T	T	0	F	maj	T	T	T
OSPF neighbor state up	ospf neighbor state down	ospf neighbor state up	N	IIPInterfac e	F	F	F	0	F	clr	F	T	T

Table 42-20 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 42-20 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 42-20 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	NetEquipOSS	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 42-20 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 42-20 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 42-21 lists the associated event types, event subtypes, and Cisco ANA registry parameters for the Cisco ACE SNMP V1 traps shown in Table 42-9.

Table 42-21 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
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 42-22 lists the associated event types, event subtypes, and Cisco ANA registry parameters for the Cisco ACE SNMP V2/V3 traps shown in Table 42-10.

Table 42-22 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	Min or	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	Min or	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	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	Min or	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	Min or	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	Min or	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	Min or	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	Min or	F	T	F

Table 42-22 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
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 42-23 lists the associated event types, event subtypes, and Cisco ANA registry parameters for the Cisco ACE SNMP V1 traps shown in Table 42-11.

Table 42-23 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

Table 42-23 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
cefc power status up	cefc power status changed	cefc power status up	physical-c ommand	IModule	F	F	F	0	F	clr	F	T	T
cefc FRU inserted	cefc fru removed	cefc fan status up	physical-c ommand	IModule	F	F	F	0	T	clr	F	T	T
cefc FRU removed	cefc fru removed	cefc fru removed	physical-c ommand	IModule	F	T	T	0	T	maj	F	T	T
sensor value crossed threshold in entSensorThres holdTable	entity sensor threshold notification	entity sensor threshold notification	N	IManagedE lement	F	F	F	0	F	maj	T	T	T
cps IfVlan Secure MacAddr Violation Trap	cps-IfVlan-S ecur-MacAd dr-Violation-Trap	cps-IfVlan-S ecur-MacAd dr-Violation-Trap	N	IPortLayer 1	F	F	T	0	F	maj	T	T	F
cps Secure MacAddr Violation Trap	cps-Secure-MacAddr-Vi olation-Trap	cps-Secure-MacAddr-Vi olation-Trap	N	IPortLayer 1	F	F	T	0	F	maj	T	T	F
Stpx Pvid Inconsistency Trap	stpx port inconsistency update	PvidInconsist ent trap	N	IManagedE lement	F	T	F	0	F	info	F	T	F
Stpx Type Inconsistency Trap	stpx port inconsistency update	TypeInconsis tent trap	N	IManagedE lement	F	T	F	0	F	info	F	T	F
stpx loop inconsistency discovered	stpx loop inconsistency update	stpx loop inconsistency discovered	N	IManagedE lement	F	T	F	0	F	maj	T	T	F
stpx loop inconsistency resolved	stpx loop inconsistency update	stpx loop inconsistency resolved	N	IManagedE lement	F	F	F	0	F	clr	T	T	F
stpx root inconsistency discovered	stpx root inconsistency update	stpx root inconsistency discovered	N	IManagedE lement	F	T	F	0	F	maj	T	T	F
stpx root inconsistency resolved	stpx root inconsistency update	stpx root inconsistency resolved	N	IManagedE lement	F	F	F	0	F	clr	T	T	F

Table 42-23 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
SNMP Link down	snmp link down	snmp link down	ip interface oper status,port -status	IPPhysicalL ayer	F	T	F	0	T	min	F	T	T
SNMP Link up	snmp link down	snmp link up	ip interface oper status,port -status	IPPhysicalL ayer	F	T	F	0	F	clr	F	T	T
RMON Rising Alarm	RMON-Alarm-Trap	Rising Alarm	N	IManagedE lement	F	T	F	0	T	WA RNI NG	F	T	F
RMON Falling Alarm	RMON-Alarm-Trap	Falling Alarm	N	IManagedE lement	F	T	F	0	T	WA RNI NG	F	T	F
Cold start trap	cold start trap	cold start trap	N	IManagedE lement	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	IManagedE lement	F	T	T	0	F	min	F	T	T
OSPF neighbor state down	ospf neighbor state down	ospf neighbor state down	N	IManagedE lement	T	T	T	0	F	maj	T	T	T
OSPF neighbor state up	ospf neighbor state down	ospf neighbor state up	N	IManagedE lement	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	IManagedE lement	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	IManagedE lement	F	F	F	0	F	clr	F	T	T
OSPF interface configuration error	ospf-if-config-err	ospf-if-config-err	N	IManagedE lement	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	IManagedE lement	F	T	F	0	F	min	F	T	F
OSPF interface authentication failure	ospf-if-authentic-fail	ospf-if-authentic-fail	N	IManagedE lement	F	T	F	0	F	wrn	T	T	F

Table 42-23 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 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
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

Table 42-23 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 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 42-24 lists the associated event types, event subtypes, and Cisco ANA registry parameters for the Cisco Nexus SNMP V2/V3 traps shown in Table 42-12.

Table 42-24 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

Table 42-24 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
cefc power status up	cefc power status changed	cefc power status up	physical-c ommand	IModule	F	F	F	0	F	clr	F	T	T
cefc FRU inserted	cefc fru removed	cefc fan status up	physical-c ommand	IModule	F	F	F	0	T	clr	F	T	T
cefc FRU removed	cefc fru removed	cefc fru removed	physical-c ommand	IModule	F	T	T	0	T	maj	F	T	T
sensor value crossed threshold in entSensorThres holdTable	entity sensor threshold notification	entity sensor threshold notification	N	IManagedE lement	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	IPortLayer 1	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	IPortLayer 1	F	F	T	0	F	maj	T	T	F
Stpx Pvid Inconsistency Trap	stpx port inconsistency update	PvidInconsistent trap	N	IManagedE lement	F	T	F	0	F	info	F	T	F
Stpx Type Inconsistency Trap	stpx port inconsistency update	TypeInconsistent trap	N	IManagedE lement	F	T	F	0	F	info	F	T	F
stpx loop inconsistency discovered	stpx loop inconsistency update	stpx loop inconsistency discovered	N	IManagedE lement	F	T	F	0	F	maj	T	T	F
stpx loop inconsistency resolved	stpx loop inconsistency update	stpx loop inconsistency resolved	N	IManagedE lement	F	F	F	0	F	clr	T	T	F
stpx root inconsistency discovered	stpx root inconsistency update	stpx root inconsistency discovered	N	IManagedE lement	F	T	F	0	F	maj	T	T	F
stpx root inconsistency resolved	stpx root inconsistency update	stpx root inconsistency resolved	N	IManagedE lement	F	F	F	0	F	clr	T	T	F

Table 42-24 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
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
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

Table 42-24 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 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
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

Table 42-24 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 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



CHAPTER 43

Syslogs

This chapter provides detailed information about the syslogs supported in Cisco ANA. Syslogs appear in the Cisco ANA EventVision Syslog tab. (For information about Cisco ANA EventVision, see the [Cisco Active Network Abstraction 3.7.1 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 Cisco ANA 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 Cisco ANA processes them (such as their severity, whether they are ticketable, can be correlated, are autocleared, and so on).

Cisco ANA 3.7.1 users can enable an additional IP in the device for traps and syslogs. This new feature is called Multisource Events. When Cisco ANA 3.7.1 receives a trap or syslog from that device (from the new IP) it will still recognize the device. For more details on multisource events see [Cisco ANA 3.7.1 Release notes](#).

This chapter includes the following sections:

- [Cisco ASR 9000 Syslogs, page 43-2](#)
- [Cisco IOS Syslogs, page 43-3](#)
- [Cisco IOX Syslogs, page 43-20](#)
- [Cisco ACE Syslogs, page 43-32](#)
- [Cisco Nexus Syslogs, page 43-36](#)
- [Cisco ASR 9000 Syslog Registry Parameters, page 43-37](#)
- [Cisco IOS Syslog Registry Parameters, page 43-39](#)
- [Cisco IOX Syslog Registry Parameters, page 43-61](#)
- [Cisco ACE Syslog Registry Parameters, page 43-71](#)
- [Cisco Nexus Syslog Registry Parameters, page 43-76](#)

Cisco ASR 9000 Syslogs

Table 43-1 lists the Cisco ASR 9000 Syslogs supported in Cisco ANA.

