



Cisco IP Solution Center Infrastructure Reference, 4.0

Corporate 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: 408 526-4100

Text Part Number: OL-6370-01



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

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

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

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

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

CCSP, CCVP, the Cisco Square Bridge logo, Follow Me Browsing, and StackWise are trademarks of Cisco Systems, Inc.; Changing the Way We Work, Live, Play, and Learn, and iQuick Study are service marks of Cisco Systems, Inc.; and Access Registrar, Aironet, ASIST, BPX, Catalyst, CCDA, CCDP, CCIE, CCIP, CCNA, CCNP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Cisco Unity, Empowering the Internet Generation, Enterprise/Solver, EtherChannel, EtherFast, EtherSwitch, Fast Step, FormShare, GigaDrive, GigaStack, HomeLink, Internet Quotient, IOS, IP/TV, iQ Expertise, the iQ logo, iQ Net Readiness Scorecard, LightStream, Linksys, MeetingPlace, MGX, the Networkers logo, Networking Academy, Network Registrar, *Packet*, PIX, Post-Routing, Pre-Routing, ProConnect, RateMUX, ScriptShare, SlideCast, SMARTnet, StrataView Plus, TeleRouter, The Fastest Way to Increase Your Internet Quotient, and TransPath are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries.

All other trademarks mentioned in this document or Website 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. (0502R)

Cisco IP Solution Center Infrastructure Reference, 4.0
Copyright © 2005, Cisco Systems, Inc.
All rights reserved.



About This Guide	xxx
Objective	xxx
Related Documentation	xxx
Audience	xxx
How This Book Is Organized	xxx
Document Conventions	xxx
Obtaining Documentation	xxx
Cisco.com	xxx
Ordering Documentation	xxx
Documentation Feedback	xxx
Obtaining Technical Assistance	xxx
Cisco Technical Support Website	xxx
Submitting a Service Request	xxx
Definitions of Service Request Severity	xxx
Obtaining Additional Publications and Information	xxx

CHAPTER 1

Getting Started	1-1
System Recommendations	1-1
Introduction	1-1
Structural Overview	1-2
Product Category Tabs	1-3
Links	1-3
Home	1-3
Shortcuts	1-3
Account	1-5
Index	1-5
Help	1-5
About	1-5
Logout	1-6
Customer	1-6
Common GUI Components	1-6
Filters	1-7
Rows per Page	1-7
Go To Page	1-7

Auto Refresh	1-8
Color Coding	1-8
Icons	1-10
Service Inventory	1-11
Service Design	1-13
Monitoring	1-15
Administration	1-16

CHAPTER 2

WatchDog Commands 2-1

startdb Command	2-1
Description	2-1
Syntax	2-1
startns Command	2-2
Description	2-2
Syntax	2-2
startwd Command	2-2
Description	2-2
Syntax	2-2
stopall Command	2-3
Description	2-3
Syntax	2-3
stopdb Command	2-3
Description	2-3
Syntax	2-3
stopns Command	2-4
Description	2-4
Syntax	2-4
stopwd Command	2-4
Description	2-4
Syntax	2-4
wdclient Command	2-5
wdclient disk Subcommand	2-5
Description	2-5
Syntax	2-5
wdclient group <group_name> Subcommand	2-6
Description	2-6
Syntax	2-6

wdclient groups Subcommand	2-6
Description	2-6
Syntax	2-6
wdclient health Subcommand	2-7
Description	2-7
Syntax	2-7
wdclient restart Subcommand	2-7
Description	2-7
Syntax	2-7
wdclient start Subcommand	2-7
Description	2-8
Syntax	2-8
wdclient status Subcommand	2-8
Description	2-8
Syntax	2-8
Information Produced: Name Column	2-9
Information Produced: State Column	2-9
Information Produced: Gen Column	2-10
Information Produced: Exec Time Column	2-10
Information Produced: PID Column	2-10
Information Produced: Success Column	2-10
Information Produced: Missed Column	2-10
wdclient stop Subcommand	2-10
Description	2-11
Syntax	2-11
wdclient syshealth Subcommand	2-11
Description	2-11
Syntax	2-11

CHAPTER 3**Service Inventory > Inventory and Connection Manager 3-1**

Service Requests	3-3
Traffic Engineering Management	3-5
Inventory Manager	3-5
Topology Tool	3-5
Introduction	3-6
Launching Topology Tool	3-7
Conventions	3-9
Accessing the Topology Tool for ISC-VPN Topology	3-11
Types of Views	3-13

VPN View	3-15
Logical View	3-19
Physical View	3-22
Viewing Device and Link Properties	3-23
Device Properties	3-24
Link Properties	3-27
Filtering and Searching	3-30
Filtering	3-30
Searching	3-33
Using Maps	3-34
Loading a map	3-35
Layers	3-36
Map data	3-37
Node locations	3-37
Adding new maps	3-38
Devices	3-38
Configuring SSH	3-39
Configuring SSH on Cisco IOS Routers	3-39
Configuring SSH on VPN 3000 Concentrators	3-40
Configuring SSH on PIX Firewall Devices	3-40
Setting Up SNMP	3-41
Setting Up SNMPv1/v2c on Cisco IOS Routers	3-42
Setting SNMPv3 Parameters on Cisco IOS Routers	3-42
Manually Enabling RTR Responder on Cisco IOS Routers	3-43
Accessing the Devices Window	3-44
Creating a Device	3-45
Creating a Catalyst Switch	3-46
Creating a Cisco IOS Device	3-52
Creating a Terminal Server	3-58
Creating a VPN 3000	3-63
Creating a Firewall	3-66
Creating a Cisco CNS IE2100	3-72
Editing a Device	3-73
Deleting Devices	3-75
Editing a Device Configuration	3-76
E-mailing a Device's Owner	3-77
Copying a Device	3-79
Device Groups	3-80
Accessing the Device Groups Window	3-81
Creating a Device Group	3-81

Editing a Device Group	3-84
Deleting Device Groups	3-84
E-mailing a Device Group	3-85
Customers	3-86
Accessing the Customers Window	3-86
Creating a Customer	3-87
Editing a Customer	3-88
Deleting Customers	3-89
Creating Customer Sites	3-90
CPE Devices	3-91
Create CPE Device	3-92
Edit CPE Device	3-93
Deploy CPE Device	3-94
Delete CPE Device	3-95
Providers	3-95
Accessing the Providers Window	3-96
Creating a Provider	3-97
Editing a Provider	3-97
Deleting Providers	3-98
Creating Provider Regions	3-99
Creating PE Devices	3-100
Creating Access Domains	3-101
Resource Pools	3-102
Accessing the Resource Pools Window	3-103
Creating an IP Address Pool	3-104
Creating a Multicast Pool	3-105
Creating a Route Distinguisher and Route Target Pool	3-106
Creating a Site of Origin Pool	3-109
Creating a VC ID Pool	3-111
Creating a VLAN Pool	3-112
Deleting Resource Pools	3-113
CE Routing Communities	3-114
Accessing the CE Routing Communities Window	3-115
Creating CE Routing Communities	3-115
Deleting CE Routing Communities	3-117
VPNs	3-117
Accessing the VPNs Window	3-118
Creating a VPN	3-118
Deleting VPNs	3-120

AAA Servers	3-121
Accessing the AAA Servers Window	3-121
Defining an AAA Server	3-121
Deleting AAA Servers	3-123
Named Physical Circuits	3-123
Accessing the Named Physical Circuits Window	3-124
Creating a Named Physical Circuit	3-125
Deleting Named Physical Circuits	3-128
Creating NPC Rings	3-129
Editing NPC Rings	3-133
Deleting NPC Rings	3-133

CHAPTER 4

Service Inventory > Inventory and Connection Manager > Inventory Manager 4-1

Overview of Inventory Manager	4-1
Prerequisites and Limitations	4-2
Inventory Manager from End to End	4-2
Launching Inventory Manager	4-3
Importing Devices	4-5
Importing Devices from Configuration Files	4-5
Importing Devices with Auto Discovery	4-6
Configuring Device Credentials and SNMP Parameters	4-7
Collecting Configuration Files	4-9
Marking Interfaces for IPsec, Firewall, NAT, or QoS	4-9
Creating a New Customer with Devices	4-10
Creating a New Provider with Devices	4-10
Importing Connections with NPC Auto Discovery	4-11
Importing Services with Service Discovery	4-11
Introducing the Inventory Manager GUI	4-12
Spreadsheet Features	4-13
Understanding the Spreadsheet	4-13
Editing the Spreadsheet	4-14
Provider Spreadsheet	4-15
General	4-15
Passwords	4-16
SNMPv3 Attributes	4-17
PE Attributes	4-18
PE Interfaces	4-19
CNS Attributes	4-21
Platform Information	4-21

Customer Spreadsheet	4-22
General	4-23
Passwords	4-24
SNMPv3 Attributes	4-25
CPE Attributes	4-26
CPE Interfaces	4-26
CNS Attributes	4-28
Platform Information	4-29
Device Group Spreadsheet	4-29
General	4-30
Passwords	4-31
SNMPv3 Attributes	4-32
CNS Attributes	4-33
Platform Information	4-33
Inventory Manager GUI Reference	4-34
Viewer and Task Watcher Tabs	4-35
File Menu	4-35
New	4-35
Open	4-52
Required Attributes	4-62
Save	4-83
Close	4-83
Exit	4-84
Edit Menu	4-84
Insert More Devices	4-84
Remove Selected Devices	4-85
Move to New Customer	4-85
Move to New Provider	4-85
Move to Customer	4-86
Move to Provider	4-86
Edit Selected Devices	4-87
Edit Default Attributes	4-88
Load Default Values to Selected Cells	4-89
Apply Interface Marking Rules to Selection	4-89
Select All	4-89
View Menu	4-90
Fit Columns in Window	4-90
Show Color Coded Column Headers	4-90
Tasks Menu	4-90
Collect Latest Configuration Files	4-90

Start Auto Discovery	4-91
Start NPC Auto Discovery	4-95
Start Service Discovery	4-96
Tools Menu	4-97
File	4-98
Edit	4-104
Help	4-104
Logging Menu	4-104
Help	4-105
About	4-105
Auto Discovery	4-105
Auto Discovery Overview	4-105
Auto Discovery Prerequisites	4-106
Process Flow	4-106
User Interface	4-106
Inventory Manager GUI	4-106
UNIX Command Line Interface (UNIX CLI)	4-107
Service Discovery	4-108
MPLS Service Discovery	4-108
MPLS Service Discovery Overview	4-108
Limitations	4-108
MPLS Service Discovery Process	4-109
Synchronization	4-110
CERC Creation	4-110
User Input After Discovery	4-110
Grey Management Discovery	4-110
Layer 2 VPN Discovery	4-111
Topology	4-111
Logic (MPLS Core)	4-111
Logic (L2TPv3)	4-112
VPLS Service Discovery	4-112
Topology	4-112
Logic	4-113
Restrictions	4-113
Ring Topology Discovery (Connection Discovery)	4-113

CHAPTER 5

Service Inventory > Device Console 5-1

Device Console	5-1
Download Commands	5-2

Download Template	5-3
Device Configuration Manager	5-8
EXEC Commands	5-10
Reload	5-15

CHAPTER 6

Service Design 6-1

Policies	6-2
Templates	6-2
View Templates Tree and Data Pane	6-3
Create Folders and Subfolders	6-4
Copying Folders or Subfolders	6-5
Create Template	6-5
Copying Templates	6-14
Create Data File	6-14
Edit	6-19
Delete	6-21
Template Examples	6-22
Summary of Repository Variables	6-25
Protocols	6-43
Protocols	6-44
Create TCP	6-44
Create UDP	6-45
Create ICMP	6-47
Create IGMP	6-47
Create IP	6-48
Edit	6-48
Delete	6-49
Protocol Bundles	6-49
Create Protocol Bundles	6-50
Edit Protocol Bundles	6-50
Delete Protocol Bundles	6-51
Link QoS	6-51
Create	6-52
Copy	6-56
Edit	6-56
Delete	6-56
Network Objects	6-57
Create Network Objects	6-57

Edit Network Objects	6-59
Delete Network Objects	6-59

CHAPTER 7

Monitoring 7-1

Task Manager	7-1
Tasks	7-2
Starting Task Manager	7-2
Creating a New Task	7-3
Audit	7-5
Task Logs	7-6
Ping	7-8
MPLS	7-9
IPsec	7-11
SLA	7-14
Setup Prior to Using SLA	7-14
Probes	7-15
Create From Any SA Agent Device(s)	7-16
Create from MPLS CPE	7-22
Create from MPLS PE or MVRP-CE	7-29
Create from IPsec CPE	7-36
Protocols	7-41
Details	7-46
Delete	7-47
Enable Probes	7-49
Enable Traps	7-50
Disable Probes	7-51
Disable Traps	7-53
Reports	7-54
Summary Report	7-55
HTTP Report	7-57
Jitter Report	7-58
Summary CoS Report	7-58
HTTP CoS Report	7-59
Jitter CoS Report	7-59
TEM Performance Report	7-59

CHAPTER 8**Administration 8-1**

Security 8-2

Users 8-2

Details 8-4

Create 8-4

Copy 8-7

Edit 8-7

Delete 8-7

User Groups 8-8

Create 8-9

Edit 8-10

Delete 8-10

User Roles 8-11

Create 8-14

Copy 8-17

Edit 8-17

Delete 8-18

Object Groups 8-18

Create 8-20

Edit 8-21

Delete 8-21

User Roles Design Example 8-22

Example 8-22

Illustration of Setup 8-23

Steps to Set Up Example 8-24

Control Center 8-25

Hosts 8-25

Details 8-26

Config 8-27

Servers 8-28

Watchdog 8-29

Install 8-30

Uninstall 8-31

Logs 8-31

Collection Zones 8-32

Licensing 8-34

Active Users 8-37

User Access Log 8-37

Manage TIBCO Rendezvous 8-39

APPENDIX A

Cisco CNS IE2100 Appliances A-1

Creating a Cisco CNS IE2100 Appliance A-1

Creating a Cisco IOS Device Using the Cisco CNS Device Access Protocol A-3

Using Plug-and-Play A-6

APPENDIX B

Property Settings B-1

INDEX



FIGURES

Figure 1-1	Home Window	1-2
Figure 1-2	ISC Shortcuts	1-4
Figure 1-3	New ISC Shortcut	1-4
Figure 1-4	Index of all Choices	1-5
Figure 1-5	Customer Context	1-6
Figure 1-6	Example of Filtering, Rows per Page, and Changing Pages	1-8
Figure 1-7	Example of Auto Refresh	1-8
Figure 1-8	Colors as Identifiers	1-10
Figure 1-9	Devices—Icons	1-11
Figure 1-10	Service Inventory Selections	1-11
Figure 1-11	Inventory and Connection Manager Selections	1-13
Figure 1-12	Service Design Selections	1-14
Figure 1-13	Templates Selections	1-14
Figure 1-14	Protocols Selections	1-15
Figure 1-15	Monitoring Selections	1-15
Figure 1-16	Administration Selections	1-16
Figure 1-17	Security Selections	1-17
Figure 1-18	Control Center Selections	1-17
Figure 3-1	Service Inventory Selections	3-1
Figure 3-2	Inventory and Connection Manager Selections	3-2
Figure 3-3	Service Request States Transition Diagram	3-5
Figure 3-4	Topology Launch	3-7
Figure 3-5	Security Warning	3-8
Figure 3-6	Topology Desktop Integration	3-8
Figure 3-7	Log On to ISC	3-8
Figure 3-8	Topology Application Window	3-12
Figure 3-9	The File Menu	3-13
Figure 3-10	The View Menu	3-14
Figure 3-11	Folder View	3-15
Figure 3-12	Aggregate View	3-16
Figure 3-13	Virtual Circuit with IP Core	3-17

Figure 3-14	Attachment Circuit View	3-18
Figure 3-15	Emulated Circuit View	3-19
Figure 3-16	Logical View	3-20
Figure 3-17	Device Properties	3-20
Figure 3-18	Interface Details Table	3-21
Figure 3-19	Detailed Connection View	3-22
Figure 3-20	Physical View	3-23
Figure 3-21	Device Properties	3-24
Figure 3-22	Logical Device Properties	3-24
Figure 3-23	Physical Device Properties	3-25
Figure 3-24	Device Interface Properties	3-26
Figure 3-25	Service Request Properties	3-27
Figure 3-26	Link Properties	3-27
Figure 3-27	Expand Link	3-28
Figure 3-28	Link Service Request Properties	3-29
Figure 3-29	Link MPLS VPN Properties	3-30
Figure 3-30	Physical View with Dimmed Nodes	3-31
Figure 3-31	Advanced Filter dialog	3-32
Figure 3-32	Find Dialog Box	3-33
Figure 3-33	The Map Menu	3-34
Figure 3-34	Load Map Window	3-35
Figure 3-35	Map Layers	3-36
Figure 3-36	Physical View with a Map of Japan	3-37
Figure 3-37	Devices List Window	3-44
Figure 3-38	Create Options Window	3-45
Figure 3-39	Create Catalyst Device Window	3-46
Figure 3-40	Catalyst Device Properties Window	3-50
Figure 3-41	Create Cisco IOS Device Window	3-53
Figure 3-42	Cisco IOS Device Properties Window	3-56
Figure 3-43	Create Terminal Server Window	3-59
Figure 3-44	Terminal Server Device Properties Window	3-62
Figure 3-45	Create VPN 3000 Device Window	3-64
Figure 3-46	Create PIX Firewall Window	3-67
Figure 3-47	PIX Device Properties Window	3-70
Figure 3-48	Create IE2100 Device Window	3-72

Figure 3-49	Devices List Window	3-73
Figure 3-50	Editing a Device Window	3-74
Figure 3-51	Devices List Window	3-75
Figure 3-52	Confirm Delete Window	3-75
Figure 3-53	Devices List Window	3-76
Figure 3-54	Device Configurations Window	3-77
Figure 3-55	Device Configuration Window	3-77
Figure 3-56	Devices List Window	3-78
Figure 3-57	Send Mail to Device Owners Window	3-79
Figure 3-58	Devices List Window	3-80
Figure 3-59	Device Groups Window	3-81
Figure 3-60	Create Device Group Window	3-82
Figure 3-61	Select Group Members Window	3-83
Figure 3-62	Create Device Group Window	3-83
Figure 3-63	Edit Device Group Window	3-84
Figure 3-64	Confirm Delete Window	3-85
Figure 3-65	Send Mail to Device Owners of Selected Groups Window	3-86
Figure 3-66	Customers Window	3-87
Figure 3-67	Create Customer Window	3-88
Figure 3-68	Edit Customer Window	3-89
Figure 3-69	Confirm Delete Window	3-90
Figure 3-70	Customer Sites Window	3-90
Figure 3-71	CPE Devices Window	3-91
Figure 3-72	Create CPE Device	3-93
Figure 3-73	Edit CPE Device	3-94
Figure 3-74	Service Deployment Task	3-95
Figure 3-75	Providers Window	3-96
Figure 3-76	Create Provider Window	3-97
Figure 3-77	Edit Provider Window	3-98
Figure 3-78	Confirm Delete Window	3-99
Figure 3-79	Provider Regions Window	3-100
Figure 3-80	PE Devices Window	3-101
Figure 3-81	Access Domains Window	3-102
Figure 3-82	Resource Pools Window	3-104
Figure 3-83	Create IP Address Pool Window	3-105

Figure 3-84	Create Multicast Pool Window	3-106
Figure 3-85	Create Route Distinguisher Pool Window	3-107
Figure 3-86	Provider for New Resource Pool Window	3-107
Figure 3-87	Create Route Target Pool Window	3-108
Figure 3-88	Provider for New Resource Pool Window	3-109
Figure 3-89	Create Site of Origin Pool Window	3-110
Figure 3-90	Provider for New Resource Pool Window	3-111
Figure 3-91	Create VC ID Pool Window	3-111
Figure 3-92	Create VLAN Pool Window	3-112
Figure 3-93	Access Domain for new VLAN Pool Window	3-113
Figure 3-94	Confirm Delete Window	3-113
Figure 3-95	CE Routing Communities Window	3-115
Figure 3-96	Create CE Routing Community Window	3-116
Figure 3-97	VPNs Window	3-118
Figure 3-98	Create VPN Window	3-119
Figure 3-99	AAA Servers Window	3-121
Figure 3-100	Create AAA Servers Window	3-122
Figure 3-101	Named Physical Circuits Window	3-124
Figure 3-102	Create a Named Physical Circuit	3-125
Figure 3-103	Select Device	3-126
Figure 3-104	Select Device	3-126
Figure 3-105	Select Outgoing Interface	3-127
Figure 3-106	Select Incoming Interface	3-127
Figure 3-107	Select NPC Ring	3-128
Figure 3-108	NPC Rings	3-129
Figure 3-109	Create Ring	3-129
Figure 3-110	Select Source Device—CPE/PE	3-130
Figure 3-111	Select Source Interface	3-130
Figure 3-112	Select Destination Device—CPE/PE	3-131
Figure 3-113	Select Destination Interface	3-132
Figure 3-114	NPC Rings	3-133
Figure 3-115	NPC Rings	3-134
Figure 3-116	Delete Rings	3-134
Figure 4-1	Inventory Manager	4-3
Figure 4-2	Start Java Web Start	4-4

Figure 4-3	Log On to ISC	4-4
Figure 4-4	Inventory Manager Opening Screen	4-5
Figure 4-5	Inventory Manager GUI	4-12
Figure 4-6	Provider Spreadsheet - General Tab	4-15
Figure 4-7	Provider Spreadsheet - Password Tab	4-16
Figure 4-8	Provider Spreadsheet - SNMPv3 Attributes Tab	4-17
Figure 4-9	Provider Spreadsheet - PE Attributes Tab	4-18
Figure 4-10	Provider Spreadsheet - PE Interfaces Tab	4-19
Figure 4-11	Provider Spreadsheet - CNS Attributes Tab	4-21
Figure 4-12	Provider Spreadsheet - Platform Information Tab	4-22
Figure 4-13	Customer Spreadsheet - General Tab	4-23
Figure 4-14	Customer Spreadsheet - Passwords Tab	4-24
Figure 4-15	Customer Spreadsheet - SNMPv3 Attributes Tab	4-25
Figure 4-16	Customer Spreadsheet - CPE Attributes Tab	4-26
Figure 4-17	Customer Spreadsheet - CPE Interfaces Tab	4-26
Figure 4-18	Customer Spreadsheet - CNS Attributes Tab	4-28
Figure 4-19	Customer Spreadsheet - Platform Information Tab	4-29
Figure 4-20	Device Group Spreadsheet - General Tab	4-30
Figure 4-21	Device Group Spreadsheet - Passwords Tab	4-31
Figure 4-22	Device Group Spreadsheet - SNMPv3 Attributes Tab	4-32
Figure 4-23	Device Group Spreadsheet - CNS Attributes Tab	4-33
Figure 4-24	Device Group Spreadsheet - Platform Information Tab	4-33
Figure 4-25	Inventory Manager	4-34
Figure 4-26	Choose New Device Group	4-36
Figure 4-27	Create New Device Group	4-36
Figure 4-28	Config Files Tab	4-37
Figure 4-29	Open Config Files	4-38
Figure 4-30	Highlighted Config Files	4-38
Figure 4-31	Config Files List	4-39
Figure 4-32	Device Group Spreadsheet	4-39
Figure 4-33	Domain Name	4-40
Figure 4-34	Management Address	4-40
Figure 4-35	Device Type	4-40
Figure 4-36	Device Description	4-41
Figure 4-37	Access Protocol	4-41

Figure 4-38	Config Upload/Download	4-41
Figure 4-39	Login User	4-42
Figure 4-40	Login Password	4-42
Figure 4-41	Enable Password	4-42
Figure 4-42	SNMP Read-Only	4-43
Figure 4-43	SNMP Read-Write	4-43
Figure 4-44	New Provider	4-44
Figure 4-45	Config Files Tab	4-44
Figure 4-46	Highlighted Config Files	4-45
Figure 4-47	Config Files List	4-45
Figure 4-48	New Provider Spreadsheet	4-46
Figure 4-49	New Region for Provider	4-47
Figure 4-50	New Provider Spreadsheet	4-47
Figure 4-51	New Customer	4-48
Figure 4-52	New Customer Spreadsheet	4-49
Figure 4-53	New Site	4-49
Figure 4-54	New Customer Spreadsheet	4-50
Figure 4-55	New Device Spreadsheet	4-50
Figure 4-56	Enter IP Address	4-51
Figure 4-57	Choose New IPsec VPN Service Module	4-51
Figure 4-58	Create New IPsec VPN Service Module	4-52
Figure 4-59	Open Devices	4-53
Figure 4-60	Open Devices Found	4-53
Figure 4-61	Devices Spreadsheet	4-54
Figure 4-62	Open Discovery Seed File	4-54
Figure 4-63	Device Information	4-55
Figure 4-64	Device in the Repository	4-55
Figure 4-65	Device Chooser	4-55
Figure 4-66	Device Information	4-56
Figure 4-67	Open Device Group	4-56
Figure 4-68	Device Spreadsheet Editor	4-57
Figure 4-69	Open Provider	4-57
Figure 4-70	Provider Spreadsheet Editor	4-58
Figure 4-71	Open Provider	4-58
Figure 4-72	Open Region	4-59

Figure 4-73	PE Spreadsheet Editor	4-59
Figure 4-74	Open Customer	4-60
Figure 4-75	CPE Spreadsheet Editor	4-60
Figure 4-76	Open Customer	4-60
Figure 4-77	Open Site	4-61
Figure 4-78	CPE Spreadsheet Editor	4-61
Figure 4-79	Open Device Group	4-63
Figure 4-80	Generic Device - General Attributes	4-63
Figure 4-81	Generic Device - Password Attributes	4-64
Figure 4-82	Generic Device - SNMPv3 Attributes	4-65
Figure 4-83	Generic Device - CNS Attributes	4-66
Figure 4-84	Generic Device - Platform Information Attributes	4-67
Figure 4-85	Open Provider	4-68
Figure 4-86	PE Device - General Attributes	4-69
Figure 4-87	PE Device - Password Attributes	4-70
Figure 4-88	PE Device - SNMPv3 Attributes	4-71
Figure 4-89	PE Device - PE Attributes	4-72
Figure 4-90	PE Device - PE Interfaces	4-73
Figure 4-91	PE Device - CNS Attributes	4-74
Figure 4-92	PE Device - Platform Information	4-75
Figure 4-93	Open Customer	4-76
Figure 4-94	CPE Device - General Attributes	4-77
Figure 4-95	CPE Device - Password Attributes	4-78
Figure 4-96	CPE Device - SNMPv3 Attributes	4-79
Figure 4-97	CPE Device - CPE Attributes	4-80
Figure 4-98	CPE Device - CPE Interfaces	4-81
Figure 4-99	CPE Device - CNS Attributes	4-82
Figure 4-100	CPE Device - Platform Information Attributes	4-83
Figure 4-101	New Device Spreadsheet	4-91
Figure 4-102	Enter IP Address	4-91
Figure 4-103	Start Device Discovery	4-92
Figure 4-104	Discovery Policy	4-92
Figure 4-105	Please Wait	4-93
Figure 4-106	Discovered Devices	4-93
Figure 4-107	Save Connection Information	4-93

Figure 4-108	Save Connection Information Confirmation	4-94
Figure 4-109	Save Device Information	4-94
Figure 4-110	Save Device Information Confirmation	4-95
Figure 4-111	Device Information	4-95
Figure 4-112	Service Discovery	4-96
Figure 4-113	Interface Marking Rule Editor	4-97
Figure 4-114	Interface Rule Editor Task Bar	4-98
Figure 4-115	Interface Rule Editor Dialog Box	4-99
Figure 4-116	Property Drop-Down List	4-99
Figure 4-117	Relationship Drop-Down List	4-100
Figure 4-118	Pos Drop-Down Button	4-100
Figure 4-119	Type Drop-Down List	4-100
Figure 4-120	Then Clause Drop-Down List	4-100
Figure 4-121	IPsec Drop-Down List	4-101
Figure 4-122	NAT Drop-Down List	4-101
Figure 4-123	QoS Drop-Down List	4-101
Figure 4-124	Firewall Drop-Down List	4-102
Figure 4-125	Then Clause Drop-Down List	4-102
Figure 4-126	Additional If Clause Drop-Down List	4-102
Figure 4-127	Example of a Rule	4-103
Figure 4-128	Auto Discovery Process Flow	4-106
Figure 4-129	L2VPN Discovery Topology	4-111
Figure 4-130	MPLS Network	4-113
Figure 4-131	Sample Ring Topology	4-114
Figure 5-1	Service Inventory Selections	5-1
Figure 5-2	Device Console Selections	5-2
Figure 5-3	Device Console—Download Commands: Select Devices	5-3
Figure 5-4	Device Console—Download Template: Select Devices	5-4
Figure 5-5	Device Selection	5-4
Figure 5-6	Device Group Selection	5-5
Figure 5-7	Group Association	5-5
Figure 5-8	Select Download Template	5-6
Figure 5-9	Add/Remove Templates	5-6
Figure 5-10	Download Template Summary	5-7
Figure 5-11	Download Template Results	5-8

Figure 5-12	Device Configuration Manager	5-9
Figure 5-13	Device Selection	5-9
Figure 5-14	Device Console—EXEC Commands: Select Devices	5-11
Figure 5-15	Device Selection	5-12
Figure 5-16	Device Group Selection	5-13
Figure 5-17	Group Association	5-13
Figure 5-18	Operation Commands	5-14
Figure 5-19	EXEC Commands Summary	5-15
Figure 5-20	Device Console—Reload: Select Devices	5-16
Figure 5-21	Device Selection	5-17
Figure 5-22	Device Group Selection	5-18
Figure 5-23	Group Association	5-18
Figure 5-24	Reload Summary	5-19
Figure 6-1	Service Design Selections	6-1
Figure 6-2	Templates	6-3
Figure 6-3	Tree and Data Pane Structure	6-4
Figure 6-4	Folder Naming	6-5
Figure 6-5	Folder with Existing Templates	6-6
Figure 6-6	Template Editor	6-6
Figure 6-7	Example Template	6-7
Figure 6-8	Template Variables	6-8
Figure 6-9	Variable Definition—Type String	6-8
Figure 6-10	Variable Definition—Type Integer	6-10
Figure 6-11	Variable Definition—Type Float	6-11
Figure 6-12	Variable Definition—Type IPv4	6-12
Figure 6-13	Variable Definition—Type Sub-Template	6-13
Figure 6-14	Variable Definition—Type Dynamic Java Class	6-13
Figure 6-15	Variable Definition—Type Dynamic URL	6-14
Figure 6-16	Choose Existing Template > Create Data File	6-15
Figure 6-17	Choose Existing Template > Create Data File	6-15
Figure 6-18	Template Data File Editor	6-16
Figure 6-19	Template Data File Editor	6-17
Figure 6-20	Editing a One-Dimensional Array	6-17
Figure 6-21	Adding a Variable	6-18
Figure 6-22	Editing a Two-Dimensional Array	6-18

Figure 6-23	Enter Row Information	6-18
Figure 6-24	Enter Column Information	6-19
Figure 6-25	Two-Dimensional Array Results	6-19
Figure 6-26	Choose Existing Template > Edit	6-20
Figure 6-27	Choose Existing Data File > Edit	6-20
Figure 6-28	Choose Existing Template > Delete	6-21
Figure 6-29	Choose Existing Data File > Delete	6-21
Figure 6-30	Protocols	6-44
Figure 6-31	Create TCP Protocol	6-45
Figure 6-32	Create UDP Protocol	6-46
Figure 6-33	Create ICMP Protocol	6-47
Figure 6-34	Create IGMP Protocol	6-47
Figure 6-35	Create IP Protocol	6-48
Figure 6-36	Protocols Bundles	6-49
Figure 6-37	Create Protocol Bundles	6-50
Figure 6-38	Link QoS Settings	6-51
Figure 6-39	IP Link Settings Editor	6-52
Figure 6-40	Aggregated Traffic Shaper	6-53
Figure 6-41	Link Efficiency Settings	6-54
Figure 6-42	Interface-based Aggregated Rate Limiter List	6-55
Figure 6-43	Network Objects	6-57
Figure 6-44	Create Network Object	6-58
Figure 7-1	Monitoring Selections	7-1
Figure 7-2	Tasks	7-2
Figure 7-3	Create Tasks	7-3
Figure 7-4	Task Devices	7-4
Figure 7-5	Task Service Requests	7-4
Figure 7-6	Task Schedule Details	7-5
Figure 7-7	Tasks	7-6
Figure 7-8	Task Runtime Actions	7-6
Figure 7-9	Runtime Actions	7-7
Figure 7-10	Task Log	7-7
Figure 7-11	Services	7-8
Figure 7-12	MPLS Parameters	7-9
Figure 7-13	MPLS CE Selection	7-10

Figure 7-14	MPLS Ping Test Results	7-11
Figure 7-15	IPsec Parameters	7-12
Figure 7-16	IPsec CE Selection	7-13
Figure 7-17	IPsec Ping Test Results	7-13
Figure 7-18	SLA Probes	7-15
Figure 7-19	SLA Probes > Create > From Any SA Agent Device(s)	7-16
Figure 7-20	SLA Common Parameters	7-17
Figure 7-21	SLA Source Devices	7-19
Figure 7-22	SLA Devices > Add	7-20
Figure 7-23	SLA Destination Devices	7-21
Figure 7-24	SLA Probes > Create > From MPLS CPE	7-22
Figure 7-25	SLA Common Parameters	7-23
Figure 7-26	SLA CPE Parameters	7-25
Figure 7-27	Select VPN	7-25
Figure 7-28	Select CPE	7-26
Figure 7-29	Interfaces	7-26
Figure 7-30	Connected PE Interface	7-27
Figure 7-31	CPEs	7-28
Figure 7-32	Select CPE Associated with the Specified VPN	7-28
Figure 7-33	SLA Probes > Create > From MPLS PE or MVRP-CE	7-29
Figure 7-34	SLA Common Parameters	7-30
Figure 7-35	SLA CPE Parameters	7-32
Figure 7-36	Select VPN	7-32
Figure 7-37	Select PE	7-33
Figure 7-38	Select Device Interface	7-33
Figure 7-39	Connected PE Interface	7-34
Figure 7-40	PEs	7-35
Figure 7-41	Select PE Associated with the Specified VPN	7-35
Figure 7-42	SLA Probes > Create > From IPsec CPE	7-36
Figure 7-43	SLA Common Parameters	7-37
Figure 7-44	SLA CPE Parameters	7-39
Figure 7-45	Select VPN	7-39
Figure 7-46	Select CPE	7-40
Figure 7-47	Select CPE Associated with the Specified VPN	7-40
Figure 7-48	Protocols	7-41