Table 43-1 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_WARNIN G_HIGH_WATERMARK	BFD rate limit high warning syslog	%L2-BFD-4-RATE_LIMIT_WARNIN G_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_LOOPB ACK	Ethernet OAM Remote loopback session started/stopped syslog	%L2-ELO-6-INTF_REMOTE_LOOPB ACK : TenGigE0/2/0/3: OAM remote loopback has been stopped on the interface	Ethernet OAM Remote loopback session stopped Syslog

Table 43-1 Cisco ASR 9000 Syslogs (continued)

Syslog Name	Description	Raw Format	Short Description
L2-ELO-6-INTF_REMOTE_LOOPB ACK	Ethernet OAM Remote loopback session started/stopped syslog	%L2-ELO-6-INTF_REMOTE_LOOPB ACK : 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_LOOPB ACK	Ethernet OAM Remote loopback session started/stopped syslog	%L2-ELO-6-INTF_REMOTE_LOOPB ACK : 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_LOOPB ACK	Ethernet OAM Remote loopback session started/stopped syslog	%L2-ELO-6-INTF_REMOTE_LOOPB ACK : 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

Cisco IOS Syslogs

Table 43-2 lists the Cisco IOS syslogs supported in Cisco ANA.

If SNMP syslogs are disabled in a device, wrapped syslogs are enabled by Cisco ANA 3.7.1. Wrapped syslogs are SNMP traps that enclose the syslog information. For more details on wrapped syslogs, see [Cisco ANA 3.7.1 Release notes](#).

Table 43-2 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
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

Table 43-2 Cisco IOS Syslogs (continued)

Syslog Name	Description	Raw Format	Short Description
DUAL-3-SIA	The EIGRP router hasn't received a reply to a query from one or more neighbors within the time allotted, so it clears the neighbors that didn't 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
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 router's configuration 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

Table 43-2 Cisco IOS Syslogs (continued)

Syslog Name	Description	Raw Format	Short Description
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
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

Table 43-2 Cisco IOS Syslogs (continued)

Syslog Name	Description	Raw Format	Short Description
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
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 isis syslog	%CLNS-5-ADJCHANGE: ISIS: Adjacency to edge-02(POS0/0) Down, hold time expired	IS-IS neighbor down syslog
CLNS-5-ADJCHANGE	handle isis syslog	%CLNS-5-ADJCHANGE: ISIS: Adjacency to edge-02(POS0/0) Up, hold time expired	IS-IS neighbor up syslog

Table 43-2 Cisco IOS Syslogs (continued)

Syslog Name	Description	Raw Format	Short Description
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
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

Table 43-2 Cisco IOS Syslogs (continued)

Syslog Name	Description	Raw Format	Short Description
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-(REMIINS)CARD	handle module out syslog	%OIR-6-INSCARD: Card inserted from slot 4, interfaces disabled	card in syslog
OIR-6-(REMIINS)CARD	handle module out syslog	%OIR-6-REMCARD: Card removed from slot 4, interfaces disabled	card out syslog
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

Table 43-2 Cisco IOS Syslogs (continued)

Syslog Name	Description	Raw Format	Short Description
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
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

Table 43-2 Cisco IOS Syslogs (continued)

Syslog Name	Description	Raw Format	Short Description
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_DISABLE D: 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
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

Table 43-2 Cisco IOS Syslogs (continued)

Syslog Name	Description	Raw Format	Short Description
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_RESOLUTION: 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_RESOLUTION: 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
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

Table 43-2 Cisco IOS Syslogs (continued)

Syslog Name	Description	Raw Format	Short Description
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 Secondary 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
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

Table 43-2 Cisco IOS Syslogs (continued)

Syslog Name	Description	Raw Format	Short Description
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
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

Table 43-2 Cisco IOS Syslogs (continued)

Syslog Name	Description	Raw Format	Short Description
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
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

Table 43-2 Cisco IOS Syslogs (continued)

Syslog Name	Description	Raw Format	Short Description
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
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

Table 43-2 Cisco IOS Syslogs (continued)

Syslog Name	Description	Raw Format	Short Description
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
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: V11 Grp 1 state Backup -> Master	VRRP backup to master syslog
VRRP-6-STATECHANGE	VRRP state change syslog	%VRRP-6-STATECHANGE: V12 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

Table 43-2 Cisco IOS Syslogs (continued)

Syslog Name	Description	Raw Format	Short Description
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
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

Table 43-2 *Cisco IOS Syslogs (continued)*

Syslog Name	Description	Raw Format	Short Description
ETHERNET_OAM-6-LOOPBACK	Link loopback OAM Event	%ETHERNET_OAM-6-LOOPBACK: Interface Gi1/1/1 has exited the slave loopback mode.	Loam 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
OIR-SP-6-REMCARD	handle card remove syslog	%OIR-SP-6-REMCARD: Card removed from slot 3, interfaces disabled	card out syslog

Cisco IOX Syslogs

Table 43-3 lists the Cisco IOX Syslogs supported in Cisco ANA.

Table 43-3 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-CHANGE D: Interface Ethernet5/1, changed state to administratively up	Link down syslog
LINK-5-CHANGED	The interface has changed state.	%LINK-5-CHANGE D: Interface Ethernet5/1, changed state to administratively down	Link up syslog
LINEPROTO-5-UPDOWN	The data link level line protocol changed state.	%LINEPROTO-5-UP DOWN: 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-UP DOWN: Line protocol on Interface GigabitEthernet1/0/1, changed state to up	Line up 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 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

Table 43-3 Cisco IOX Syslogs (continued)

Syslog Name	Description	Raw Format	Short Description
ENVMON-ADDITIVE-POWER-OVERBUDGET	The power calculated in use by the chassis exceeds that available by the powershell. 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 = 0x x)	envmon fan 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 : 1 temperature has reached high level	envmon tempreature 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 tempreature 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

Table 43-3 Cisco IOX Syslogs (continued)

Syslog Name	Description	Raw Format	Short Description
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 tempreature 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_CLEAR : 1 temperature has returned to a normal level	envmon tempreature clear syslog

Table 43-3 *Cisco IOX Syslogs (continued)*

Syslog Name	Description	Raw Format	Short Description
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-SHELF_MGR-3-SHUTDOWN_RESET : Node 0/SM2/* is reset due to admin shut request	Module reset syslog

Table 43-3 Cisco IOX Syslogs (continued)

Syslog Name	Description	Raw Format	Short Description
NODE-STATE-CHANGE	Indicates a change in the card oper status	PLATFORM-INVMG R-6-NODE_STATE_ CHANGE : Node: 0/RP0/*, state: BRINGDOWN	Card oper status changed
NODE-STATE-CHANGE	Indicates a change in the card oper status	PLATFORM-INVMG R-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/CPU 0/1	pim neighbor loss syslog
PIM-5-NBRCHG	handle pim neighbor syslog	PIM-5-NBRCHG: neighbor 192.168.2.1 UP on MgmtEth0/RSP0/CPU 0/1	pim neighbor up syslog
PIM-5-UPDOWN	handle pim interface syslog	ROUTING-IPV4_PI M-5-INTCHG : PIM interface GigabitEthernet0/3/0/ 0 DOWN	pim interface down syslog
PIM-5-UPDOWN	handle pim interface syslog	ROUTING-IPV4_PI M-5-INTCHG : PIM interface GigabitEthernet0/3/0/ 0 UP	pim interface up syslog

Table 43-3 Cisco IOX Syslogs (continued)