Figure 7-49	Protocol ICMP Echo	7-42
Figure 7-50	Protocol TCP Connect	7-42
Figure 7-51	Protocol UDP Echo	7-43
Figure 7-52	Protocol Jitter	7-43
Figure 7-53	Protocol FTP	7-44
Figure 7-54	Protocol DNS	7-44
Figure 7-55	Protocol HTTP	7-45
Figure 7-56	SLA Probes > Details	7-46
Figure 7-57	SLA Probes Details	7-47
Figure 7-58	SLA Probes > Delete	7-48
Figure 7-59	Confirm Delete Probes	7-48
Figure 7-60	SLA Probes > Enable > Probes	7-49
Figure 7-61	Confirm Enable Probes	7-49
Figure 7-62	SLA Probes > Enable > Traps	7-50
Figure 7-63	Confirm Enable Traps	7-51
Figure 7-64	SLA Probes > Disable > Probes	7-52
Figure 7-65	Confirm Disable Probes	7-52
Figure 7-66	SLA Probes > Disable > Traps	7-53
Figure 7-67	Confirm Disable Traps	7-53
Figure 7-68	SLA Reports	7-54
Figure 7-69	Parameters of Summary Report	7-55
Figure 7-70	Parameters of CoS Summary Report	7-58
Figure 8-1	Administration Selections	8-1
Figure 8-2	Security Window	8-2
Figure 8-3	Users Window	8-3
Figure 8-4	Create/Edit Users Window	8-5
Figure 8-5	Users Confirm Delete	8-8
Figure 8-6	User Groups Window	8-8
Figure 8-7	Create/Edit User Groups Window	8-9
Figure 8-8	User Groups Confirm Delete	8-11
Figure 8-9	User Roles Window	8-13
Figure 8-10	Create/Edit User Roles Window (Top)	8-14
Figure 8-11	Create/Edit User Roles Window (Bottom)	8-15
Figure 8-12	User Roles Confirm Delete	8-18
Figure 8-13	Object Groups Window	8-19

Figure 8-14	Create/Edit Object Group Window	8-20
Figure 8-15	Delete Object Groups Confirm Delete	8-22
Figure 8-16	Contents in Example	8-23
Figure 8-17	Control Center > Hosts	8-25
Figure 8-18	Host Details	8-26
Figure 8-19	Properties	8-27
Figure 8-20	Properties Detail Example	8-28
Figure 8-21	Servers	8-29
Figure 8-22	WatchDog Logs	8-29
Figure 8-23	Remote Install	8-30
Figure 8-24	Remote Uninstall	8-31
Figure 8-25	Choose Control Center > Collection Zones	8-32
Figure 8-26	Collection Zones	8-32
Figure 8-27	Create Collection Zone	8-33
Figure 8-28	Collection Zone Devices	8-34
Figure 8-29	Choose Control Center > Licensing	8-35
Figure 8-30	Install Button	8-36
Figure 8-31	Enter License Key	8-36
Figure 8-32	Active Users	8-37
Figure 8-33	User Access Log Viewer with Simple Filter	8-38
Figure 8-34	User Access Log Viewer with Advanced Filter	8-38
Figure 8-35	TIBCO Rendezvous	8-40
Figure 8-36	Connection Configuration	8-40
Figure A-1	Devices Window	A-2
Figure A-2	Create IE2100 Device Window	A-2
Figure A-3	Create Cisco IOS Device Window	A-4
Figure A-4	Cisco IOS Device Additional Properties	A-5



TABLES

<i>Table 2-1</i>	Servers and Their Functions	2-9
<i>Table 2-2</i>	Valid States	2-9
<i>Table 3-1</i>	Summary of Cisco IP Solution Center Service Request States	3-3
<i>Table 3-2</i>	Device Role Shapes	3-9
<i>Table 3-3</i>	Link Type Color Scheme	3-11
<i>Table 3-4</i>	Link State Pattern Scheme	3-11
<i>Table 3-5</i>	SNMP Security Models and Levels	3-41
<i>Table 3-6</i>	Create Catalyst Device Interfaces Fields	3-47
<i>Table 3-7</i>	Create Cisco IOS Device Interface Fields	3-54
<i>Table 3-8</i>	Create Terminal Server Device Interfaces Fields	3-60
<i>Table 3-9</i>	Create VPN 3000 Device Interfaces Fields	3-65
<i>Table 3-10</i>	Create PIX Firewall Device Interfaces Fields	3-68
<i>Table 6-1</i>	Template Examples and Their Descriptions	6-22
<i>Table 6-2</i>	IPsec Remote Access Repository Variables - NOT SUPPORTED in this release. -	6-26
<i>Table 6-3</i>	IPsec Site-to-Site Repository Variables - NOT SUPPORTED in this release. -	6-26
<i>Table 6-4</i>	L2VPN Repository Variables	6-29
<i>Table 6-5</i>	MPLS Repository Variables	6-32
<i>Table 6-6</i>	NAT Repository Variables - NOT SUPPORTED in this release. -	6-39
<i>Table 6-7</i>	QoS Repository Variables	6-40
<i>Table 6-8</i>	VPLS Repository Variables	6-41
<i>Table 7-1</i>	Meanings of Precedence Values	7-18
<i>Table 7-2</i>	Meanings of Precedence Values	7-24
<i>Table 7-3</i>	Meanings of Precedence Values	7-31
<i>Table 7-4</i>	Meanings of Precedence Values	7-38
<i>Table B-1</i>	DCPL Properties	B-1



About This Guide

This preface defines the following:

- [Objective, page xxxi](#)
- [Related Documentation, page xxxi](#)
- [Audience, page xxxii](#)
- [How This Book Is Organized, page xxxii](#)
- [Document Conventions, page xxxiii](#)
- [Obtaining Documentation, page xxxiv](#)
- [Documentation Feedback, page xxxiv](#)
- [Obtaining Technical Assistance, page xxxv](#)
- [Obtaining Additional Publications and Information, page xxxvi](#)

Objective

This manual provides details about the WatchDog commands and the Full Menus Graphical User Interface (GUI) for the Cisco IP Solution Center (ISC) product. Detailed explanations are given for common components across all applications.

Related Documentation

The entire documentation set for Cisco IP Solution Center, 4.0 can be accessed at:

http://www.cisco.com/univercd/cc/td/doc/product/rtrmgmt/isc/4_0

The following documents comprise the ISC 4.0 documentation set.

General documentation (in suggested reading order):

- *Cisco IP Solution Center Documentation Guide, 4.0*
- *Cisco IP Solution Center Release Notes, 4.0*
- *Cisco IP Solution Center Installation Guide, 4.0*
- *Cisco IP Solution Center Infrastructure Reference, 4.0*
- *Cisco IP Solution Center System Error Messages, 4.0*

Application and technology documentation (listed alphabetically):

- [Cisco IP Solution Center L2VPN User Guide, 4.0](#)
- [Cisco IP Solution Center MPLS VPN User Guide, 4.0](#)
- [Cisco IP Solution Center Quality of Service User Guide, 4.0](#)
- [Cisco IP Solution Center Traffic Engineering Management User Guide, 4.0](#)

API documentation:

- [Cisco IP Solution Center API Programmer Guide, 4.0](#)
- Index: [Cisco IP Solution Center API Programmer Reference, 4.0](#)



Note

All documentation *might* be upgraded.

Audience

This manual is written as a resource for experienced users and administrators who use ISC. It provides details about how to implement the infrastructure functionality of ISC that is common to all applications.

It is assumed that you have a basic understanding of network design, operation, and terminology, and that you are familiar with your own network configurations.

How This Book Is Organized

This manual is organized as follows:

- [Chapter 1, “Getting Started,”](#) provides a reference to the system recommendations, provides an overview of the ISC product, provides an overview of the Full Menus GUI structure, and explains the common GUI components.
- [Chapter 2, “WatchDog Commands,”](#) provides the description, syntax, and arguments for the commands for WatchDog, a background daemon process that is automatically installed as part of the installation procedure for ISC.
- [Chapter 3, “Service Inventory > Inventory and Connection Manager,”](#) explains the navigation path from the **Service Inventory** tab to **Inventory and Connection Manager** and how to use the topics found there, except Inventory Manager, which is explained in Chapter 4.
- [Chapter 4, “Service Inventory > Inventory and Connection Manager > Inventory Manager,”](#) explains the navigation path from the **Service Inventory** tab to **Inventory and Connection Manager** and then to **Inventory Manager** and how to use the Inventory Manager.
- [Chapter 5, “Service Inventory > Device Console,”](#) explains the navigation path from the **Service Inventory** tab to **Device Console** and how to use the topics found there.
- [Chapter 6, “Service Design,”](#) explains the **Service Design** tab and how to use the topics found there.
- [Chapter 7, “Monitoring,”](#) explains the **Monitoring** tab and how to use the topics found there.
- [Chapter 8, “Administration,”](#) explains the **Administration** tab and how to use the topics found there.
- [Appendix A, “Cisco CNS IE2100 Appliances,”](#) explains how to use the Cisco CNS IE2100 functionality on ISC.

- [Appendix B, “Property Settings,”](#) explains the Dynamic Component Properties Library (DCPL) properties, their defaults, and ranges and rules.
- [Glossary](#) explains terminology used in the ISC product.

Document Conventions

This section discusses conventions and terminology used throughout this manual.

- *pointer*—indicates where the mouse action is to occur
- *select*—to push and hold down the left mouse button
- *release*—to let up on a mouse button to initiate an action
- *click*—to select and release a mouse button without moving the pointer
- *double-click*—to click a mouse button twice quickly without moving the pointer
- *drag*—to move the pointer by sliding the mouse with one or more buttons selected

This manual uses this terminology throughout (even though it is possible for individual users to customize their devices to use the buttons in an alternative manner).

In situations that allow more than one item to be selected from a list simultaneously, the following actions are supported:

- To select a single item in a list, click the entry. Clicking a second time on a previously selected entry deselects it.
- To select a contiguous block of items, click the first entry; then, without releasing the mouse button, drag to the last desired entry and release. (A subsequent click anywhere on the window deselects all previous selections.)
- To extend a currently selected block, hold the **Shift** key down and click the entry at the end of the group to be added
- To add a noncontiguous entry to the selection group, press the **Ctrl** (Control) key and click the entry to be added.

Names of on-window elements that you click or select (menu names, commands, and controls such as buttons, drop-down lists, and so on) are printed in **bold** font.

Bold font is also used for keywords, names of commands, and names of keys on the keyboard.

Text displayed as on-window examples is printed in *courier* font.

When set off from the main text, words and characters you should enter by the keyboard are printed in **bold** font. When the word or character string is enclosed in angle brackets (< and >), you should substitute your own character string for the example presented in the text.

For example, when you see:

login: **root**

you should specify the string **root** at the **login** prompt. However, when you see:

password: <*rootpassword*>

you should specify your own password in place of the character string <*rootpassword*>.

The *italic style* is used to emphasize words, to introduce new terms, and for titles of printed publications (however, not titles of CD-ROMs or floppy disks).

**Note**

Means *reader take note*. Notes contain helpful suggestions or references to materials not contained in this manual.

**Caution**

Means *reader be careful*. In this situation, you might do something that could result in equipment damage or loss of data.

Obtaining Documentation

Cisco documentation and additional literature are available on Cisco.com. Cisco also provides several ways to obtain technical assistance and other technical resources. These sections explain how to obtain technical information from Cisco Systems.

Cisco.com

You can access the most current Cisco documentation at this URL:

<http://www.cisco.com/univercd/home/home.htm>

You can access the Cisco website at this URL:

<http://www.cisco.com>

You can access international Cisco websites at this URL:

http://www.cisco.com/public/countries_languages.shtml

Ordering Documentation

You can find instructions for ordering documentation at this URL:

http://www.cisco.com/univercd/cc/td/doc/es_inpk/pdi.htm

You can order Cisco documentation in these ways:

- Registered Cisco.com users (Cisco direct customers) can order Cisco product documentation from the Ordering tool:
<http://www.cisco.com/en/US/partner/ordering/index.shtml>
- Nonregistered Cisco.com users can order documentation through a local account representative by calling Cisco Systems Corporate Headquarters (California, USA) at 408 526-7208 or, elsewhere in North America, by calling 1 800 553-NETS (6387).

Documentation Feedback

You can send comments about technical documentation to bug-doc@cisco.com.

You can submit comments by using the response card (if present) behind the front cover of your document or by writing to the following address:

Cisco Systems
Attn: Customer Document Ordering
170 West Tasman Drive
San Jose, CA 95134-9883

We appreciate your comments.

Obtaining Technical Assistance

For all customers, partners, resellers, and distributors who hold valid Cisco service contracts, Cisco Technical Support provides 24-hour-a-day, award-winning technical assistance. The Cisco Technical Support Website on Cisco.com features extensive online support resources. In addition, Cisco Technical Assistance Center (TAC) engineers provide telephone support. If you do not hold a valid Cisco service contract, contact your reseller.

Cisco Technical Support Website

The Cisco Technical Support Website provides online documents and tools for troubleshooting and resolving technical issues with Cisco products and technologies. The website is available 24 hours a day, 365 days a year, at this URL:

<http://www.cisco.com/techsupport>

Access to all tools on the Cisco Technical Support Website requires a Cisco.com user ID and password. If you have a valid service contract but do not have a user ID or password, you can register at this URL:

<http://tools.cisco.com/RPF/register/register.do>



Note

Use the Cisco Product Identification (CPI) tool to locate your product serial number before submitting a web or phone request for service. You can access the CPI tool from the Cisco Technical Support Website by clicking the **Tools & Resources** link under Documentation & Tools. Choose **Cisco Product Identification Tool** from the Alphabetical Index drop-down list, or click the **Cisco Product Identification Tool** link under Alerts & RMAs. The CPI tool offers three search options: by product ID or model name; by tree view; or for certain products, by copying and pasting **show** command output. Search results show an illustration of your product with the serial number label location highlighted. Locate the serial number label on your product and record the information before placing a service call.

Submitting a Service Request

Using the online TAC Service Request Tool is the fastest way to open S3 and S4 service requests. (S3 and S4 service requests are those in which your network is minimally impaired or for which you require product information.) After you describe your situation, the TAC Service Request Tool provides recommended solutions. If your issue is not resolved using the recommended resources, your service request is assigned to a Cisco TAC engineer. The TAC Service Request Tool is located at this URL:

<http://www.cisco.com/techsupport/servicerequest>

For S1 or S2 service requests or if you do not have Internet access, contact the Cisco TAC by telephone. (S1 or S2 service requests are those in which your production network is down or severely degraded.) Cisco TAC engineers are assigned immediately to S1 and S2 service requests to help keep your business operations running smoothly.

To open a service request by telephone, use one of the following numbers:

Asia-Pacific: +61 2 8446 7411 (Australia: 1 800 805 227)

EMEA: +32 2 704 55 55

USA: 1 800 553-2447

For a complete list of Cisco TAC contacts, go to this URL:

<http://www.cisco.com/techsupport/contacts>

Definitions of Service Request Severity

To ensure that all service requests are reported in a standard format, Cisco has established severity definitions.

Severity 1 (S1)—Your network is “down,” or there is a critical impact to your business operations. You and Cisco will commit all necessary resources around the clock to resolve the situation.

Severity 2 (S2)—Operation of an existing network is severely degraded, or significant aspects of your business operation are negatively affected by inadequate performance of Cisco products. You and Cisco will commit full-time resources during normal business hours to resolve the situation.

Severity 3 (S3)—Operational performance of your network is impaired, but most business operations remain functional. You and Cisco will commit resources during normal business hours to restore service to satisfactory levels.

Severity 4 (S4)—You require information or assistance with Cisco product capabilities, installation, or configuration. There is little or no effect on your business operations.

Obtaining Additional Publications and Information

Information about Cisco products, technologies, and network solutions is available from various online and printed sources.

- Cisco Marketplace provides a variety of Cisco books, reference guides, and logo merchandise. Visit Cisco Marketplace, the company store, at this URL:

<http://www.cisco.com/go/marketplace/>

- The Cisco *Product Catalog* describes the networking products offered by Cisco Systems, as well as ordering and customer support services. Access the Cisco Product Catalog at this URL:

<http://cisco.com/univercd/cc/td/doc/pcat/>

- *Cisco Press* publishes a wide range of general networking, training and certification titles. Both new and experienced users will benefit from these publications. For current Cisco Press titles and other information, go to Cisco Press at this URL:

<http://www.ciscopress.com>

- *Packet* magazine is the Cisco Systems technical user magazine for maximizing Internet and networking investments. Each quarter, Packet delivers coverage of the latest industry trends, technology breakthroughs, and Cisco products and solutions, as well as network deployment and troubleshooting tips, configuration examples, customer case studies, certification and training information, and links to scores of in-depth online resources. You can access Packet magazine at this URL:

<http://www.cisco.com/packet>

- *iQ Magazine* is the quarterly publication from Cisco Systems designed to help growing companies learn how they can use technology to increase revenue, streamline their business, and expand services. The publication identifies the challenges facing these companies and the technologies to help solve them, using real-world case studies and business strategies to help readers make sound technology investment decisions. You can access iQ Magazine at this URL:

<http://www.cisco.com/go/iqmagazine>

- *Internet Protocol Journal* is a quarterly journal published by Cisco Systems for engineering professionals involved in designing, developing, and operating public and private internets and intranets. You can access the Internet Protocol Journal at this URL:

<http://www.cisco.com/ipj>

- World-class networking training is available from Cisco. You can view current offerings at this URL:

<http://www.cisco.com/en/US/learning/index.html>



Getting Started

This chapter provides information about how to get started to use Cisco IP Solution Center (ISC) and gives a structural overview of this manual. The information is in the following categories:

- [System Recommendations, page 1-1](#)
- [Introduction, page 1-1](#)
- [Structural Overview, page 1-2](#)
- [Service Inventory, page 1-11](#)
- [Service Design, page 1-13](#)
- [Monitoring, page 1-15](#)
- [Administration, page 1-16](#)

System Recommendations

The system recommendations and requirements are listed in Chapter 1, “System Recommendations” of *Cisco IP Solution Center Installation Guide, 4.0*. The recommendation is to thoroughly review this list before even planning your installation, to be sure that you have all the hardware and software you must successfully install.



Caution

There is no identified and supported way to upgrade from ISC 3.0 to ISC 4.0. To upgrade from ISC 3.0 to ISC 4.0, you *must* contact ISC Marketing, e-mail: isc-mktg@cisco.com.