Syslog Name	Description	Raw Format	Short Description
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-SHELF MGR-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-SHELF MGR-3-POWERDOWN_RESET : Node 0/0/CPU0 is powered on due to admin power on request	Card oper status changed
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

Table 43-3 Cisco IOX Syslogs (continued)

Syslog Name	Description	Raw Format	Short Description
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 7.7.7.0, 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
MGBL-INVENTORY-6-PORTS	Sent by the XR device after a card-in event has occurred and the If and Entity tables are in sync. Once Cisco ANA 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

Table 43-3 Cisco IOX Syslogs (continued)

Syslog Name	Description	Raw Format	Short Description
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
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

Table 43-3 Cisco IOX Syslogs (continued)

Syslog Name	Description	Raw Format	Short Description
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-IPv6	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.	%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-IPv6	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.	%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 43-3 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
BGP-5-ADJCHANGE-IPv6	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	Routing BGP neighbor down syslog
BGP-5-ADJCHANGE-IPv6	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	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

Table 43-3 Cisco IOX Syslogs (continued)

Syslog Name	Description	Raw Format	Short Description
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
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

Table 43-3 Cisco IOX Syslogs (continued)

Syslog Name	Description	Raw Format	Short Description
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
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

Table 43-3 Cisco IOX Syslogs (continued)

Syslog Name	Description	Raw Format	Short Description
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 LOW	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

Cisco ACE Syslogs

Table 43-4 lists the Cisco ACE Syslogs supported in Cisco ANA.

Table 43-4 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

Table 43-4 Cisco ACE Syslogs (continued)

Syslog Name	Description	Raw Format	Short Description
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
ACE-1-727003	Mismatch in context names detected for FT group.	%ACE-1-727003: hostname: HA: Mismatch in context names detected for FT	Mismatch in context names detected for FT group
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

Table 43-4 Cisco ACE Syslogs (continued)

Syslog Name	Description	Raw Format	Short Description
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
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 43-4 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 43-4 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 43-5 lists the Cisco Nexus Syslogs supported in Cisco ANA.

Table 43-5 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

Cisco ASR 9000 Syslog Registry Parameters

Table 43-6 lists the associated event types, event subtypes, and Cisco ANA registry parameters for the Cisco ASR 9000 syslog shown in Table 43-1.

Table 43-6 Cisco ASR 9000 Syslog Registry Parameters

Short Description	Event Type	Event Subtype	Subtype Value	Expedited 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	F	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
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 authentication failed syslog	rip authentication failed syslog	N/A	N	IIPInterface	F	F	F	0	T	min	F	T	F
RIP configuration error syslog	rip configuration error syslog	rip configuration error syslog	N/A	N	IManagedElement	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	IManagedElement	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	IPhysicalLayer	F	T	F	0	F	maj	F	T	F

Table 43-6 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
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
Ethernet OAM Remote loopback session stopped Syslog	Ethernet OAM loopback session stopped	Ethernet OAM Remote loopback session stopped	remote,stopped	oam	IPhysicalLayer	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,started	oam	IPhysicalLayer	F	F	F	0	T	min	F	T	F
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

Table 43-6 Cisco ASR 9000 Syslog Registry Parameters (continued)

Short Description	Event Type	Event Subtype	Subtype Value	Expedited Polling	Event Source (IMO Name)	Activate	Correlate	Is Correlation Allowed	Weight	Auto Clear	Severity	Is Ticketable	Auto Remove	Flapping
CFM cc error syslog	CFM cc error syslog	CFM cc error syslog	errors set		ICFMServic e	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		ICFMServic e	F	F	F	0	F	clr	F	T	F

Cisco IOS Syslog Registry Parameters

Table 43-7 lists the associated event types, event subtypes, and Cisco ANA registry parameters for the Cisco IOS syslogs shown in Table 43-2.

Table 43-7 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-mlpp pbundle-st atus-telnet/ mtop-ima- group-state -telnet/mto p-cem-gro up-status/b un dle-status/ mpls traffic engineerin g tunnel informatio n/ip interface oper status	IIPInterface	F	T	F	0	T	maj	F	T	T
Link up syslog	link down syslog	link up syslog		mtop-mlpp pbundle-st atus-telnet/ mtop-ima- group-state -telnet/mto p-cem-gro up-status/b un dle-status/ mpls traffic engineerin g tunnel informatio n/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
FR DLCI up syslog	dlci change syslog	dlci up		N	IPhysicalLayer	F	F	F	0	F	clr	F	T	F

Table 43-7 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
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 timed out syslog	EIGRP router query to neighbors timed out syslog	EIGRP router query to neighbors timed out 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
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

Table 43-7 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 down syslog	line down syslog	line down syslog		basetech-ll dp-neighb ors-snmp/b asetech-cd p-neighbor s-snmp/mt op-mlpppb undle-statu s-telnet/mt op-ima-gro up-state-te lnet/mtop- cem-group -status/bun dle-status/ mpls trafficengi neering tunnel informatio n/port-stat us/ip interface oper status	IIPInterface	F	T	F	0	T	maj	F	T	T

Table 43-7 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-ll dp-neighb ors-snm p/b asetech-cd p-neighbor s-snm p/mt op-mlpppb undle-statu s-telnet/mt op-ima-gro up-state-te lnet/mtop- cem-group -status/bun dle-status/ mpls traffice ngi neering tunnel informatio n/port-stat us/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 43-7 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
BPDUs 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 down syslog	ospf neighbor down syslog		N	IIPInterface	T	T	F	0	T	maj	F	T	F
OSPF neighbor up syslog	ospf neighbor up syslog	ospf neighbor up syslog		N	IIPInterface	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 unblock syslog	span tree 2 loop guard unblock syslog		N	IPhysicalLayer	F	T	F	0	T	min	F	T	F

Table 43-7 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 43-7 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 43-7 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-mlppbundle-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 43-7 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-mlppbundle-status-telnet/ mtop-imagroup-state-telnet/ mto p-cem-group-status/ bundle-status/ mpls traffic engineering tunnel information/ ipinterfa ce 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-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
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 43-7 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	ntp 5 non port trunk syslog	ntp 5 non port trunk syslog		N	IPhysicalLayer	F	T	F	0	T	min	F	T	F
Interface changed to trunk	ntp 5 non port trunk syslog	ntp 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 43-7 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 43-7 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 43-7 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 stdbdy 4 err disable syslog	pm sp stdbdy 4 err disable	pm sp stdbdy 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 43-7 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 powersupply 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 43-7 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	N	IManagedElement	T	T	F	0	T	maj	F	T	F
OSPFv3 neighbor up syslog	ospfv3 neighbor syslog	ospfv3 neighbor up syslog	Up / FULL	N	IManagedElement	F	F	F	0	T	clr	F	T	F

Table 43-7 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 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
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

Table 43-7 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 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	ICfmMaintenance AssociationOid	F	T	F	0	T	minor	F	T	F
CFM Mep Up syslog	Mep Down syslog	Mep Up syslog	UP	N	ICfmMaintenance AssociationOid	F	F	F	0	F	clr	F	T	F
CFM Mep Down syslog	Mep Down syslog	Mep Down syslog	DOWN	N	ICfmMaintenance AssociationOid	F	T	F	0	T	minor	F	T	F
CFM Mep Up syslog	Mep Down syslog	Mep Up syslog	UP	N	ICfmMaintenance AssociationOid	F	F	F	0	F	clr	F	T	F
CFM Mep Down syslog	Mep Down syslog	Mep Down syslog	DOWN	N	ICfmMaintenance AssociationOid	F	T	F	0	T	minor	F	T	F
CFM Mep Up syslog	Mep Down syslog	Mep Up syslog	UP	N	ICfmMaintenance AssociationOid	F	F	F	0	F	clr	F	T	F
OSPFv3 neighbor down syslog	ospfv3 neighbor syslog	ospfv3 neighbor down syslog	Down / DOWN	N	IManagedElement	T	T	F	0	T	maj	F	T	F
OSPFv3 neighbor up syslog	ospfv3 neighbor syslog	ospfv3 neighbor up syslog	Up / FULL	N	IManagedElement	F	F	F	0	T	clr	F	T	F

Table 43-7 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 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
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

Table 43-7 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 exited the session	Ethernet OAM Session Syslog	EOAM exit session	EXIT	N	IPhysicalLayer	F	F	F	0	F	info	F	T	F
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

Table 43-7 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 - admin shutdown on peer	EOAMrfi dying gasp failure syslog	admin shutdown on peer	remote client down	oam	IPhysicalLayer	F	T	F	0	T	min	F	T	F
EOAM RFI dying gasp syslog - no ethernet oam	EOAMrfi 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	EOAMrfi 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	EOAMrfi 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	EOAMrfi dying gasp failure syslog	dying gasp clear syslog		oam	IPhysicalLayer	F	F	F	0	T	clr	F	T	F
EOAM RFI link fault syslog	EOAMrfi link fault syslog	EOAMrfi link fault syslog		oam	IPhysicalLayer	F	T	F	0	T	min	F	T	F
EOAM RFI link fault clear syslog	EOAMrfi link fault syslog	EOAMrfi 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

Table 43-7 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 Error disable syslog	PM SP Error disable syslog	PM SP Error disable syslog		oam	IPhysicalLayer	F	T	F	0	T	maj	F	T	F
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	transceiver removed syslog	transceiver inserted syslog		physical-c ommand	IPortConnector	F	F	F	0	F	clr	T	T	F
Transceiver removed syslog	transceiver removed syslog	transceiver removed syslog		physical-c ommand	IPortConnector	F	F	F	0	F	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

Cisco IOX Syslog Registry Parameters

Table 43-8 lists the associated event types, event subtypes, and Cisco ANA registry parameters for the Cisco IOX syslogs shown in Table 43-3.

Table 43-8 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

Table 43-8 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 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	IPortLayer 1	F	T	F	0	T	maj	F	T	T
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	IPortLayer 1	F	F	F	0	F	clr	F	T	T
OSPF neighbor down syslog	ospf neighbor syslog	ospf neighbor down syslog	Down	N	IIPInterface	T	T	F	0	T	maj	F	T	F
OSPF neighbor up syslog	ospf neighbor syslog	ospf neighbor up syslog	Up / LOADIN G to FULL	N	IIPInterface	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_C ONDITI ON	N	IManagedElement	F	T	T	0	T	maj	F	T	F
envmon condition clear syslog	envmon condition syslog	envmon condition clear syslog	ENV_C ONDITI ON_CL EAR	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

Table 43-8 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 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 tempreature syslog	envmon tempreature syslog	envmon tempreature syslog	OVERTEMP	N	IManagedElement	F	T	T	0	T	maj	F	T	F
envmon tempreature clear syslog	envmon tempreature clear syslog	envmon tempreature 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	POWER_SUPPLY_CURRENT	N	IManagedElement	F	T	T	0	T	maj	F	T	F
envmon powersupply clear syslog	envmon powersupply clear syslog	envmon powersupply clear syslog	POWER_SUPPLY_CURRENT_CLEAR	N	IManagedElement	F	F	F	0	F	clr	F	T	F
envmon powersupply syslog	envmon powersupply syslog	envmon powersupply syslog	POWER_SUPPLY_NONOP	N	IManagedElement	F	T	T	0	T	maj	F	T	F
envmon powersupply clear syslog	envmon powersupply clear syslog	envmon powersupply clear syslog	POWER_SUPPLY_NONOP_CLEAR	N	IManagedElement	F	F	F	0	F	clr	F	T	F
envmon powersupply syslog	envmon powersupply syslog	envmon powersupply syslog	POWER_SUPPLY_VOLTAGE	N	IManagedElement	F	T	T	0	T	maj	F	T	F

Table 43-8 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 powersupply clear syslog	envmon powersupply syslog	envmon powersupply clear syslog	POWER_SUPPLY_VOLTAGE_CLEAR	N	IManagedElement	F	F	F	0	F	clr	F	T	F
envmon temperature syslog	envmon temperature syslog	envmon temperature syslog	TEMP	N	IManagedElement	F	T	T	0	T	maj	F	T	F
envmon temperature clear syslog	envmon temperature clear syslog	envmon temperature 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 clear 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 clear 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

Table 43-8 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 down syslog	UNPOWERED / DOWN / BRING DOWN / NOT / DISABLED	card status	IModule	F	T	F	0	T	min	F	T	T
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	F	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

Table 43-8 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 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	IPortLayer 1	F	T	F	0	T	maj	F	T	T
Line up syslog	line down syslog	line up syslog	cleared	N	IPortLayer 1	F	F	F	0	F	clr	F	T	T
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

Table 43-8 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
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
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	min	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	N	IIPInterface	T	T	F	0	F	maj	T	T	F
OSPF routing neighbor up syslog	ospf routing neighbor syslog	ospf routing neighbor up syslog	Up / LOADIN G to FULL	N	IIPInterface	F	F	F	0	F	clr	F	T	F

Table 43-8 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 neighbor down syslog	ospfv3 neighbor syslog	ospfv3 neighbor down syslog	Down / DOWN	N	IManagedElement	T	T	F	0	T	maj	F	T	F
OSPFv3 neighbor up syslog	ospfv3 neighbor syslog	ospfv3 neighbor up syslog	Up / FULL	N	IManagedElement	F	F	F	0	F	clr	F	T	F
OSPFv3 routing neighbor down syslog	ospfv3 routing neighbor down syslog	ospfv3 routing neighbor down syslog	Down / DOWN	N	IManagedElement	F	T	F	0	T	maj	F	T	F
OSPFv3 routing neighbor up syslog	ospfv3 routing neighbor down syslog	ospfv3 routing neighbor up syslog	Up / FULL	N	IManagedElement	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	F	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

Table 43-8 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
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
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 checkpoint failure syslog	PLIM checkpoint 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

Table 43-8 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 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
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	F	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

Table 43-8 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
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	F	minor	F	T	F
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

Cisco ACE Syslog Registry Parameters

Table 43-9 lists the associated event types, event subtypes, and Cisco ANA registry parameters for the Cisco ACE syslogs shown in Table 43-4.

Table 43-9 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

Table 43-9 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
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-106021-syslog				F	F	F	0	T	maj	F	T	F
Access rule memory exhausted	ACE-106028-syslog	ACE-106028-syslog				F	F	F	0	T	maj	F	T	F
License manager exiting	ACE-444006-syslog	ACE-444006-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-456029-syslog				F	F	F	0	T	maj	F	T	F
Critical shared memory setup failure	ACE-456078-syslog	ACE-456078-syslog				F	F	F	0	T	maj	F	T	F
Critical Semaphore related errors	ACE-456080-syslog	ACE-456080-syslog				F	F	F	0	T	maj	F	T	F
A generic alert-level message	ACE-456085-syslog	ACE-456085-syslog				F	F	F	0	T	info	F	T	F
The ACE initialization has failed	ACE-456086-syslog	ACE-456086-syslog				F	F	F	0	T	maj	F	T	F
Peer IP address is not reachable	ACE-727001-syslog	ACE-727001-syslog				F	F	F	0	T	maj	F	T	F
Peer device is not reachable on an FT Interface	ACE-727002-syslog	ACE-727002-syslog				F	F	F	0	T	maj	F	T	F
Mismatch incontext names detected for FTgroup	ACE-727003-syslog	ACE-727003-syslog				F	F	F	0	T	maj	F	T	F
Both devices were detected to be Active for the same FT group	ACE-727004-syslog	ACE-727004-syslog				F	F	F	0	T	maj	F	T	F
Configuration could not be synced to the peer device	ACE-727005-syslog	ACE-727005-syslog				F	F	F	0	T	maj	F	T	F