Introduction

Cisco IP Solution Center, 4.0 (ISC 4.0) is a follow-on release to Cisco IP Solution Center, 3.2 (ISC 3.2), with the exceptions listed in *Cisco IP Solution Center Release Notes, 4.0*.

This manual lists many features that are common among all the applications, which are sold and licensed separately. The applications and their respective *User Guides* reference this document for setup steps necessary before creating a policy and then a service request specific to the application.

The Full Menus Graphical User Interface (GUI), is separated into the following large sections (tabs):

- Service Inventory
- Service Design

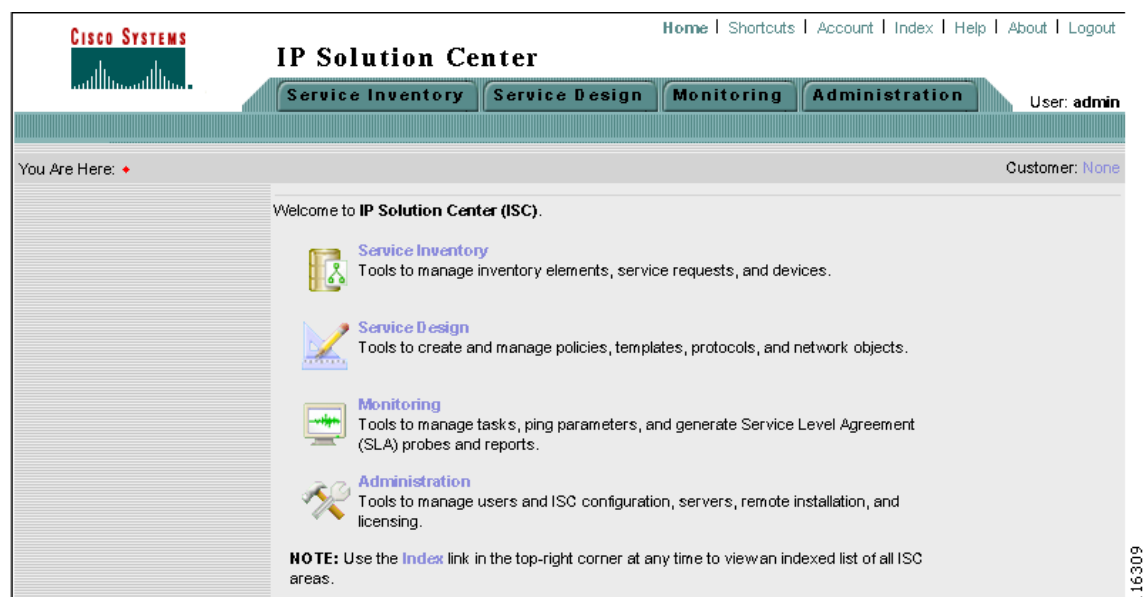
- Monitoring
- Administration

The remaining sections in this chapter explain the sections and subsections of this manual that explain the functionality available from these tabs.

Structural Overview

After you log into Cisco IP Solution Center (ISC), the first window to appear is the Home window, as shown in [Figure 1-1](#), “Home Window.”

Figure 1-1 Home Window



Note

The tabs and the choices navigating within the tabs that appear depend on the user permission, explained in [Chapter 8, “Administration”](#) (**Administration > Security > User Roles**). The choices shown in this manual are for all permissions (**admin**).

This overview includes the following sections:

- [Product Category Tabs, page 1-3](#)
- [Links, page 1-3](#)
- [Common GUI Components, page 1-6](#)

Product Category Tabs

The organization of this manual is based on the tabs shown in [Figure 1-1](#), “Home Window.” Click either the specific tab or the name in the data pane:

- **Service Inventory** An overview is given in the “Service Inventory” section on page 1-11 and detailed information is given in [Chapter 3](#), “Service Inventory > Inventory and Connection Manager,” [Chapter 4](#), “Service Inventory > Inventory and Connection Manager > Inventory Manager,” and [Chapter 5](#), “Service Inventory > Device Console.”
- **Service Design** An overview is given in the “Service Design” section on page 1-13 and detailed information is given in [Chapter 6](#), “Service Design.”
- **Monitoring** An overview is given in the “Monitoring” section on page 1-15 and detailed information is given in [Chapter 7](#), “Monitoring.”
- **Administration** An overview is given in the “Administration” section on page 1-16 and detailed information is given in [Chapter 8](#), “Administration.”

Links

In the upper right-hand corner of the Home window ([Figure 1-1](#)), additional links appear that function as follows:

- [Home](#), page 1-3
- [Shortcuts](#), page 1-3
- [Account](#), page 1-5
- [Index](#), page 1-5
- [Help](#), page 1-5
- [About](#), page 1-5
- [Logout](#), page 1-6

On the far right of the **You are Here:** line on the Home window ([Figure 1-1](#)), is the name of a Customer Context, which is explained in the “Customer” section on page 1-6.

Home

When you click **Home**, you always return to the first window to appear, as shown in [Figure 1-1](#), “Home Window.”

Shortcuts

When you click **Shortcuts**, you can define shortcuts to help quickly navigate to day to day operations. In addition, by grouping these shortcuts together into folders, you can create work flows specific to your operating environment. Shortcuts are further explained in the following steps:

-
- Step 1** After you click **Shortcuts**, you receive a window as shown in [Figure 1-2](#), “ISC Shortcuts.”

Figure 1-2 *ISC Shortcuts*

Showing 1 - 5 of 5 records

#	☐	Folder Name	Shortcut Name	Description
1.	☐		test1	
2.	☐		test2	
3.	☐		test3	
4.	☒	testfolder1	testf1	
5.	☐	testfolder1	test4	

Rows per page: All Go to page: 1 of 1 Go

Go Create Edit Delete Close

- Step 2** To create a shortcut, click the **Create** button in [Figure 1-2](#) and you receive a window as shown in [Figure 1-3](#), “New ISC Shortcut.”

Figure 1-3 *New ISC Shortcut*

Name :

URL :

Type or paste the desired URL into the field above. If the URL is external to ISC, it must begin with "http://". Or, select an internal URL from the list below and click "Set":

Choose...

Description:

Folder:

Folder Shortcut Ordering:

- test1
- test2
- test3

Save Cancel

- Step 3** Fill in the required **Name** and **URL** (you can type in the URL, in which case if it is external to ISC, you must start the URL name with **http://**, or you can click the drop-down button and choose a path internal to ISC and then click the **Set** button) and optionally the **Description**, **Folder**, and **Folder Shortcut Ordering**. Then click **Save**.
- Step 4** You return to [Figure 1-2](#) and can repeat [Step 2](#) and [Step 3](#) to **Create** more shortcuts or you can select a shortcut to proceed to **Go**, select a shortcut to **Edit**, select one or more shortcuts to **Delete**, or select **Close**.

- Step 5** Any time you want to go directly to a URL, you can click **Shortcuts** on the **Home** page and from [Figure 1-2](#) select the shortcut of your choice and click **Go**.

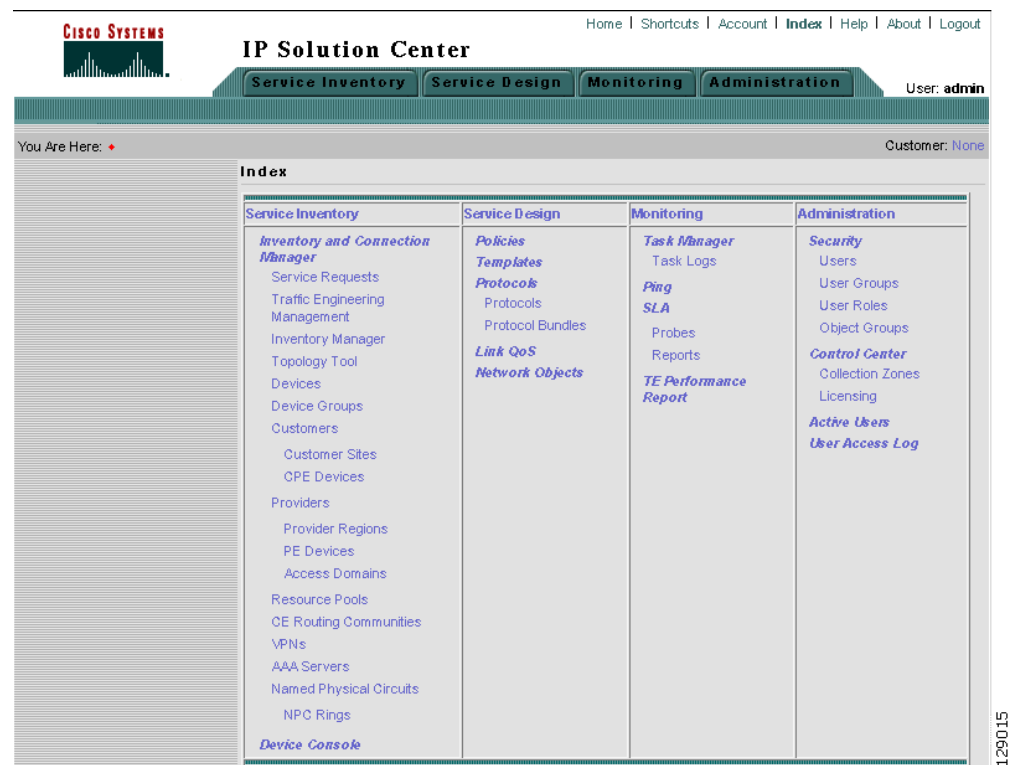
Account

When you click **Account**, you can change your password without the SysAdmin or UserAdmin privileges. This allows you to edit the user profile, including changing the password.

Index

When you click **Index**, you receive an overall picture of all choices from which you can click and jump to, as shown in [Figure 1-4](#), “Index of all Choices.”

Figure 1-4 Index of all Choices



Help

When you click **Help**, you receive a pointer to the documentation set once it is on CCO.

About

When you click **About**, you receive the product name and version.

Logout

When you click **Logout**, you log out of the product.

Customer

On the far right of the **You are Here** line of the Home page is **Customer:** followed by **None** (default) or a customer name. This is referred to as Customer Context. The advantage of Customer Context is to focus only on information for a specified customer. Set the Customer Context, as follows:

- Step 1** Click on the name after **Customer:** on the far right of the line that starts with **You are Here**. The default is **None**. The window shown in [Figure 1-5](#), “Customer Context,” appears.

Figure 1-5 Customer Context

- Step 2** Click the **Select** button and you receive a list of all the currently created customers.
- Step 3** Select the customer for which you want information and click **Save**.
- Step 4** [Figure 1-5](#), “Customer Context,” reappears with the name of the selected customer. Click **Save** or highlight the customer name and click **Clear** to reset the customer for which you want information.
- Step 5** The customer you chose now appears after **Customer:** on the Home window and it is the only customer for which information appears.
- Step 6** You can reset the Customer Context by clearing and reselecting.

Common GUI Components

GUI components that are common on many windows are as follows:

- [Filters](#), page 1-7
- [Rows per Page](#), page 1-7
- [Go To Page](#), page 1-7
- [Auto Refresh](#), page 1-8
- [Color Coding](#), page 1-8
- [Icons](#), page 1-10

Filters

At the top of many windows you can filter information that appears in the window. As shown in [Figure 1-6, “Example of Filtering, Rows per Page, and Changing Pages,”](#) you can click the drop-down menu for categories, then in the **matching** field enter the search criteria, using * if you wish to indicate anything will be a match (you can enter only * or you can place * before other characters, in the middle of other characters, at the end of other characters, or in multiple locations), and click **Find**. In some cases you might also have a field after the **matching** field from which you can select or enter more specifics for your **Find**.

Rows per Page

In the bottom left corner of many windows, as shown in [Figure 1-6, “Example of Filtering, Rows per Page, and Changing Pages,”](#) you can change the number of rows shown on this window in **Rows per page**. Click the drop-down menu and you can select **5**, **10**, **20**, **30**, **40**, or **All**.



Note

When you navigate **Service Inventory > Inventory and Connection Manager > Service Requests**, if the number of service requests stored in the repository exceeds 3000, then for the **Rows per page** drop-down, do *not* choose **All**.

Go To Page

In the bottom right corner of many windows, as shown in [Figure 1-6, “Example of Filtering, Rows per Page, and Changing Pages,”](#) there is **Go to page field of y**. In the *field*, you can enter the page to which you want to navigate and then click the **Go** button to get there. The *y* indicates the last page for this topic. Another way to navigate to a specific page is to use the arrows. You can click the > arrow to navigate to the next page or the furthest arrow to the right >| to navigate to the last page. You can click the < arrow to navigate to the previous page or the furthest arrow to the left |< to navigate to the first page.

Figure 1-6 Example of Filtering, Rows per Page, and Changing Pages

Devices

ShowDevices with matching

Showing 1-10 of 30 records

#	☐	Device Name	Management IP Address	Type
1.	☐	abc		IE2100
2.	☐	ipsec-cpe-london-test.cisco.com	172.29.151.10	Cisco IOS Device
3.	☐	ipsec-cpe-paris-test.cisco.com	172.29.151.11	Cisco IOS Device
4.	☐	ence11	192.168.115.70	Cisco IOS Device
5.	☐	ence132	192.168.115.116	Cisco IOS Device
6.	☐	ence21	192.168.115.73	Cisco IOS Device
7.	☐	ence51	192.168.115.81	Cisco IOS Device
8.	☐	ence61	192.168.115.87	Cisco IOS Device
9.	☐	ipsec-cpe-london	66.66.66.66	Cisco IOS Device
10.	☐	ipsec-cpe-ny	55.55.55.55	Cisco IOS Device

Rows per page:

Auto Refresh

At the bottom left corner of several windows, there is a check box used to enable or disable the **Auto Refresh** feature, as shown in [Figure 1-7, “Example of Auto Refresh.”](#) Checking this box causes the screen and its data to refresh every **n** milliseconds. The amount of time between refresh cycles can be set in the DCPL property: GUI.srRefreshRate. By default, the **Auto Refresh** feature is enabled to 30000 milliseconds.

Figure 1-7 Example of Auto Refresh

Services

ShowServices with Matching of Type

Showing 1 - 1 of 1 record

#	☐	Job ID	State	Type	Operation Type	Creator	Customer Name	Policy Name	Last Modified	Description
1.	☐	1	FAILED_DEPLOY	IPsec	MODIFY	admin	Cisco	Gold	1/28/04 2:08 PM	

Rows per page:

Auto Refresh: ☒

Color Coding

In the Service Request table, the Task table, and the Device table, the colors you see indicate the state of the items, as shown in [Figure 1-8, “Colors as Identifiers.”](#)

In the **Service Request** table, the states have the following colors:

- BROKEN is bright yellow
- CLOSED is no color
- DEPLOYED is bright green
- FAILED AUDIT is bright yellow
- FAILED DEPLOY is bright red
- FUNCTIONAL is bright green
- INVALID is bright red
- LOST is bright yellow
- PENDING is bright green
- REQUESTED is cream
- WAIT DEPLOYED is cream

In the **Task** table, the states have the following colors:

- ABORTED is orange
- RUNNING is bright green
- WAITING_TO_RUN is cream
- errors is bright red
- successfully is bright green
- warnings is cyan

In the **devices** table, the states have the following colors:

- device returns anything else is bright red
- device returns success is bright green
- no result from device is dark blue

Figure 1-8 Colors as Identifiers

Service Requests

Show Services with Job ID Matching * of Type All Find

Showing 1 - 12 of 12 records

#	Job ID	State	Type	Operation Type	Creator	Customer Name	Policy Name	Last Modified	Description
1.	1	REQUESTED	QoS	ADD	user-qos	Customer1	Customer1_QoS_Policy	1/12/04 11:42 AM	
2.	2	REQUESTED	MPLS	MODIFY	user-mpls	Customer1	Customer1_MPLS_Po...	1/12/04 12:00 PM	
3.	3	FAILED_DEPLOY	MPLS	ADD	user-mpls	Customer3	CE-PE	2/13/04 4:12 PM	CE PE
4.	4	INVALID	MPLS	ADD	user-mpls	Customer3	no_ce	1/12/04 1:40 PM	No CE
5.	6	REQUESTED	L2VPN	ADD	user-l2vpn	Customer1	Customer1_L2VPN_P...	1/12/04 12:09 PM	
6.	7	FAILED_DEPLOY	Firewall	ADD	user-firewall	Customer1	Gold_fw_policy	2/19/04 11:58 AM	
7.	8	REQUESTED	IPsec	ADD	user-ipsec	Customer2	Gold	1/12/04 1:27 PM	
8.	9	REQUESTED	IPsec	ADD	user-ipsec	Customer2	Group1	1/12/04 1:31 PM	
9.	10	REQUESTED	NAT	ADD	user-nat	Customer1		1/12/04 1:35 PM	
10.	11	FAILED_DEPLOY	MPLS	ADD	admin	Customer1	MPLSforTwo-Box	2/19/04 11:58 AM	
11.	12	REQUESTED	IPsec	MODIFY	admin	Customer1	Group2	2/20/04 4:15 PM	
12.	14	REQUESTED	NAT	MODIFY	admin	Customer1		2/25/04 11:36 PM	

Rows per page: All Go to page: 1 of 1 Go

Auto Refresh: ☒ Create Details Edit Deploy Decommission Purge

116236

Icons

In some windows with tables of information, icons appear to show the type of device, as shown in Figure 1-9, “Devices—Icons.”



Note

A list of possible icons can be found in Table 3-2 in the Topology Tool section of Chapter 3, “Service Inventory > Inventory and Connection Manager.”