Table 43-9 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
Peer is incompatible	ACE-727006-syslog	ACE-727006-syslog				F	F	F	0	T	maj	F	T	F
Module Initialization failure	ACE-727007-syslog	ACE-727007-syslog				F	F	F	0	T	maj	F	T	F
Failed to send heartbeats to peer	ACE-727008-syslog	ACE-727008-syslog				F	F	F	0	T	maj	F	T	F
Initialization failure - general	ACE-728001-syslog	ACE-728001-syslog				F	F	F	0	T	maj	F	T	F
Initialization failure - sticky	ACE-728002-syslog	ACE-728002-syslog				F	F	F	0	T	maj	F	T	F
Initialization failure - sticky hash	ACE-728003-syslog	ACE-728003-syslog				F	F	F	0	T	maj	F	T	F
The CLI end of line (EOL) function	ACE-100001-syslog	ACE-100001-syslog				F	F	F	0	T	maj	F	T	F
Reload started	ACE-199006-syslog	ACE-199006-syslog				F	F	F	0	T	maj	F	T	F
SNMPD initialization failed	ACE-212007-syslog	ACE-212007-syslog				F	F	F	0	T	maj	F	T	F
ICMP Manager Initialization Failed	ACE-313006-syslog	ACE-313006-syslog				F	F	F	0	T	maj	F	T	F
System experienced fatal failure	ACE-443001-syslog	ACE-443001-syslog				F	F	F	0	T	maj	F	T	F
License checkout failure	ACE-444001-syslog	ACE-444001-syslog				F	F	F	0	T	maj	F	T	F
Evaluation license expired	ACE-444004-syslog	ACE-444004-syslog				F	F	F	0	T	maj	F	T	F
Invalid stream	ACE-456014-syslog	ACE-456014-syslog				F	F	F	0	T	maj	F	T	F
Critical error parsing ACC module configuration	ACE-456090-syslog	ACE-456090-syslog				F	F	F	0	T	maj	F	T	F
Communication failure	ACE-727009-syslog	ACE-727009-syslog				F	F	F	0	T	maj	F	T	F

Table 43-9 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
Data replication failed and not synced to the peer device	ACE-727010-syslog	ACE-727010-syslog				F	F	F	0	T	maj	F	T	F
Configuration synchronization does not occurred	ACE-727011-syslog	ACE-727011-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-727012-syslog				F	F	F	0	T	info	F	T	F
The peer is now reachable	ACE-727013-syslog	ACE-727013-syslog				F	F	F	0	T	info	F	T	F
The redundancy heartbeats from a peer have become unidirectional	ACE-727014-syslog	ACE-727014-syslog				F	F	F	0	T	maj	F	T	F
Detected mismatch in heartbeat interval from the peer	ACE-727015-syslog	ACE-727015-syslog				F	F	F	0	T	info	F	T	F
The replication is being carried out to a peer	ACE-727016-syslog	ACE-727016-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_General-728033-syslog	ACE-LB_General-728033-syslog				F	F	F	0	T	info	F	T	F

Table 43-9 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 43-10 lists the associated event types, event subtypes, and Cisco ANA registry parameters for the Cisco Nexus syslogs shown in Table 43-5.

Table 43-10 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,St andby	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



PART 4

Commands



CHAPTER 44

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 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 ANA 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, Cisco ANA 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

Cisco ANA 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

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

Cisco ANA associates alarms with the corresponding MEP or global CFM logical inventory objects.

Cisco ANA 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

See Part 1—Cisco VNEs for details on the software versions Cisco ANA supports for these network elements.



Note

You can execute the CFM commands that are supported by the software installed on the device.

Configuring CFM Components

The following commands facilitate the configuration of CFM components.

- [Configure CFM Maintenance Domain, page 44-3](#)
- [Configure CFM Global Parameters, page 44-4](#)
- [Configure CFM MIP, page 44-5](#)
- [Configure CFM Continuity Check, page 44-6](#)
- [Configure CFM Service ID, page 44-7](#)
- [Configure CFM MEP, page 44-8](#)
- [Enable CFM Continuity Check, page 44-9](#)
- [Enable CFM SNMP Server Traps, page 44-10](#)

**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 domain is owned and operated by a single entity and 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.

Input Parameter	Description
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 parallels 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 run the commands, click **Execute**.
Any errors are displayed in the Result tab.
- Step 6** 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 run the commands, click **Execute**.
Any errors are displayed in the Result tab.
- Step 6** 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 relay function.
- All CFM frames at a higher level are forwarded, independent of whether they arrive from the wire or 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.

- 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	VLAN ID on which to apply the remote maintenance point ID. The VLAN ID range is from 1 to 4094. Alternatively, you can choose <i>any</i> 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 device.
Inner VLAN ¹	Check the checkbox if you have an inner VLAN tag.
Inner VLANs ¹	Inner VLAN ID on which to apply the remote maintenance 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 (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 run the commands, click **Execute**.
Any errors are displayed in the Result tab.
- Step 6** 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 <i>any</i> 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 4094. You can choose: - A single VLAN ID from 1 to 4094 - A range of VLAN IDs separated by a hyphen (-) - A series of VLAN IDs separated by commas (,) <i>any</i> to specify all VLAN IDs
Interval for CC Messages	Interval, in seconds, for continuity check messages. The default value is 30 seconds.
Loss Threshold Level for CC Packets	Loss threshold level for continuity check packets. The default value is 2 seconds.

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 run the commands, click **Execute**.

Any errors are displayed in the Result tab.

Step 6 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, and is identified by a globally unique service ID. The Service VLAN ID range is from 1 to 4094.

Input Parameter	Description
Inner VLAN ¹	Check the checkbox if you have an inner VLAN tag.
Inner VLANs ¹	Inner VLAN ID on which to apply the remote maintenance 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 (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 run the commands, click **Execute**.
Any errors are displayed in the Result tab.
- Step 6** 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

- 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.

Input Parameter	Description
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. It is also used to 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 4094. Alternatively, you can choose <i>any</i> 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 device.

- 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 run the commands, click **Execute**.
Any errors are displayed in the Result tab.
- Step 6** 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
Maintenance Level	Maintenance level number. The range is from 0 to 7. Alternatively, you can choose <i>any</i> 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 <i>any</i> to specify all VLAN IDs.

- 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 run the commands, click **Execute**.
Any errors are displayed in the Result tab.

Step 6 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 run the command, click **Execute**.
- Any errors are displayed in the Result tab.
- Step 4** 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 44-10](#)
- [Diagnose CFM with Show MEP Crosscheck Status, page 44-11](#)
- [Diagnose CFM with Ping Remote MEP with MAC, page 44-11](#)
- [Diagnose CFM with Ping Remote MEP with MPID, page 44-12](#)
- [Diagnose CFM with Ping Remote MEP with Multicast, page 44-13](#)
- [Diagnose CFM with Traceroute Remote MEP with MAC, page 44-13](#)
- [Diagnose CFM with Traceroute Remote MEP with MPID, page 44-14](#)

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 run the command, click **Execute**.
- Any errors are displayed in the Result tab.

- Step 4** 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 run the command, click **Execute**.
- Any errors are displayed in the Result tab.
- Step 4** 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 <i>aaaa.bbbb.cccc</i> ; 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 run the commands, click **Execute**.
Any errors are displayed in the Result tab.
- Step 6** 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 Service configuration.
VLAN ID ¹	VLAN ID on which to apply the remote maintenance 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 (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 run the commands, click **Execute**.
Any errors are displayed in the Result tab.
- Step 6** 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 run the commands, click **Execute**.
Any errors are displayed in the Result tab.
- Step 6** 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 <i>aaaa.bbbb.cccc</i> . The default MAC address is 0000.0000.0000.
Domain Name	Name of the domain.

Input Parameter	Description
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 run the commands, click **Execute**.
Any errors are displayed in the Result tab.
- Step 6** 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 run the commands, click **Execute**.
Any errors are displayed in the Result tab.

Step 6 To close the dialog box, click **Close**.



CHAPTER 45

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 ANA discovers and displays the following REP attributes in the Logical Inventory tree of the Cisco ANA NetworkVision application:

- REP Segments. All of these segments are identified by a REP segment ID 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.

The following REP port attributes are modeled in Cisco ANA:

- 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 ANA NetworkVision application.

You can view the REP port roles (open, alternate, and failed) in the Cisco ANA NetworkVision map. The REP port role is displayed as a tool-tip between the REP enabled trunk ports in the Ethernet links. Using the Cisco ANA NetworkVision 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.

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 3800X Carrier Ethernet Switch Routers
- Cisco ME 3600X Ethernet Access Switches
- Cisco Catalyst 3750 Metro Series Switches
- All Cisco Catalyst Switches

See Part 1—Cisco VNEs for details on the software versions Cisco ANA 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 run the commands, click **Execute**.
- 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 5** To close the dialog box, click **Close**.
-



CHAPTER 46

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. In future, Carrier Grade NAT may also offer 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 ANA 3.7.1 displays the following attributes in the logical inventory of the Cisco ANA NetworkVision application:

- Carrier Grade NAT Instance Name — The Carrier Grade NAT instance name identifies the Carrier Grade NAT instance.

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-1 Series Routers

See Part 1—Cisco VNEs for details on the software versions Cisco ANA 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.

Configuring Carrier Grade NAT Instance

Use the **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).
Address Family	Name of the IP address family. The default and only value is IPv4.
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 ([1-65535])	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 run the commands, click **Execute**.
- The newly added Carrier Grade NAT instance appears in the Carrier Grade NAT tree. Any errors are displayed in the Result tab.
- Step 6** 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 run the commands, click **Execute**.
The Carrier Grade NAT instance is no longer visible under the Carrier Grade NAT tree. Any errors are displayed in the Result tab.
- Step 6** 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
Carrier Grade NAT Instance Name	Name of the Carrier Grade NAT 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 run the commands, click **Execute**.
Any errors are displayed in the Result tab.
- Step 6** To close the dialog box, click **Close**.
-



CHAPTER 47

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 ANA supports the discovery and modeling of Any Transport over MPLS (AToM) and Ethernet over MPLS (EoMPLS) domains that span multisegment pseudowires.

Cisco ANA 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 ANA discovers and displays the pseudowires configured on a selected network element in the Logical Inventory tree of the Cisco ANA NetworkVision application. Each pseudowire is configured with the following set of attributes:

- Name—The name of the pseudowire.
- Multisegment Pseudowire—Whether or not the pseudowire is multisegment: 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 ANA NetworkVision application. The following tunnel or interface attributes are modeled in Cisco ANA:

- 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 pseudowire commands on all Cisco IOS and Cisco IOS XR devices that support pseudowire technology, such as Cisco 7200 series routers, Cisco 7600 series routers, ASR 9000 series aggregation services routers, and Cisco XR 12000 series routers.

See Part 1—Cisco VNEs for details on the software versions Cisco ANA 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 multi segment 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	Select Enable or Disable to activate or deactivate multisegment ping. Note This parameter is available only for Cisco IOS XR devices.
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.

Step 3 To see the command that will be applied on the device, click **Preview**.

Step 4 To run the command, click **Execute**.

Any errors are displayed in the Result tab.

Step 5 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 ID. 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 run the command, click **Execute**.

Any errors are displayed in the Result tab.

Step 5 To close the dialog box, click **Close**.



CHAPTER 48

Using Link 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 L-OAM protocol are discovery, link monitoring, remote fault detection, and remote loopback.

Supported Network Elements

You can run the L-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

See Part 1—Cisco VNEs for details on the software versions Cisco ANA supports for these network elements. To run the L-OAM commands, the software on the network element must support the L-OAM technology.

Configuring L-OAM Components

The following sections explain how to configure L-OAM components:

- [Applying a Template on an Interface, page 48-2](#)
- [Creating a Template, page 48-3](#)
- [Disabling OAM on an Interface, page 48-4](#)
- [Enabling OAM on an Interface, page 48-4](#)
- [Configuring OAM Parameters on an Interface, page 48-5](#)
- [Starting the Remote Loopback, page 48-5](#)
- [Stopping the Remote Loopback, page 48-6](#)



Note

In the GUI, parameters that are displayed in bold text are mandatory.

Applying a Template on an Interface

Use the **Apply Template on Interface** command to apply a template on an interface.

- Step 1** In the inventory window, expand the Logical Inventory tree.
- Step 2** Right-click the OAM node and choose **Commands > Apply Template on Interface**. The Apply 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 run the commands, click **Execute**.

Any errors are displayed in the Result tab.

Step 6 To close the dialog box, click **Close**.

Creating a Template

Use the **Create Template** command to create a template.

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 0 to 65535. The low threshold value must be lower than the high threshold.
Symbol-Period Threshold High	The range is from 1 to 65535. You can also enter none as an option.
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 0 to 65535. The low threshold value must be lower than the high threshold.
Frame Threshold High	The range is from 1 to 65535. You can also enter none as an option.
Frame-Period Window	The range is from 1 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 1 to 65535. You can also enter none as an option.
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. You can also enter none as an option.
Receive-Crc Window	The range is from 10 to 1800, which represents milliseconds in multiples of 100. The default is 100.
Receive-Crc Threshold High	The range is from 1 to 65535. You can also enter none as an option.
Transmit-Crc Window	The range is from 10 to 1800.
Transmit-Crc Threshold High	The range is from 1 to 65535. You can also enter none as an option.

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 run the commands, click **Execute**.

Any errors are displayed in the Result tab.

- Step 6** 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 run the commands, click **Execute**.
Any errors are displayed in the Result tab.
- Step 6** 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 run the commands, click **Execute**.

Any errors are displayed in the Result tab.

Step 6 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	Enables or disables 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 run the commands, click **Execute**.

Any errors are displayed in the Result tab.

Step 6 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 run the commands, click **Execute**.
Any errors are displayed in the Result tab.
- Step 6** 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 run the commands, click **Execute**.
Any errors are displayed in the Result tab.
- Step 6** To close the dialog box, click **Close**.



CHAPTER 49

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 ME 3400 Series Ethernet Access Switches

- Cisco MWR 2941 Mobile Wireless Routers

See Part 1—Cisco VNEs for details on the software versions Cisco ANA 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 49-2](#)
- [Configuring Multipoint-to-Multipoint or Point-to-Point Ethernet Virtual Connection, page 49-2](#)
- [Configuring UNI on an Interface, page 49-3](#)
- [Enabling Ethernet LMI on an Interface, page 49-4](#)
- [Configuring the Service Instance VLAN ID on an Interface, page 49-4](#)



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.

-
- 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 run the command, click **Execute**.
- Any errors are displayed in the Result tab.
- Step 4** 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	Unified network interface (UNI) range, from 2 to 1024. The default is 2.
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 run the commands, click **Execute**.
Any errors are displayed in the Result tab.
- Step 6** 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. Length can be from 1 to 64.

- 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 run the commands, click **Execute**.
Any errors are displayed in the Result tab.
- Step 6** 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 run the commands, click **Execute**.
Any errors are displayed in the Result tab.
- Step 6** 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 4294967295.
VLAN-to-EVC map	The value can be [1-4094], any, default, or untagged.
Evc Name	Name of the Ethernet virtual connection.