Figure 1-9 Devices—Icons

Devices

ShowDevices with Matching

Showing 1 - 54 of 54 records

#	☐	Device Name	Management IP Address	Type	Parent Device Name
1.	☐	 ipsec-cpe-london-test.cisco.com	172.29.151.10	Cisco IOS Device	
2.	☐	 ipsec-cpe-paris-test.cisco.com	172.29.151.11	Cisco IOS Device	
3.	☐	 ence11	192.168.115.70	Cisco IOS Device	
4.	☐	 ence132	192.168.115.116	Cisco IOS Device	
5.	☐	 ence21	192.168.115.73	Cisco IOS Device	
6.	☐	 ence51	192.168.115.81	Cisco IOS Device	
7.	☐	 ence61	192.168.115.87	Cisco IOS Device	
8.	☐	 ipsec-cpe-london	66.66.66.66	Cisco IOS Device	
9.	☐	 ipsec-cpe-ny	55.55.55.55	Cisco IOS Device	
10.	☐	 barnes.cisco.com	10.128.32.1	Cisco IOS Device	
11.	☐	 carson.cisco.com	10.128.32.254	Cisco IOS Device	
12.	☐	 enpe1	192.168.115.64	Cisco IOS Device	
13.	☐	 enpe12	192.168.115.55	Cisco IOS Device	
14.	☐	 enpe2	192.168.115.65	Cisco IOS Device	
15.	☐	 enpe4	192.168.115.68	Cisco IOS Device	
16.	☐	 enpe5	192.168.115.69	Cisco IOS Device	
17.	☐	 enpe6	192.168.115.95	Cisco IOS Device	
18.	☐	 enswostr1	10.200.0.3	Cisco IOS Device	

116237

Service Inventory

Service Inventory contains tools to manage inventory elements, service requests, and devices. This is explained in [Chapter 3, “Service Inventory > Inventory and Connection Manager,”](#) and [Chapter 5, “Service Inventory > Device Console.”](#)

From the Home window you receive upon logging in, click the **Service Inventory** tab and you receive a window as shown in [Figure 1-10, “Service Inventory Selections.”](#)

Figure 1-10 Service Inventory Selections

Cisco Systems Home | Shortcuts | Account | Index | Help | About | Logout

IP Solution Center

Service Inventory
Service Design
Monitoring
Administration
User: admin

Inventory and Connection Manager
Device Console

You Are Here: ♦ Service Inventory Customer: None

Service Inventory

Tools to manage inventory elements, service requests, and devices.

 **Inventory and Connection Manager**

Create and manage inventory elements and Service Requests (SRs) for licensed services, and view topology maps.

 **Device Console**

Download commands and configlets to devices and view device configuration.

129016

The selections are as follows:

- **Inventory and Connection Manager** (explained in detail in [Chapter 3, “Service Inventory > Inventory and Connection Manager”](#))

The functions within **Inventory and Connection Manager** are shown in [Figure 1-11, “Inventory and Connection Manager Selections,”](#) and are as follows:

- **Service Requests** Create, deploy, and manage service requests (SRs). Details are explained in *User Guides*.
- **Traffic Engineering Management** Create, deploy, and manage elements of Traffic Engineering Management (explained in detail in *Cisco IP Solution Center Traffic Engineering Management User Guide, 4.0*).
- **Inventory Manager** Bulk-manage inventory elements (explained in detail in [Chapter 4, “Service Inventory > Inventory and Connection Manager > Inventory Manager”](#)).
- **Topology Tool** View topology maps.
- **Devices** Create and manage devices.
- **Device Groups** Create and manage device groups.
- **Customers** Create and manage customers.
- **Providers** Create and manage Providers.
- **Resource Pools** Create and manage pools for IP address, multicast address, route distinguisher, route target, site of origin, VC ID, and VLAN.
- **CE Routing Communities** Create and manage CE Routing Communities.
- **VPNs** Create and manage VPNs.
- **AAA Servers** Create and manage AAA Servers.
- **Named Physical Circuits** Create and manage Named Physical Circuits (NPCs).

Figure 1-11 Inventory and Connection Manager Selections



- **Device Console** Download commands and configlets to devices and view device configuration (explained in detail in [Chapter 5, “Service Inventory > Device Console”](#)).

Service Design

Service Design contains management tools for creating and managing policies, templates, protocols - **NOT SUPPORTED in this release.** -, Link QoS, and service attributes. This is explained in [Chapter 6, “Service Design.”](#)

From the Home window you receive upon logging in, click the **Service Design** tab and you receive a window as shown in [Figure 1-12, “Service Design Selections.”](#)

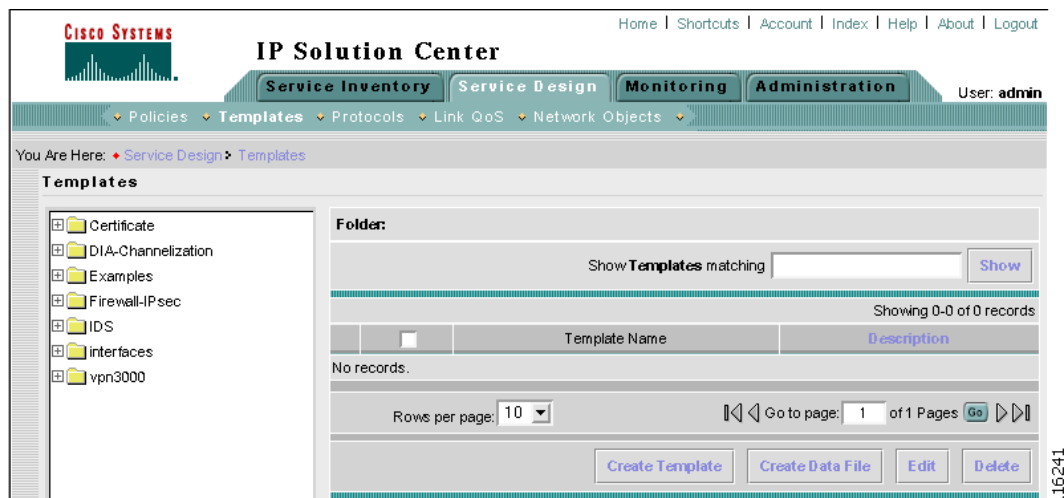
Figure 1-12 Service Design Selections



The selections are as follows:

- **Policies** Create and manage policies for licensed services. Details are explained in *User Guides*.
- **Templates** Create and manage templates and associated data. The available choices are shown in the left column of Figure 1-13, “[Templates Selections](#).”

Figure 1-13 Templates Selections



- **Protocols** Create and manage protocols and protocol bundles, currently used only by firewall policy - **NOT SUPPORTED in this release.** - The following choices are shown in Figure 1-14, “[Protocols Selections](#)”:
 - **Protocols** Create new or manage existing protocols. - **NOT SUPPORTED in this release.** -

- **Protocol Bundles** Create new or manage existing protocol bundles. - **NOT SUPPORTED** in this release. -

Figure 1-14 Protocols Selections



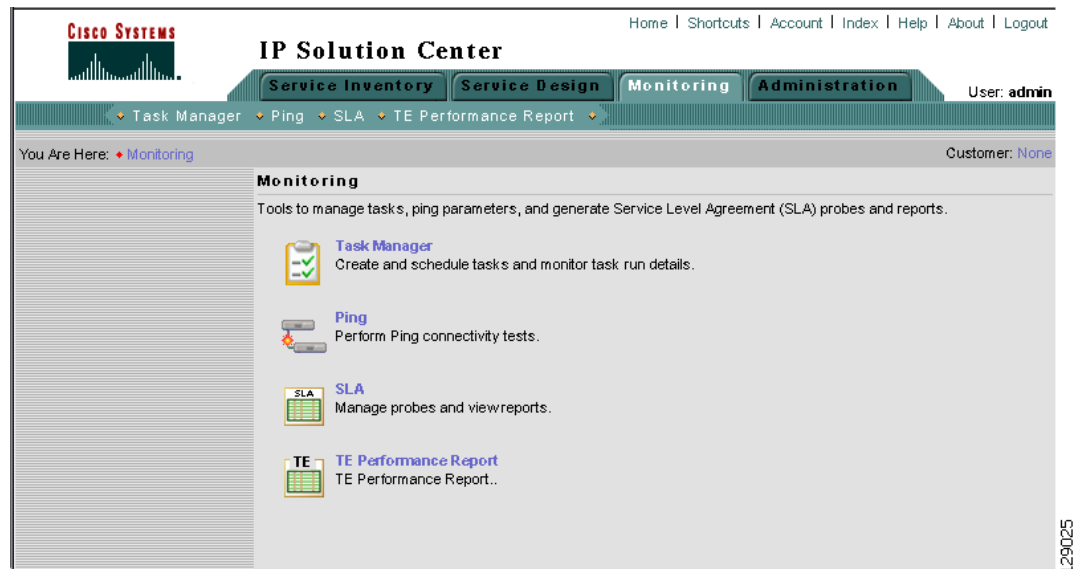
- **Link QoS** Create and manage IP Link QoS settings, currently used only by QoS.
- **Network Objects** Create and manage network objects for security services.

Monitoring

Monitoring contains tools to manage tasks, ping parameters, and Service Level Agreement (SLA) probes and reports. This is explained in [Chapter 7, “Monitoring.”](#)

From the Home window you receive upon logging in, click the **Monitoring** tab and you receive a window as shown in [Figure 1-15, “Monitoring Selections.”](#)

Figure 1-15 Monitoring Selections



The selections are as follows:

- **Task Manager** Create and schedule tasks and monitor task run details.
- **Ping** Perform Ping connectivity tests.
- **SLA** Manage probes and view reports.
- **TE Performance Report** TE Performance report.

Administration

Administration contains tools to manage users, ISC configuration, servers, remote installation, and licensing, to view users and the user access log, and to specify attributes for some messages. This is explained in detail in [Chapter 8, “Administration.”](#)

From the Home window you receive upon logging in, click the **Administration** tab and you receive a window as shown in [Figure 1-16, “Administration Selections.”](#)

Figure 1-16 Administration Selections

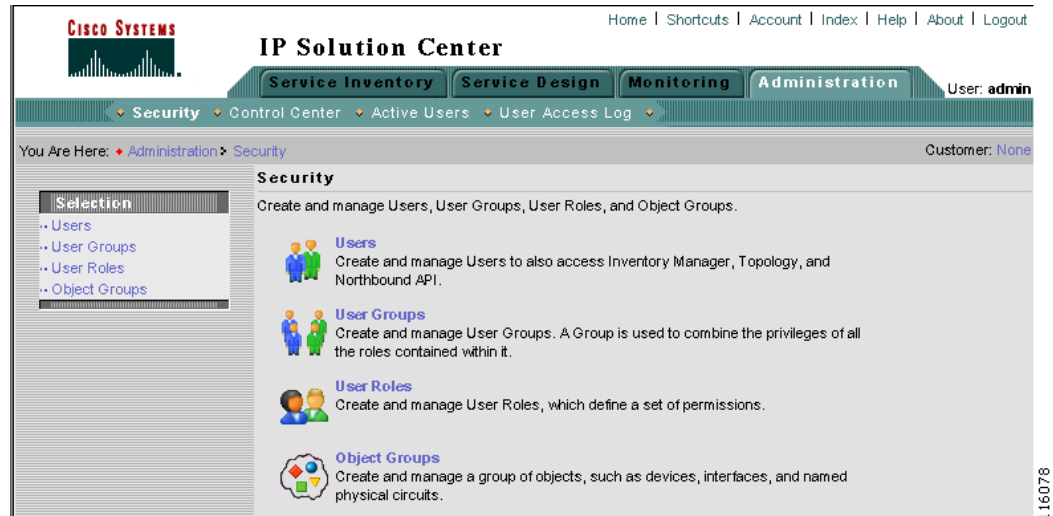


The selections are as follows:

- **Security** Create and manage Users, User Groups, User Roles, and Object Groups. The following choices are shown in [Figure 1-17, “Security Selections”](#):
 - **Users** Create and manage Users to also access Inventory Manager, Topology, and Northbound API.
 - **User Groups** Create and manage User Groups. A Group is used to combine the privileges of all the roles contained within it.
 - **User Roles** Create and manage User Roles, which define a set of permissions.

- **Object Groups** Create and manage a group of objects, such as devices, interfaces, and named physical circuits.

Figure 1-17 Security Selections



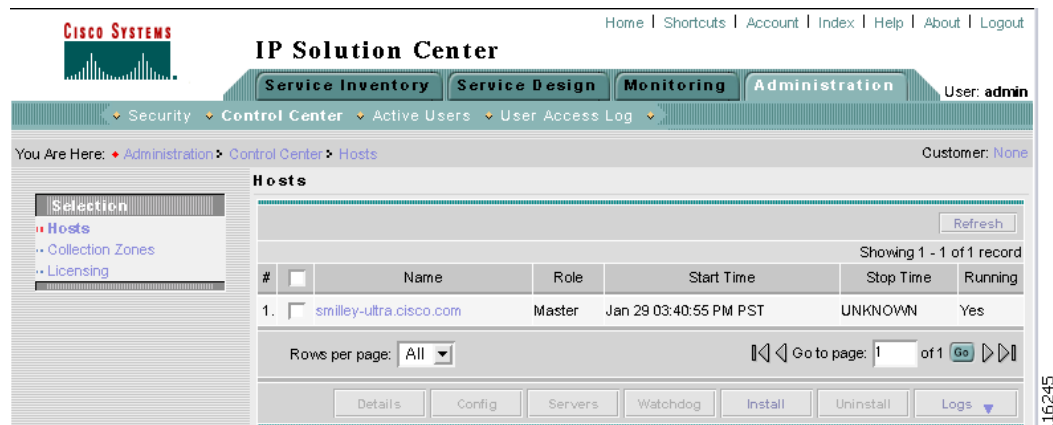
- **Control Center** Manage ISC configuration, servers, remote installation, and licensing. The following choices are shown in the left column of Figure 1-18, “Control Center Selections”:
 - **Hosts**

**Note**

From **Hosts**, you can choose **Install**. You can remotely install a Processing Server, Collection Server, or Interface Server. In this Remote Install, you *must* accept the default values, similar to the **express** install. If you want to do a **custom** install, this is only available through the Installation procedure explained in *Cisco IP Solution Center Installation Guide*.

- **Collection Zones**
- **Licensing**

Figure 1-18 Control Center Selections



- **Active Users** View users currently connected to ISC. Disconnect users.
- **User Access Log** View the user access log.
- **Manage TIBCO Rendezvous** Specify attributes for proper messaging among all Java™ Web Start distributed applications.



WatchDog Commands

The WatchDog is responsible for bootstrapping Cisco IP Solution Center (ISC) and starting the necessary set of server processes. In addition, the WatchDog monitors the health and performance of each server to ensure it is functioning properly. In the event of a software error that causes a server to fail, the WatchDog automatically restarts the errant server.

The WatchDog is a background daemon process that is automatically installed as part of the installation procedure for ISC. After the installation procedure has completed, WatchDog is started automatically. You can execute the **startwd** command to run the WatchDog after the installation. The WatchDog is automatically started any time the machine is rebooted.

This chapter provides the description, syntax, and arguments (listed alphabetically) for the following WatchDog commands:

- [startdb Command, page 2-1](#)
- [startns Command, page 2-2](#)
- [startwd Command, page 2-2](#)
- [stopall Command, page 2-3](#)
- [stopdb Command, page 2-3](#)
- [stopns Command, page 2-4](#)
- [stopwd Command, page 2-4](#)
- [wdclient Command, page 2-5](#)

startdb Command

This section provides the description and syntax for the **startdb** command.

Description

The **startdb** command starts the database.

Syntax

startdb

The **startdb** command has no arguments and starts the database.

The location of **startdb** is: *<ISC Directory>/bin*.


Note

Do *not* run **startwd** in the background. Do *not* enter **startwd &**.

startns Command

This section provides the description and syntax for the **startns** command.

Description

The **startns** command starts the name server.

Syntax

startns

The **startns** command has no arguments and starts the name server.

The location of **startns** is: *<ISC Directory>/bin*.

startwd Command

This section provides the description and syntax for the **startwd** command.

Description

The **startwd** command starts the WatchDog and all ISC processes. The **startwd** command includes the functionality of **startdb** (see the [“startdb Command” section on page 2-1](#)) and **startns** (see the [“startns Command” section on page 2-2](#)). Executing this command is a necessary procedure and occurs automatically as part of the installation. Use this **startwd** command after issuing a **stopwd** command to restart the WatchDog. The master ISC host *must* be started first. Other ISC hosts can be started any time after the master ISC host, but all hosts *must* be started before starting to use ISC.

If for some reason the master ISC host is stopped, either inadvertently or by issuing the **stopwd** command, this master ISC host can be restarted by using the **startwd** command.

orbd (from JDK) is required, but **startwd** starts it if it is not already running. The **startns** and **stopns** commands deal with **orbd**.

Syntax

startwd

The **startwd** command has no arguments and starts the WatchDog only for the machine where it is executed.

The location of **startwd** is: *<ISC Directory>/bin*.



Note

Do *not* run **startwd** in the background. Do *not* enter **startwd &**.

stopall Command

This section provides the description and syntax for the **stopall** command.

Description

The **stopall** command stops the database, name server, and WatchDog on the machine on which it is run. The **stopall** command includes the functionality of **stopdb -y** (see the “[stopdb Command](#)” section on page 2-3), **stopns -y** (see the “[stopns Command](#)” section on page 2-4), and **stopwd -y** (see the “[stopwd Command](#)” section on page 2-4). Normally this is only necessary before installing new versions of ISC.

Syntax

stopall



Caution

There is no **-y** parameter. Therefore, everything stops without the ability to cancel.

The location of **stopall** is: *<ISC Directory>/bin*.

stopdb Command

This section provides the description and syntax for the **stopdb** command.

Description

The **stopdb** command stops the database.