- 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 run the commands, click **Execute**.
Any errors are displayed in the Result tab.
- Step 6** To close the dialog box, click **Close**.
-



INDEX

Numerics

- 1588 Clocking
 - description [32-1](#)
- 6VPE
 - description [12-2](#)

A

- ACL
 - description [34-1](#)
 - IMOs [34-2](#)
 - network topology [34-3](#)
 - service alarms [34-3](#)
- Adaptive Clock Recovery (ACR)
 - description [32-2](#)
- adaptive polling
 - alarm description [41-4](#)
 - registry parameters [41-60](#)
- All IP Interfaces Down alarm [41-4, 41-62](#)
- ARP (Address Resolution Protocol)
 - description [10-2](#)
- ATM
 - description [20-1](#)
 - IMOs [20-3](#)
 - service alarms [20-14](#)
 - VNE topology type [38-7](#)
- ATM Cross Connect
 - description [20-2](#)
- ATM IMA Down
 - event registry [41-63](#)
- ATM IMA Service
 - alarm description [41-5, 41-46, 41-154](#)

B

- BFD
 - description [13-1](#)
 - IMOs [13-2](#)
 - service alarms [13-3](#)
- BGP
 - description [11-1](#)
 - service alarms [11-7](#)
 - VNE topology type [38-8](#)
- BGP alarms
 - BGP Link Down [41-7, 41-69, 41-199](#)
 - BGP Neighbor Loss [41-9, 41-10, 41-16, 41-17, 41-18, 41-19, 41-20, 41-21, 41-45, 41-51, 41-71](#)
 - BGP Process Down [41-10, 41-11, 41-74](#)
- Bidirectional Forwarding Detection. *See* BFD
- Border Gateway Protocol. *See* BGP
- Broken LSP Discovered alarm [41-11, 41-13, 41-75](#)
- business, VNE topology type [38-8](#)

C

- Card Down alarm [41-14, 41-75](#)
- Card Out alarm [41-14, 41-15, 41-76](#)
- CDP
 - description [26-2](#)
 - VNE topology type [38-6](#)
- CFM
 - description [19-1](#)
- CFM Domain Fault
 - registry [41-91](#)
- CGN (Carrier-Grade NAT), description [10-2](#)
- Channelized T3, OC3, DS3 Interface

- description [31-2](#)
- Circuit Emulation over MPLS
 - description [31-2](#)
- Clocking
 - IMOs [32-2](#)
- cloud VNE
 - Cloud Problem alarm [41-22, 41-92](#)
- Common Components
 - IMOs [37-1](#)
 - network topology [37-7](#)
 - service alarms [37-7](#)
- Component Unreachable alarm [41-23, 41-93](#)
- CPU usage
 - CPU Utilization alarm [41-15, 41-25, 41-95](#)

D

- description [33-1](#)
 - 1588 Clocking [32-1](#)
 - 6VPE [12-2](#)
 - ACL [34-1](#)
 - ACR [32-2](#)
 - ARP [10-2](#)
 - ATM [20-1](#)
 - ATM Cross Connect [20-2](#)
 - BFD [13-1](#)
 - BGP [11-1](#)
 - CDP [26-2](#)
 - CFM [19-1](#)
 - CGN [10-2](#)
 - Channelized T3, OC3, DS3 Interface [31-2](#)
 - Circuit Emulation over MPLS [31-2](#)
 - DSL [28-1](#)
 - DSx [31-2](#)
 - eBGP/iBGP [11-2](#)
 - EtherChannel [18-3](#)
 - Ethernet [18-2](#)
 - Ethernet LMI [19-2](#)
 - Frame Relay [21-1](#)
 - GRE [10-2](#)
 - HDLC [24-1](#)
 - HSRP [10-2](#)
 - IMA [20-2](#)
 - IP [10-1](#)
 - IPoDWDM [30-1](#)
 - IP SLA Responder Service [10-3](#)
 - IPv6 [10-2](#)
 - ISDN [22-1](#)
 - LAG [18-2](#)
 - Layer 2 Tunnel Protocol [25-1](#)
 - LDP [15-2](#)
 - Link OAM [19-2](#)
 - LLDP [26-1](#)
 - local switching [27-1](#)
 - MP-BGP [11-2](#)
 - MPLS [15-1](#)
 - MPLS TE [16-1](#)
 - MPoA [20-2](#)
 - Multilink PPP [23-2](#)
 - OSPF [11-2](#)
 - PBB [10-3](#)
 - POS [23-2](#)
 - PPP [23-1](#)
 - PPPoA [23-2](#)
 - PPPoE [23-2](#)
 - PPPoFR [23-2](#)
 - Pseudowire [17-1](#)
 - QinQ [18-2](#)
 - SDH [29-1](#)
 - SONET [29-1](#)
 - STP [18-3](#)
 - SyncE Clocking [32-1](#)
 - T3/E3 [31-2](#)
 - TDM [31-1](#)
 - VLAN (IEEE 802.1Q) [18-2](#)
 - VNE topology [38-1](#)
 - VRF [12-1](#)
 - VRF-Lite [12-1](#)

Device Unsupported alarm [41-26, 41-96](#)

Digital Signal Hierarchy. *See* DSx

Digital Subscriber Line. *See* DSL

Discard Packets alarm [41-26, 41-97](#)

discovery

- service alarms [26-4](#)

Discovery Protocols

- IMOs [26-2](#)

Dropped Packets alarm [41-27, 41-28, 41-98](#)

DS0 Bundle alarm

- event registry [41-99](#)

DS1 Path Link Down

- alarm [41-28](#)
- event registry [41-101](#)

DS1 Path Port Down

- alarm [41-29](#)
- event registry [41-106](#)

DS3 Path Link Down

- alarm [41-29](#)
- event registry [41-110](#)

DS3 Path Port Down

- alarm [41-30](#)
- event registry [41-115](#)

DSL

- description [28-1](#)
- IMOs [28-2](#)
- network topology [28-6](#)
- service alarms [28-6](#)

DSx

- description [31-2](#)

Dual Stack IP Changed

- event registry [41-119](#)

Dual Stack IP Changed alarm [41-31](#)

DWDM Service alarm [41-31, 41-32, 41-33](#)

- event registry [41-121, 41-123](#)

E

eBGP/iBGP, description [11-2](#)

EFP Down alarm [41-32, 41-125](#)

EtherChannel

- description [18-3](#)

Ethernet

- description [18-2](#)

- IMOs [18-5](#)

- service alarms [18-22, 19-11](#)

- VNE topology type [38-8](#)

Ethernet LMI

- description [19-2](#)

Ethernet OAM

- IMOs [19-2](#)

events

- security [40-1](#)

F

forwarding components,IMOs [9-6](#)

Frame Relay

- description [21-1](#)

- IMOs [21-1](#)

- service alarms [21-4](#)

- VNE topology type [38-8](#)

G

GRE

- GRE Keepalive alarm [41-33](#)

- subtype event registry [41-127](#)

- GRE Tunnel Down alarm [41-33, 41-129](#)

- GRE Tunnel endpoint OID structure [41-199](#)

GRE, description [10-2](#)

GRE Tunnel, VNE topology type [38-9](#)

H

HDLC

- description [24-1](#)

IMOs [24-2](#)

service alarms [23-5, 24-2](#)

VNE topology type [38-8](#)

High-Level Data Link Control. *See* HDLC

HSRP

HSRP Group Status Changed alarm [41-34, 41-130](#)

HSRP, description [10-2](#)

I

IEEE 802.1ad

description [18-2](#)

IMA

description [20-2](#)

IMO overview

forwarding components [9-6](#)

polling interval values [9-6](#)

related to networking [9-4](#)

schemes [9-6](#)

termination points [9-4](#)

Information Model Object. *See* IMO

Integrated Services Digital Network. *See* ISDN

Interface Status alarm [41-35, 41-132](#)

Inverse Multiplexing over ATM. *See* IMA

Investigation State alarm [41-37, 41-134](#)

IP

description [10-1](#)

IMOs [10-4](#)

service alarms [10-14](#)

IPoDWDM

description [30-1](#)

IMOs [30-2](#)

network topology [30-4](#)

service alarms [30-4](#)