Syntax

stopdb [-y]

where:

-y indicates not to prompt before shutdown. If **-y** is not specified, you are prompted with the following message: “Are you absolutely sure you want to stop the watchdog and all of its servers? Other users may be using this system as well. No activity (for example: collections, performance monitoring, provisioning) occurs until the system is restarted.” You are then prompted to reply **yes** or **no**.

The location of **stopdb** is: *<ISC Directory>/bin*.

stopns Command

This section provides the description and syntax for the **stopns** command.

Description

The **stopns** command stops the name server.

Syntax

stopns [-y]

where:

-y indicates not to prompt before shutdown. If **-y** is not specified, you are prompted with the following message: “Are you absolutely sure you want to stop the watchdog and all of its servers? Other users may be using this system as well. No activity (for example: collections, performance monitoring, provisioning) occurs until the system is restarted.” You are then prompted to reply **yes** or **no**.

The location of **stopns** is: <ISC Directory>/bin.

stopwd Command

This section provides the description and syntax for the **stopwd** command.

Description

The **stopwd** command stops the WatchDog and all ISC processes other than the name server and the database.

Syntax

stopwd [-y] [-all]

where:

-y indicates not to prompt before shutdown. If **-y** is not specified, you are prompted with the following message: “Are you absolutely sure you want to stop the watchdog and all of its servers? Other users may be using this system as well. No activity (for example: collections, performance monitoring, provisioning) occurs until the system is restarted.” You are then prompted to reply **yes** or **no**.

-all indicates to stop all the hosts. This argument is only available to the master host.

The location of **stopwd** is: <ISC Directory>/bin.

wdclient Command

This section provides the description, syntax, and options (listed alphabetically) for the **wdclient** subcommands. These subcommands are diagnostic tools. This section also describes the column format of the output of each of the subcommands.

**Note**

The location of **wdclient** is: *<ISC Directory>/bin*.

The following are the **wdclient** subcommands:

- [wdclient disk Subcommand, page 2-5](#)
- [wdclient group <group_name> Subcommand, page 2-6](#)
- [wdclient groups Subcommand, page 2-6](#)
- [wdclient health Subcommand, page 2-7](#)
- [wdclient restart Subcommand, page 2-7](#)
- [wdclient start Subcommand, page 2-7](#)
- [wdclient status Subcommand, page 2-8](#)
 - [Information Produced: Name Column, page 2-9](#)
 - [Information Produced: State Column, page 2-9](#)
 - [Information Produced: Gen Column, page 2-10](#)
 - [Information Produced: Exec Time Column, page 2-10](#)
 - [Information Produced: Success Column, page 2-10](#)
 - [Information Produced: Missed Column, page 2-10](#)
- [wdclient stop Subcommand, page 2-10](#)
- [wdclient syshealth Subcommand, page 2-11](#)

wdclient disk Subcommand

This section provides the description and syntax for the **wdclient disk** subcommand.

Description

The **wdclient disk** subcommand gives the disk space statistics for the directories where ISC is installed.

Syntax

wdclient [-master [-host <hostname>]] disk

where:

-master is an optional parameter that indicates to give the WatchDog information for the master ISC host. If **-master** is not specified, only local information about the current host is given.

-host *<hostname>* is an optional parameter. *<hostname>* is the fully-qualified name of the remote host on which the WatchDog is running. If this optional parameter is not specified, information from all the hosts is returned.

wdclient group *<group_name>* Subcommand

This section provides the description and syntax for the **wdclient group *<group_name>*** subcommand.

Description

The **wdclient group *<group_name>*** subcommand lists the servers in the specified server group. Server groups provide a convenient way to start or stop a group of servers with a single command.

Syntax

wdclient [-master [-host *<hostname>*]] group *<group_name>*

where:

-master is an optional parameter that indicates to give the WatchDog information for the master ISC host. If **-master** is not specified, only local information about the current host is given.

-host *<hostname>* is an optional parameter. *<hostname>* is the fully-qualified name of the remote host on which the WatchDog is running. If this optional parameter is not specified, information from all the hosts is returned.

<group_name> is the name of a server group chosen from the list displayed by the **wdclient groups** command.

wdclient groups Subcommand

This section provides the description and syntax for the **wdclient groups** subcommand.

Description

The **wdclient groups** subcommand lists all the active server groups.

Syntax

wdclient [-master [-host *<hostname>*]] groups

where:

-master is an optional parameter that indicates to give the information for the master ISC host. If **-master** is not specified, only local information about the current host is given.

-host *<hostname>* is an optional parameter. *<hostname>* is the fully-qualified name of the remote host on which the WatchDog is running. If this optional parameter is not specified, information from all the hosts is returned.

wdclient health Subcommand

This section provides the description and syntax for the **wdclient health** subcommand.

Description

The **wdclient health** subcommand indicates whether all the servers are stable on the master ISC host.

Syntax

```
wdclient health
```

wdclient restart Subcommand

This section provides the description and syntax for the **wdclient restart** subcommand.

Description

The **wdclient restart** subcommand restarts one or more servers. Any dependent servers are also restarted.



Note

It is not necessary to restart servers in a properly functioning system. The **wdclient restart** command should only be run under the direction of Cisco Support.

Syntax

```
wdclient [-master [-host <hostname>]] restart [all | <server_name> | group <group_name>]
```

where:

-master is an optional parameter that indicates the restart operation should be performed on the master ISC host. If **-master** is not specified, the restart operation is performed only on the local machine.

-host <hostname> is an optional parameter. **<hostname>** is the fully-qualified name of the remote host on which the WatchDog is running. If this optional parameter is not specified, information from all the hosts is returned.

You can choose one of the following arguments. If none are chosen, the default is **all**:

all is all servers. This is the default if no argument is specified.

<server_name> is the name of a server chosen from the list displayed by the **wdclient status** command. See [Table 2-1, “Servers and Their Functions,”](#) for server descriptions.

group <group_name> is the term **group** followed by the name of a server group chosen from the list displayed by the **wdclient groups** command.

wdclient start Subcommand

This section provides the description and syntax for the **wdclient start** subcommand.

Description

The **wdclient start** subcommand starts one or more servers. Other servers that depend on the specified server(s) might also start.



Note

It is not necessary to stop and start servers in a properly functioning system. The **wdclient start** command should only be run under the direction of Cisco Support.

Syntax

```
wdclient [-master [-host <hostname>]] start [all | <server_name> | group <group_name>]
```

where:

-master is an optional parameter that indicates the start operation should be performed on the master ISC host. If **-master** is not specified, the start operation is performed only on the local machine.

-host <hostname> is an optional parameter. <hostname> is the fully-qualified name of the remote host on which the WatchDog is running. If this optional parameter is not specified, information from all the hosts is returned.

You can choose one of the following arguments. If none are chosen, the default is **all**:

all is all servers. This is the default if no argument is specified.

<server_name> is the name of a server chosen from the list displayed by the **wdclient status** command. See [Table 2-1, “Servers and Their Functions,”](#) for server descriptions.

group <group_name> is the name of a server group chosen from the list displayed by the **wdclient groups** command.

wdclient status Subcommand

This section provides the description, syntax, and information produced for the **wdclient status** subcommand.

Description

The **wdclient status** subcommand lists all the servers and their states. See [Table 2-1 on page 2-9, “Servers and Their Functions,”](#) for server descriptions. See [Table 2-2 on page 2-9, “Valid States,”](#) for the list of all the states.

Syntax

```
wdclient [-master [-host <hostname>]] [-poll <seconds>]] status
```

where:

-master is an optional parameter that indicates to give the information for the master ISC host. If

-master is not specified, only local information about the current host is given.

-host *<hostname>* is an optional parameter. *<hostname>* is the fully-qualified name of the remote host on which the WatchDog is running. If this optional parameter is not specified, information from all the hosts is returned.

-poll *<seconds>* is an optional parameter. *<seconds>* is the number of seconds. A number other than zero indicates that when new status data is available it is displayed every *<seconds>* seconds, where *<seconds>* is the specified number of seconds. The default **-poll** value is zero (0), which shows the status just once.

Information Produced: Name Column

The **Name** column provides the name of each of the servers. [Table 2-1](#) provides a list of the servers and a description of the function that each server provides.

Table 2-1 Servers and Their Functions

Server	Function
cnsserver	Handles TIBCO messages from Cisco CNS IE2100 appliances and takes appropriate actions.
cornerstonebridge	Used for peer-to-peer communication with client applications invoking auto-discovery commands.
dbpoller	Monitors database server.
dispatcher	Manages workers. Distributes work to other hosts (if any).
httpd	Web server.
lockmanager	Handles device locking so a router's configuration is not modified by multiple service requests at the same time.
nspoller	Monitors name service.
scheduler	Enables you to schedule tasks immediately or later in time, for one-time or repeated execution.
worker	Executes various ISC tasks/jobs such as Provisioning.

Information Produced: State Column

The **State** column provides the current state of the server. [Table 2-2](#) provides a description of each of the states in normal progression order.

Table 2-2 Valid States

State	Description
start_depends	This server has been asked to start, but is waiting for servers it depends on to start. After all dependent servers have started, this server transitions to the state of starting.
starting	This server is currently starting. After a successful heartbeat occurs, this server transitions to the state of started.
started	This server is currently started and running.
stop_depends	This server is supposed to be stopped, but it is waiting for servers it depends on to be stopped first.

Table 2-2 Valid States (continued)

State	Description
stopping_gently	This server is in the process of stopping in a gentle fashion. That is, it was notified that it is to stop.
stopping_hard	This server is in the process of being killed because either it did not have a way to stop gently or because the gentle stop took too long.
stopped	This server is stopped. The WatchDog either starts it again or disables it if it has been frequently dying.
disabled_dependent	This server is disabled because one or more servers it depends on are disabled. If all servers it depends on are started, this server automatically starts.
disabled	This server is disabled and must be manually restarted.
restart_delay	This server is delaying before restarting. There is a short delay after a server stops and before it is restarted again.

Information Produced: Gen Column

The **Gen** column provides the generation of the server. Each time the server is started, the generation is incremented by 1.

Information Produced: Exec Time Column

The **Exec Time** column provides the date and time the server was last started.

Information Produced: PID Column

The **PID** column provides the UNIX process identifier for each server, except for dbpoller and nspoller.

Information Produced: Success Column

The **Success** column provides the number of successful heartbeats since the server was last started. Heartbeats are used to verify that servers are functioning correctly.

Information Produced: Missed Column

The **Missed** column provides the number of missed heartbeats since the server was last started.

A few missed heartbeats could simply indicate the system was busy. However, more than a couple of missed heartbeats per day could indicate a problem. See the logs to diagnose the reason.

Three missed heartbeats in a row is the default for restarting the server.

wdclient stop Subcommand

This section provides the description and syntax for the **wdclient stop** subcommand.

Description

The **wdclient stop** subcommand stops one or more servers. Other servers that depend on the specified servers also stop.



Note

It is not necessary to stop servers in a properly functioning system. The **wdclient stop** command should *only* be run under the direction of Cisco Support.

Syntax

```
wdclient [-master [-host <hostname>]] stop [all | <server_name> | group <group_name>]
```

where:

-master is an optional parameter that indicates to perform the operation on the master ISC host.

-host <hostname> is an optional parameter. <hostname> is the fully-qualified name of the remote host on which the WatchDog is running. If this optional parameter is not specified, information from all the hosts is returned.

You can choose one of the following arguments. If none are chosen, the default is **all**.

all is all servers. This is the default if no argument is specified.

<server_name> is the name of a server chosen from the list displayed by the **wdclient status** command. See [Table 2-1, “Servers and Their Functions,”](#) for server descriptions.

group <group_name> is the name of a server group chosen from the list displayed by the **wdclient groups** command.

wdclient syshealth Subcommand

This section provides the description and syntax for the **wdclient syshealth** subcommand.

Description

The **wdclient syshealth** subcommand gives the system health information about the entire system, including the master and the hosts. Their health is listed either as **good**, which means, running, or **not good**, which means, not running.

Syntax

```
wdclient -master [-host <hostname>] syshealth
```

where:

-master is a required parameter that indicates to give the information for the master ISC host.

-host <hostname> is an optional parameter. <hostname> is the fully-qualified name of the remote host on which the WatchDog is running. If this optional parameter is not specified, information from all the hosts is returned.



Service Inventory > Inventory and Connection Manager

From the Home window of Cisco IP Solution Center (ISC), you receive upon logging in, click the **Service Inventory** tab and you receive a window, as shown in [Figure 3-1](#), “[Service Inventory Selections](#).”

Figure 3-1 Service Inventory Selections



Click on **Inventory and Connection Manager** and a window as shown in [Figure 3-2](#), “[Inventory and Connection Manager Selections](#),” appears.

Figure 3-2 Inventory and Connection Manager Selections



From **Inventory and Connection Manager**, you can navigate to any of the following functions:

- **Service Requests, page 3-3** Create, deploy, and manage Service Requests (SRs).
- **Traffic Engineering Management, page 3-5** Create, deploy, and manage elements of Traffic Engineering Management.
- **Inventory Manager, page 3-5** Bulk-manage inventory elements.
- **Topology Tool, page 3-5** View topology maps.
- **Devices, page 3-38** Create and manage Devices.
- **Device Groups, page 3-80** Create and manage Device Groups.
- **Customers, page 3-86** Create and manage Customers.
- **Providers, page 3-95** Create and manage Providers.
- **Resource Pools, page 3-102** Create and manage pools for IP address, Multicast address, Route Distinguisher, Route Target, Site of Origin, VC ID, and VLAN.
- **CE Routing Communities, page 3-114** Create and manage CE Routing Communities.
- **VPNs, page 3-117** Create and manage VPNs.
- **AAA Servers, page 3-121** Create and manage AAA Servers.
- **Named Physical Circuits, page 3-123** Create and manage Named Physical Circuits (NPCs).

Service Requests

Service Requests are explained in each of the *User Guides* for each of the licensed services.

Table 3-1, “Summary of Cisco IP Solution Center Service Request States,” describes each ISC service request state. The states are listed in alphabetical order.

Table 3-1 Summary of Cisco IP Solution Center Service Request States

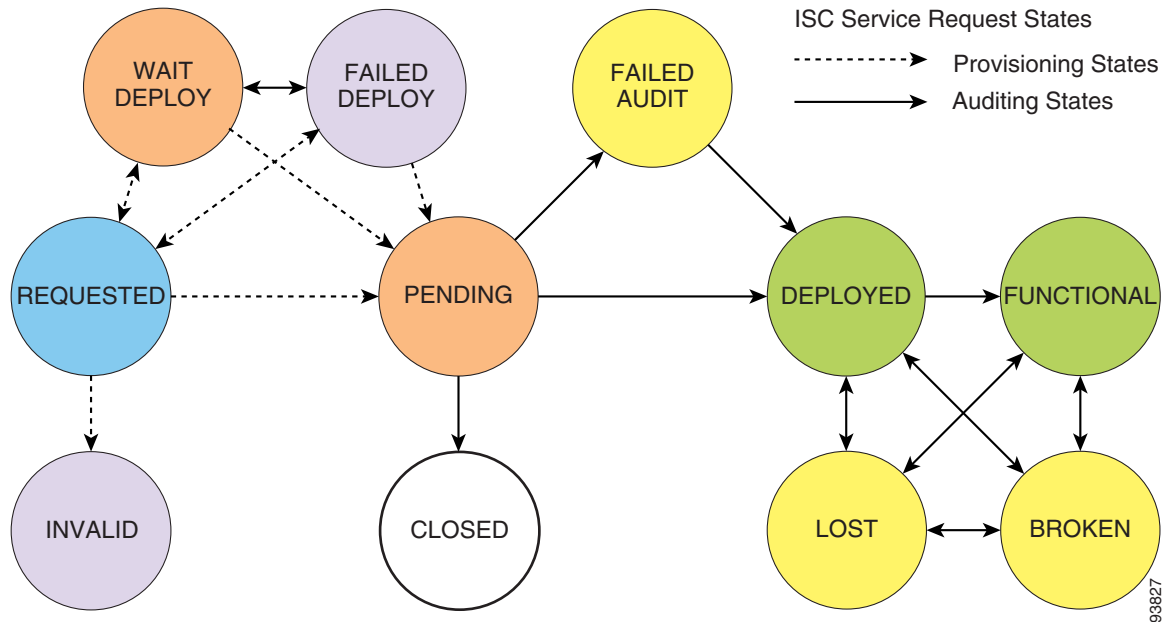
Service Request Type	Description
Broken	The router is correctly configured but the service is unavailable (due to a broken cable or Layer 2 problem, for example). An MPLS service request moves to Broken if the auditor finds the routing and forwarding tables for this service, but they do not match the service intent. An IPsec service request moves to Broken if a ping fails for all the remote peers of the current device. - NOT SUPPORTED in this release. -
Closed	A service request moves to Closed if the service request should no longer be used during the provisioning or auditing process. A service request moves to the Closed state only upon successful audit of a decommission service request. ISC does not remove a service request from the database to allow for extended auditing. Only a specific administrator purge action results in service requests being removed.
Deployed	A service request moves to Deployed if the intention of the service request is found in the router configuration file. Deployed indicates that the configuration file has been downloaded to the router, and the intent of the request has been verified at the configuration level. That is, ISC downloaded the configlets to the routers and the service request passed the audit process.
Failed Audit	This state indicates that ISC downloaded the configlet to the router successfully, but the service request did not pass the audit. Therefore, the service did not move to the Deployed state. The Failed Audit state is initiated from the Pending state. After a service request is deployed successfully, it cannot re-enter the Failed Audit state (except if the service request is redeployed).
Failed Deploy	The cause for a Failed Deploy status is that DCS reports that either the upload of the initial configuration file from the routers failed or the download of the configuration update to the routers failed (due to lost connection, faulty password, and so on).
Functional	An MPLS service request moves to Functional when the auditor finds the VPN routing and forwarding tables (VRF) for this service and they match with the service intent. This state requires that both the configuration file audit and the routing audit are successful. An IPsec service request moves to Functional when the auditor finds that the router is configured properly and the IPsec traffic is flowing (ping is used to determine if IPsec traffic is flowing). - NOT SUPPORTED in this release. -

Table 3-1 Summary of Cisco IP Solution Center Service Request States (continued)

Service Request Type	Description
Invalid	Invalid indicates that the service request information is incorrect in some way. A service request moves to Invalid if the request was either internally inconsistent or not consistent with the rest of the existing network/router configurations (for example, no more interfaces were available on the router). The Provisioning Driver cannot generate configuration updates to service this request.
Lost	A service request moves to Lost when the Auditor cannot find a configuration-level verification of intent in the router configuration files. The service request was in the Deployed state, but now some or all router configuration information is missing. A service request can move to the Lost state <i>only</i> when the service request had been Deployed .
Pending	A service request moves to Pending when the Provisioning Driver determines that the request looks consistent and was able to generate the required configuration updates for this request. Pending indicates that the service request has generated the configuration updates and the configuration updates are successfully downloaded to the routers. The Auditor regards pending service requests as new requests and begins the audit. If the service has been freshly provisioned and not yet audited, it is not an error (pending audit). However, if an audit is performed and the service is still pending, it is in an error state.
Requested	If the service is newly entered and not yet deployed, it is not an error. However, if a Deploy is done and it remains Requested , the service is in an error state.
Wait Deploy	This service request state pertains only when downloading configlets to a Cisco CNS-CE server, such as a Cisco CNS IE2100 appliance. Wait Deploy indicates that the configlet has been generated, but it has not been downloaded to the Cisco CNS-CE server because the device is not currently online. The configlet is staged in the repository until such time as the Cisco CNS-CE server notifies ISC that it is up. Configlets in the Wait Deploy state are then downloaded to the Cisco CNS-CE server.

Figure 3-3, “Service Request States Transition Diagram,” shows the transitions of states.

Figure 3-3 Service Request States Transition Diagram



Traffic Engineering Management

Traffic Engineering Management allows you to create, deploy, and manage elements of Traffic Engineering Management. This is explained in detail in [Cisco IP Solution Center Traffic Engineering Management User Guide, 4.0](#).

Inventory Manager

Inventory Manager enables an operator to import network specific data into the ISC Repository in bulk mode. Inventory Manager is explained in detail in [Chapter 4, “Service Inventory > Inventory and Connection Manager > Inventory Manager”](#).

Topology Tool

The topology tool provides a graphical view of networks set up through the ISC web client. It gives a graphical representation of the various physical and logical parts of the network, both devices and links.

- [Introduction, page 3-6](#)
- [Launching Topology Tool, page 3-7](#)
- [Conventions, page 3-9](#)
- [Accessing the Topology Tool for ISC-VPN Topology, page 3-11](#)
- [Types of Views, page 3-13](#)
 - [VPN View, page 3-15](#)

- [Logical View, page 3-19](#)
 - [Physical View, page 3-22](#)
- [Viewing Device and Link Properties, page 3-23](#)
- [Filtering and Searching, page 3-30](#)
 - [Filtering, page 3-30](#)
 - [Searching, page 3-33](#)
- [Using Maps, page 3-34](#)
 - [Loading a map, page 3-35](#)
 - [Layers, page 3-36](#)
 - [Map data, page 3-37](#)
 - [Node locations, page 3-37](#)
 - [Adding new maps, page 3-38](#)
- [Devices, page 3-38.](#)

Introduction

The topology tool includes three types of views:

- VPN view—shows connectivity between customer devices. The VPN view also gives an aggregate view of all services and individual logical and physical views of each of the services.
- Logical view—shows logical connections set up in a selected provider region
- Physical view—displays connectivity of named physical circuits in a provider region.

In addition, this chapter describes the following features:

- Filtering and Searching—filter out unnecessary detail in large graphs or jump straight to a particular device using the search tool
- Using Maps—associate maps with the individual views.

Please note that some details, such as window decorations, are system specific and might appear differently in different environments. However, the functionality should remain consistent.

Launching Topology Tool

To launch the Topology Tool, follow these steps:

- Step 1** Log into ISC.
- Step 2** Navigate **Service Inventory > Inventory and Connection Manager > Topology Tool** and a window appears, as shown in [Figure 3-4](#), “Topology Launch.” If you do not have the proper Java Runtime Environment (JRE) as specified at the bottom of the window, click the corresponding link for your system, follow that path, then quit the browser, log in again, and navigate back to the Topology Tool page.

Figure 3-4 Topology Launch

Topology Tool

View topology maps.

 **ISC-VPN Topology**
Launches a Java™ Web Start application that presents graphical views of VPNs, Regions, and Access Domains.

 **ISC-TEM Topology Interface Applet**
Launches the ISC-TEM Topology Interface Applet.

Java Runtime Environment (JRE) and Java Webstart must be installed to run Inventory Manager. If you are having trouble getting them to function properly or need to update your local JRE please download and install one appropriate for your operating system.

JRE Description	Platform	Version	Supported
Windows (all languages, including English)	Windows	1.4.2_04	Yes
Solaris SPARC 32-bit self-extracting file	Solaris SPARC	1.4.2_04	Yes
Linux self-extracting file	Linux	1.4.2_04	No

- Step 3** Click **ISC-VPN Topology** in [Figure 3-4](#), “Topology Launch” to launch the Topology Tool application on the web client. This starts up the Java Web Start application.

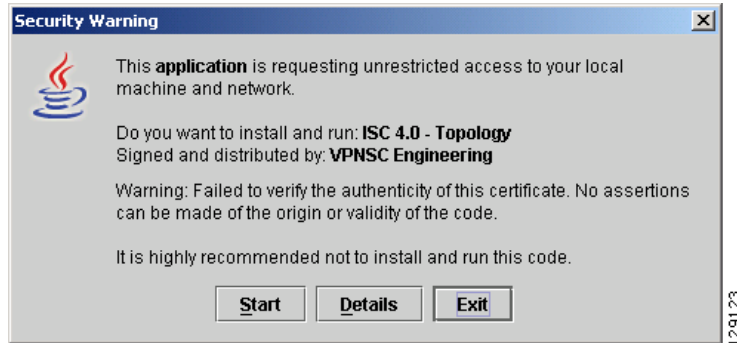


Note

Name resolution is required. The ISC HTTP server host must be in the Domain Name System (DNS) that the web client is using or the name and address of the ISC server must be in the client host file.

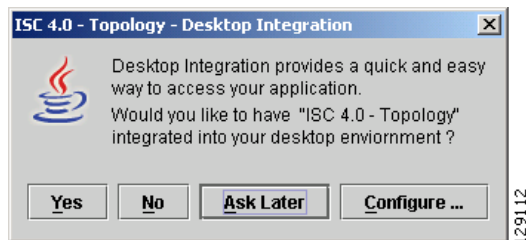
- Step 4** The first time Inventory Manager is activated, the Security Warning window in [Figure 3-5](#) appears. Click **Start** to proceed or **Details** to verify the security certificate.

Figure 3-5 Security Warning



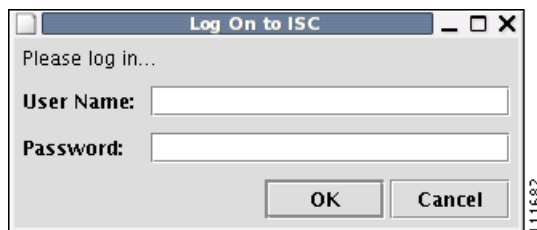
- Step 5** The Desktop Integration window in [Figure 3-6](#) appears. Click **Yes** to integrate into your desktop environment, click **No** to decline, click **Ask Later** to be prompted the next time VPN Topology is invoked, or click **Configure ...** to customize the desktop integration.

Figure 3-6 Topology Desktop Integration



The Login window in [Figure 3-7](#), “Log On to ISC.” appears whether or not a selection has been made in the Desktop Integration window.

Figure 3-7 Log On to ISC



- Step 6** Enter your **User Name** and **Password** and click **OK**. The Topology Tool launches and connects to the Master ISC server.

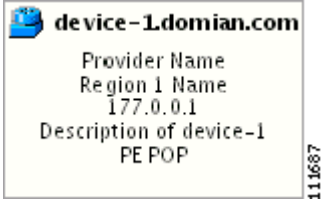
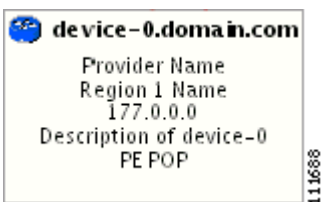
Conventions

Topology software uses several conventions to visually communicate information about displayed objects. The shape and color of a node representing a device depends on the role of the device, as shown in [Table 3-2](#):

Table 3-2 Device Role Shapes

Shape	Description
 device-b.domain.com Customer Name Site B Name 188.0.0.1 Description of device-b SPOKE 111683	Green icon for a CAT OS customer device followed by the following information: - Device name - Customer Name - Site Name - Management IP Address - Description - Role (SPOKE or HUB of a VPN)
 device-a.domain.com Customer Name Site A Name 180.0.0.0 Description of device-a SPOKE 111684	Green icon for a router customer device followed by the following information: - Device name - Customer Name - Site Name - Management IP Address - Description - Role (SPOKE or HUB of a VPN)
 device-c.domain.com Customer Name Site C Name 188.0.0.2 Description of device-c HUB 111685	Green icon for a VPN 3000 customer device (This feature is not supported in this device) followed by the following information: - Device name - Customer Name - Site Name - Management IP Address - Description - Role (SPOKE or HUB of a VPN)
 Ethernet 0/1 173.2.3.4 Default Packet Over SONET 111686	Green icon for an interface followed by the following information: - Interface name - Management IP Address - Encapsulation Type - Interface Type

Table 3-2 Device Role Shapes (continued)

Shape	Description
 device-1.domain.com Provider Name Region 1 Name 177.0.0.1 Description of device-1 PE POP 111687	Blue icon for a CAT OS provider device followed by the following information: - Device name - Provider Name - Region Name - Management IP Address - Description - Role
 device-0.domain.com Provider Name Region 1 Name 177.0.0.0 Description of device-0 PE POP 111688	Blue icon for a router provider device followed by the following information: - Device name - Provider Name - Region Name - Management IP Address - Description - Role
 Region 1 Name Provider Name 111689	Blue icon for a region followed by the following information: - Region name - Provider Name
 Site C Name Customer Name HUB 111690	Green icon for a site followed by the following information: - Site name - Customer Name - Role in which Site's device joined VPN (HUB, SPOKE, or combination of HUB and SPOKE)
 Site A Name Customer Name SPOKE 111691	Green icon for a site followed by the following information: - Site name - Customer Name - Role in which Site's device joined VPN (HUB, SPOKE, or combination of HUB and SPOKE)

A distinct color scheme is used to highlight the link type as shown in [Table 3-3](#):

Table 3-3 Link Type Color Scheme

Color	Connection Type
 (green)	End-to-end wire
 (purple)	Attachment circuit
 (light blue)	IPsec tunnel (IPsec is not supported in this release.)
 (brown)	MPLS VPN link

Finally, the four patterns shown in [Table 3-4](#) are used to indicate the service request state:

Table 3-4 Link State Pattern Scheme

Pattern	Service Request State
	Deployed, functional, pending
	Failed audit, invalid, broken, lost
	Wait deploy, requested, failed deploy
	Closed

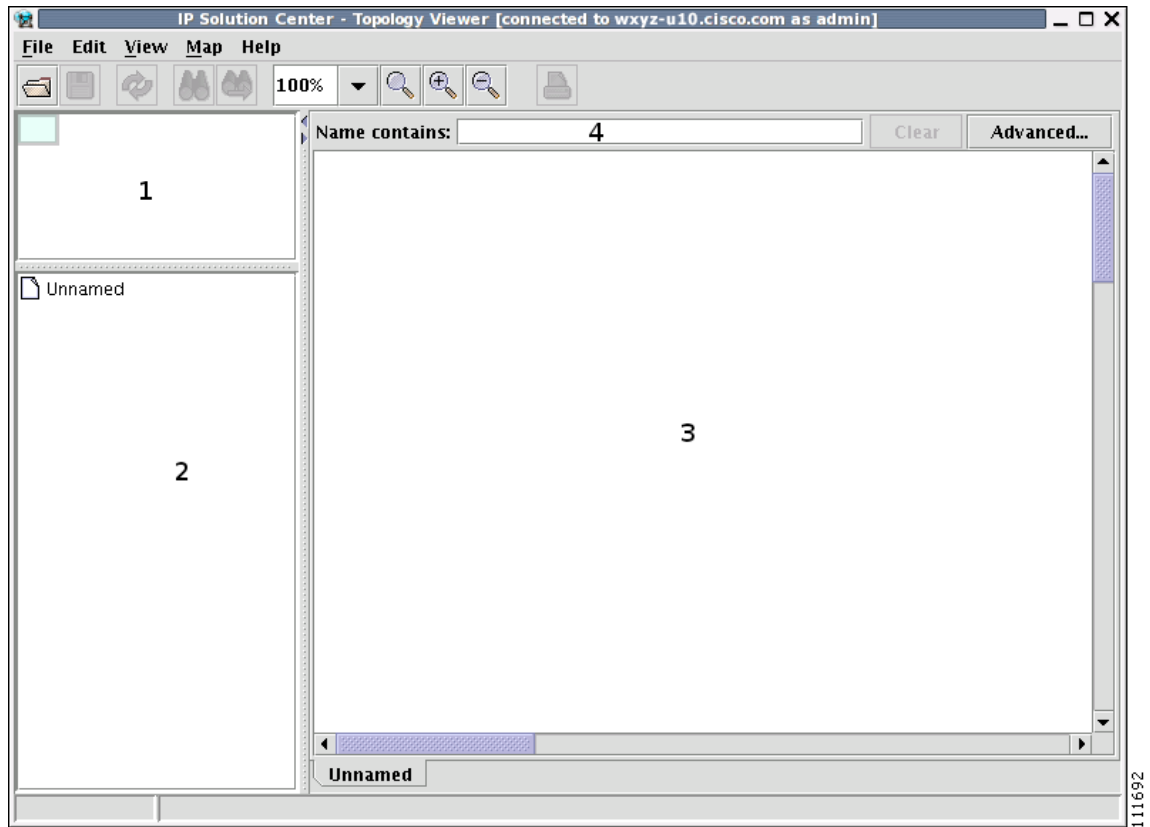
Accessing the Topology Tool for ISC-VPN Topology

Launch the Topology Tool as explained in [Figure 3-4](#), “Topology Launch,” in the “[Launching Topology Tool](#)” section on [page 3-7](#) and then use the following steps to access the **ISC-VPN Topology** tool.

- Step 1** Navigate **Service Inventory > Inventory and Connection Manager > Topology Tool > ISC-VPN Topology**.

The Topology window shown in [Figure 3-8](#) appears.

Figure 3-8 Topology Application Window



The application window is divided into four areas, as shown in [Figure 3-8](#):

- area (1)—The top left corner shows the Overview area. The colored rectangular panel, called the panner, corresponds to the area currently visible in the main area. Moving the panner around changes the part of the graph showing in the main area. This is particularly useful for large graphs.
- area (2)—The bottom left area shows the Tree View of the graph. When no graph is shown, a single node called **Unnamed** is displayed. When a graph is shown, a tree depicting devices and their possible interfaces and connections is displayed. The tree can be used to quickly locate a device or a connection.
- area (3)—The main area (Main View) of the window shows a graph representing connections between devices. The name of the displayed network is shown at the bottom. When no view is present, the name defaults to **Unnamed**.
- area (4)—Above the main window is the Filter area. It allows you to filter nodes by entering a pattern. Nodes whose name contains the entered pattern maintain the normal level of brightness. All other nodes and edges become dimmed, as shown in [Figure 3-30](#) and the “Filtering” section on [page 3-30](#).

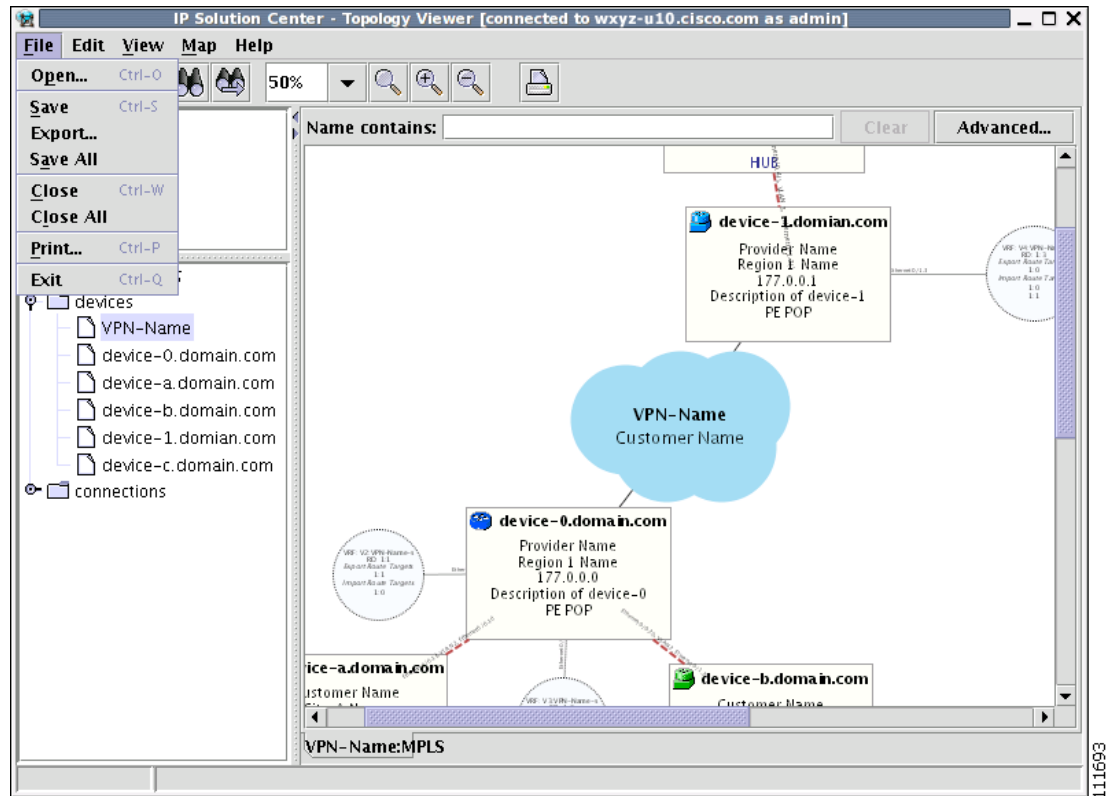


Note

The bottom bar below all the areas, is a Status bar.