IP SLA Responder Service, description [10-3](#)

IPv6, description [10-2](#)

ISDN

description [22-1](#)

IMOs [22-1](#)

service alarms [22-3](#)

K

keepalive message (GRE tunnel) [41-33](#)

L

L2TP Peer Not Established alarm [41-37, 41-135](#)

L2TP Sessions Threshold alarm [41-38, 41-137](#)

Label Distribution Protocol. *See* LDP

LAG (Link Aggregation)

description [18-2](#)

Layer 2 MPLS Tunnel Endpoint, OID structure [41-199](#)

Layer 2 Tunnel Down alarm [41-40, 41-142](#)

Layer 2 Tunnel Protocol

description [25-1](#)

IMOs [25-2](#)

service alarms [25-5](#)

LDP (Label Distribution Protocol), description [15-2](#)

LDP Neighbor Loss alarm [41-41, 41-143](#)

Link OAM

description [19-2](#)

links

Link Down alarm [41-42, 41-144](#)

Link Down alarm endpoint OID structure [41-198](#)

Link Utilization alarm [41-147](#)

Link Utilization alarm [41-43](#)

LLDP

description [26-1](#)

IMOs [26-2](#)

local switching

description [27-1](#)

IMOs [27-2](#)

network topology [27-3](#)

service alarms [27-3](#)

Logical Components

IMOs [36-1](#)

service alarms [36-4](#)
 Logical Port Down alarm [41-44, 41-150](#)

M

Memory Utilization alarm [41-46, 41-153](#)

MP-BGP, description [11-2](#)

MPLS

description [15-1](#)
 IMOs [15-2](#)
 service alarms [15-6](#)
 VNE topology type [38-8](#)

MPLS alarms

MPLS Black Hole Found alarm [41-47, 41-158](#)
 MPLS Interface Removed alarm [41-48, 41-159](#)
 MPLS TE Tunnel Down alarm [41-49, 41-162](#)
 MPLS TE Tunnel OID structure [41-196](#)

MPLS TE

IMOs [16-2](#)

MPLS TE

description [16-1](#)
 service alarms [16-5](#)

MPLS TE FRR State Changed

alarm [41-49](#)
 registry entries [41-160](#)

MPoA

description [20-2](#)

Multilink PPP, description [23-2](#)

Multiprotocol Label Switching. *See* MPLS

Multiprotocol Label Switching Traffic Engineering. *See* MPLS TE

N

network topology

ACL [34-3](#)
 Common Components [37-7](#)
 DSL [28-6](#)
 IPoDWDM [30-4](#)

local switching [27-3](#)

Serial Links [33-2](#)

SONET/SDH [29-5](#)

TDM/DSx [31-5](#)

O

obtaining documentation [i-xviii](#)

OSPF (Open Shortest Path First)

description [11-2](#)

P

Packet over SONET/SDH. *See* POS

PBB (Provider Backbone Bridge), description [10-3](#)

Physical Components

IMOs [35-1](#)
 service alarms [35-4](#)

physical layer, VNE topology type [38-9](#)

polling interval values, and IMOs [9-6](#)

port alarms

Port Down alarm [41-51, 41-168](#)

POS, description [23-2](#)

PPP

description [23-1](#)
 IMOs [23-3](#)
 service alarms [23-5](#)

PPPoA, description [23-2](#)

PPPoE, description [23-2](#)

PPPoFR, description [23-2](#)

Pseudowire

description [17-1](#)
 IMOs [17-2](#)

Pseudowire Emulation Edge-to-Edge. *See* PWE3

PWE3

service alarms [17-3](#)
 VNE topology type [38-9](#)

Q

QinQ

- description [18-2](#)
- Subinterface Down alarm [41-55](#)

R

- registry parameters, service alarms [41-58](#)
- related documentation [i-xvii](#)
- Routing Protocols
 - IMOs [11-3](#)
- Rx Dormant alarm [41-52, 41-171](#)
- Rx Utilization alarm [41-53, 41-173](#)

S

SBC

- IMOs [14-2](#)

- schemes, types of [9-6](#)

SDH

- description [29-1](#)
- IMOs [29-2](#)
- service alarms [29-5](#)

security

- events [40-1](#)

Serial Links [33-1](#)

- description [33-1](#)
- IMOs [33-2](#)
- network topology [33-2](#)
- service alarms [33-2](#)

service alarms

- ACL [34-3](#)
- ATM [20-14](#)
- BFD [13-3](#)
- BGP [11-7](#)
- Common Components [37-7](#)
- discovery [26-4](#)
- DSL [28-6](#)

Ethernet [18-22, 19-11](#)

Frame Relay [21-4](#)

HDLC [23-5, 24-2](#)

IP [10-14](#)

IPoDWDM [30-4](#)

ISDN [22-3](#)

Layer 2 Tunnel Protocol [25-5](#)

list of supported alarms [41-2](#)

local switching [27-3](#)

Logical Components [36-4](#)

MPLS [15-6](#)

MPLS TE [16-5](#)

overview [41-1](#)

Physical Components [35-4](#)

PPP [23-5](#)

PWE3 [17-3](#)

registry parameters [41-58](#)

SDH [29-5](#)

Serial Links [33-2](#)

SONET [29-5](#)

source OIDs [41-187](#)

TDM/DSx [31-5](#)

VRF [12-5](#)

Shelf Out alarm [41-54, 41-174](#)

SONET

description [29-1](#)

IMOs [29-2](#)

service alarms [29-5](#)

source OIDs (object identifiers) [41-187](#)

BGP Neighbor Entry OID [41-188](#)

DWDM Controller OID [41-190](#)

EFP OID [41-190](#)

IP Interface OID [41-191](#)

L2TP Peer OID [41-191](#)

Logical Port OID [41-192](#)

LSE (Label Switching Entity) OID [41-193](#)

LSE Entry OID [41-193](#)

Managed Element OID [41-194](#)

Module OID [41-195](#)

MP-BGP OID [41-195](#)
 MPLS TE Tunnel OID [41-196](#)
 Physical Layer OID [41-196](#)
 Shelf OID [41-197](#)
 Topological Link OID [41-197](#), [41-198](#)
 VLAN Tagged Interface OID [41-200](#)
 VSI OID [41-200](#)
 STP (Spanning Tree Protocol)
 description [18-3](#)
 Subinterface Down alarm [41-55](#), [41-181](#)
 submitting a service request [i-xviii](#)
 SyncE Clocking
 Description [32-1](#)
 Synchronous Digital Hierarchy. *See* SDH
 Synchronous Optical Network. *See* SONET

T

T3/E3
 description [31-2](#)
 TDM
 description [31-1](#)
 TDM/DSx
 IMOs [31-2](#)
 network topology [31-5](#)
 service alarms [31-5](#)
 technologies, supported [9-1](#)
 termination points, of IMOs [9-4](#)
 Tx Dormant alarm [41-56](#), [41-183](#)
 Tx Utilization alarm [41-57](#), [41-184](#)

V

VLAN (IEEE 802.1Q)
 description [18-2](#)
 VNE topology
 CDP [38-6](#)
 description [38-1](#)

physical layer [38-5](#)
 specifications [38-1](#)
 traffic signature [38-7](#)
 types
 ATM [38-7](#)
 BGP [38-8](#)
 business [38-8](#)
 Ethernet [38-8](#)
 Frame Relay [38-8](#)
 GRE Tunnel [38-9](#)
 HDLC [38-8](#)
 MPLS [38-8](#)
 physical layer [38-9](#)
 PPP [38-8](#)
 PWE3 [38-9](#)
 VPN [38-9](#)

VPN

VNE topology type [38-9](#)

VRF

description [12-1](#)
 IMOs [12-2](#)
 service alarms [12-5](#)

VRF-Lite

description [12-1](#)

VSI Down alarm [41-57](#), [41-185](#)