Views are loaded, saved, and closed using the **File** menu, as shown in [Figure 3-9](#).

Figure 3-9 The File Menu



The **File** menu contains the following menu items:

- **Open**—Opens a view.
- **Save**—Saves the open and active view with the existing file name, if any.
- **Export...**—Exports the active view in either Scalable Vector Graphics (SVG), Joint Photographic Experts Group (JPG), or Portable Network Graphics (PNG) format.
- **Save All**—Saves all open views.
- **Close**—Closes the open and active view.
- **Close All**—Closes all open views.
- **Print...**—Prints the open and active view.
- **Exit**—Exits the Topology tool.

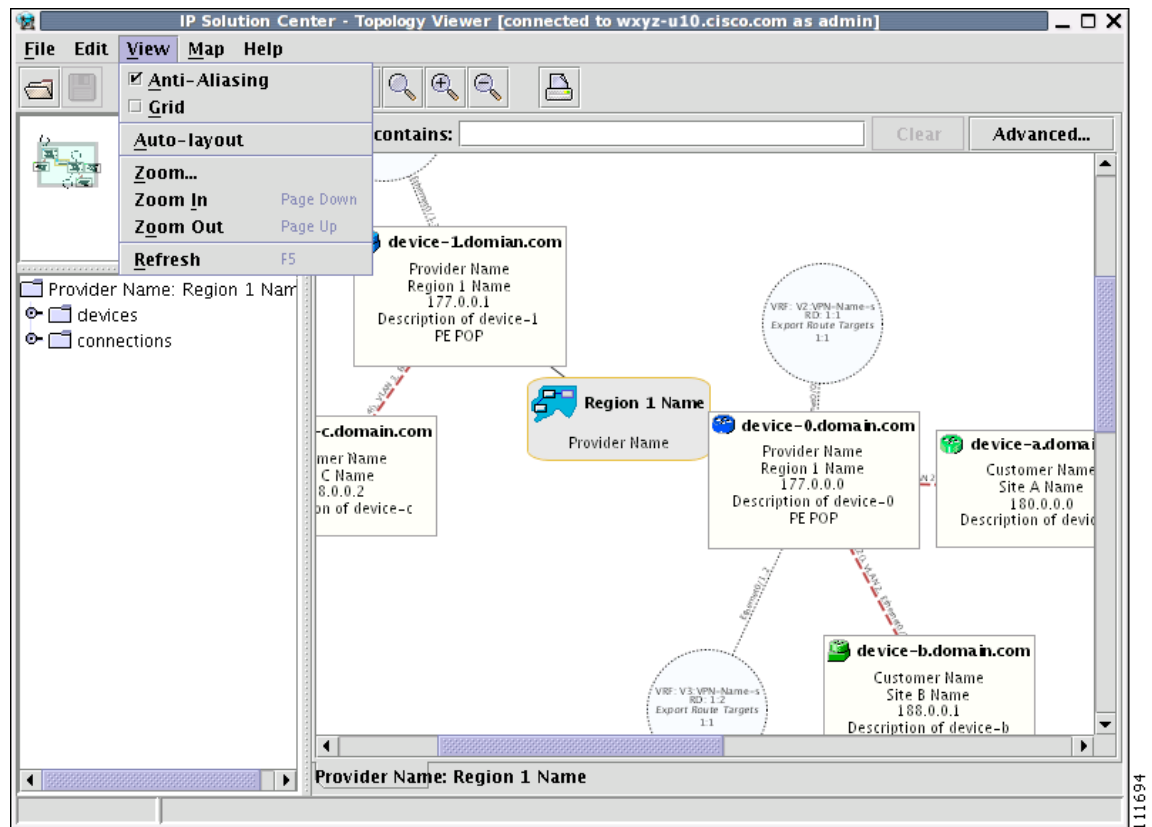
Types of Views

There are three view panes in the topology application and they are described in the following sections:

- **VPN View**, [page 3-15](#), shows connectivity between devices in a VPN
- **Logical View**, [page 3-19](#), shows connectivity between PEs and CPEs in a region
- **Physical View**, [page 3-22](#), shows physical devices and links for PEs in a region.

The view attributes can be changed using the **View** menu, as shown in Figure 3-10.

Figure 3-10 The View Menu



The **View** menu contains the following menu items:

- **Anti-Aliasing**—When drawing a view, this creates smoother lines and a more pleasant appearance at the expense of performance.
- **Grid**—Activates a magnetic grid. The grid has a 10 by 10 spacing and can be used to help align nodes in a view.
- **Auto-Layout**—Generates an automatic layout of nodes in a view. If selected, the program tries to find the most presentable arrangement of nodes.
- **Zoom**—Opens a dialog where the desired magnification level can be specified.
- **Zoom In**—Increases the magnification level.
- **Zoom Out**—Decreases the magnification level.
- **Refresh**—Regenerates the view. This is especially useful if the data in the repository changes. To see an updated view, select **Refresh** or click the Refresh toolbar button.

VPN View

The VPN view shows connectivity between devices forming a given VPN. To activate the VPN view, use the following steps:

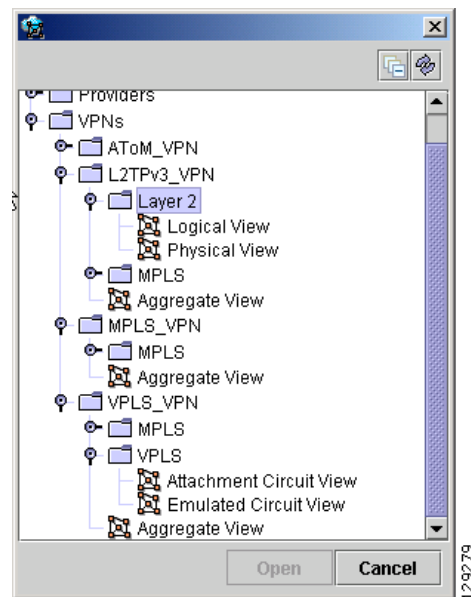
Step 1 In the menu bar, select **File > Open**.

or

click the **Open** button in the tool bar.

The Folder View window in [Figure 3-11](#) appears displaying a directory tree with available VPNs.

Figure 3-11 Folder View



Step 2 Navigate to the desired VPN's folder, select the folder, and click **Open**. This opens the desired folder to display any logical and physical views associated with that VPN.

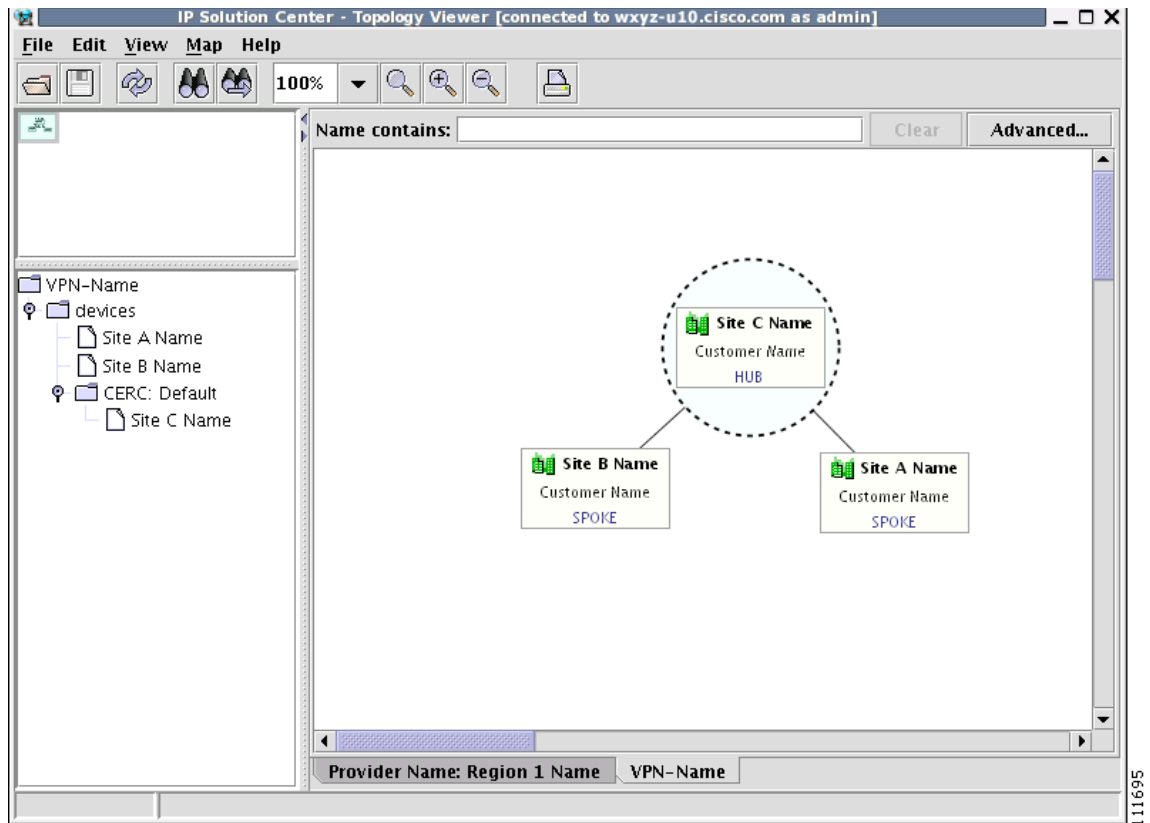
Step 3 Click a logical or a physical view item in the folder tree. The logical view minimizes the amount of detail and shows connectivity between customer devices. The physical view reveals more about the physical structure of the VPN. For example, for MPLS it shows connectivity between customer and provider devices and the core of the provider.

Aggregate View

The Aggregate View, as shown in [Figure 3-12](#), “[Aggregate View](#),” shows connectivity between all customer devices, regardless of the type of technology used to connect them.

A single view might show a combination of MPLS, Layer 2, VPLS, and IPsec VPNs (**IPsec is not supported in this release.**). For MPLS and IPsec, only the Customer Premises Equipment devices (CPEs) are shown.

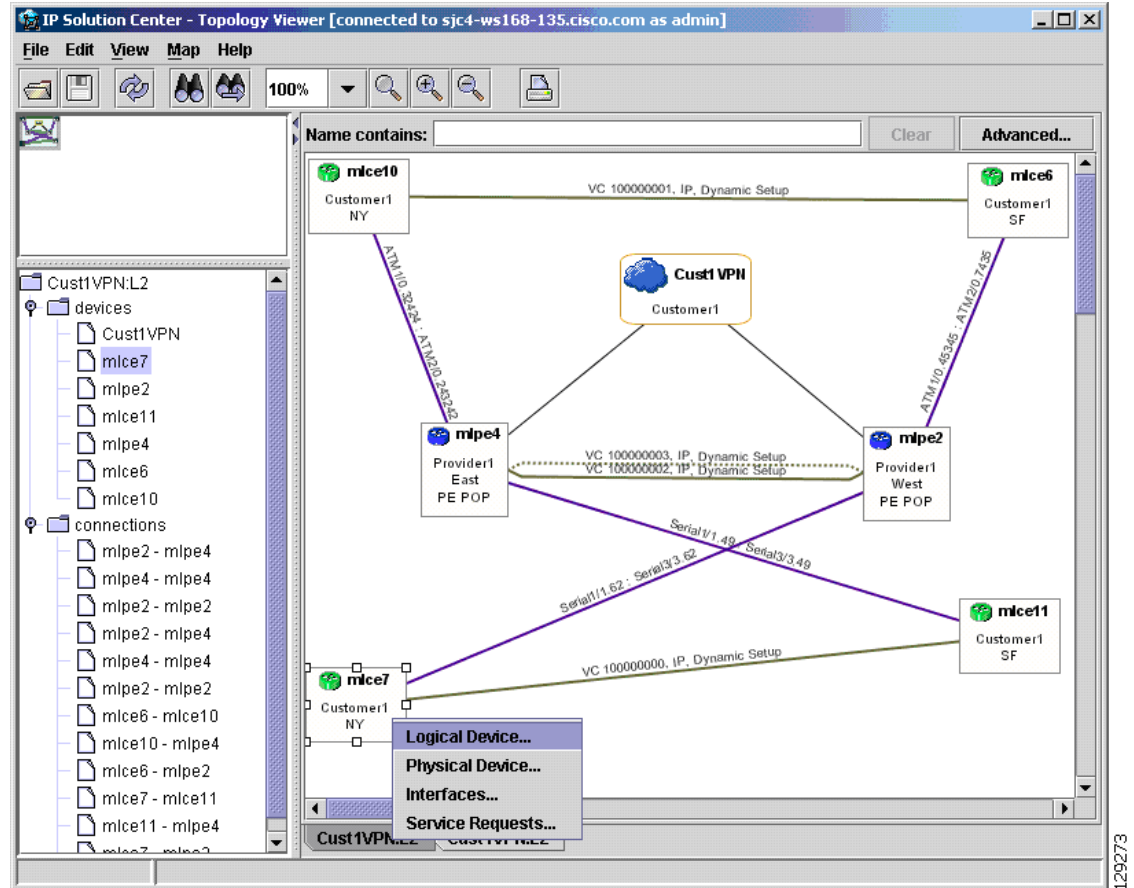
Figure 3-12 Aggregate View



The Layer 2 VPN might in addition to CPEs show connectivity between Customer Location Edge devices (CLEs) or Provider Edge devices (PE). For VPLS, you see connectivity between CPEs. For missing CPEs, you see connectivity to PEs.

In MPLS Layer 2 VPN, the topology displays Virtual Circuit (VC) with MPLS core (as MPLS string) but with L2TPv3, the topology will display Virtual Circuit (VC) with IP core (as IP string) as shown in [Figure 3-13](#).

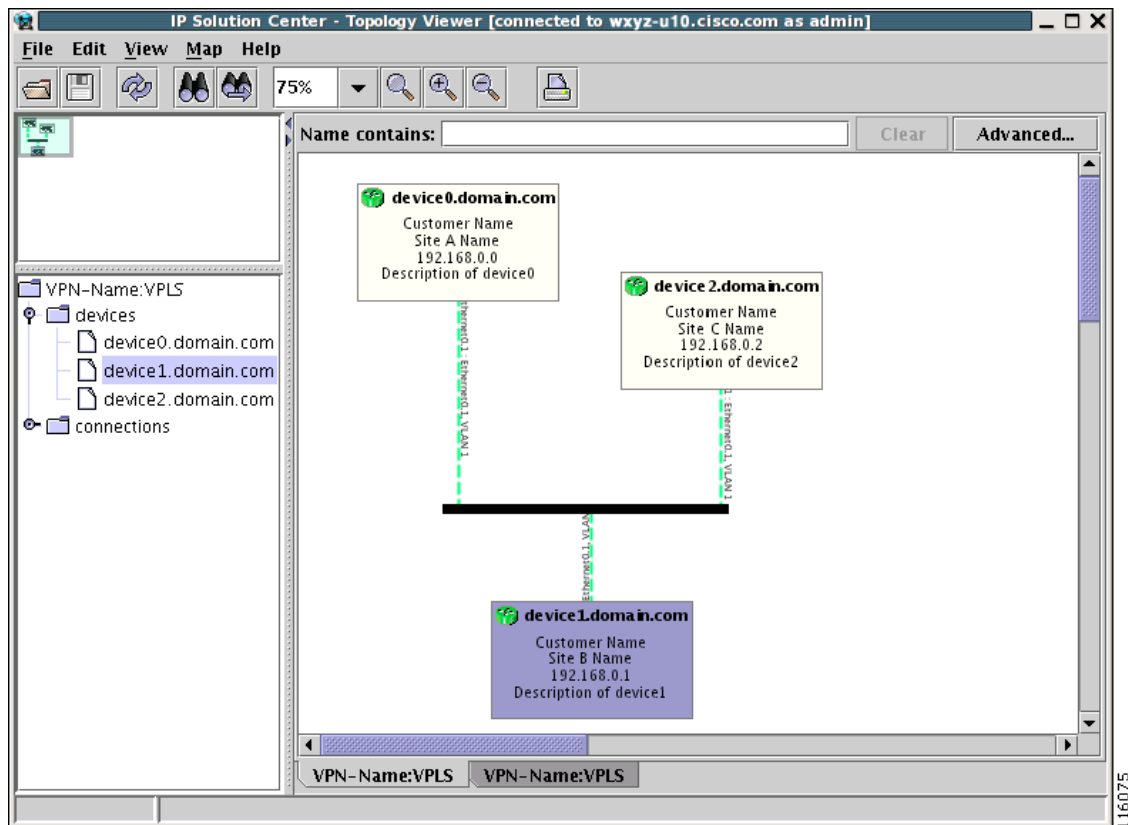
Figure 3-13 Virtual Circuit with IP Core



VPLS Topology

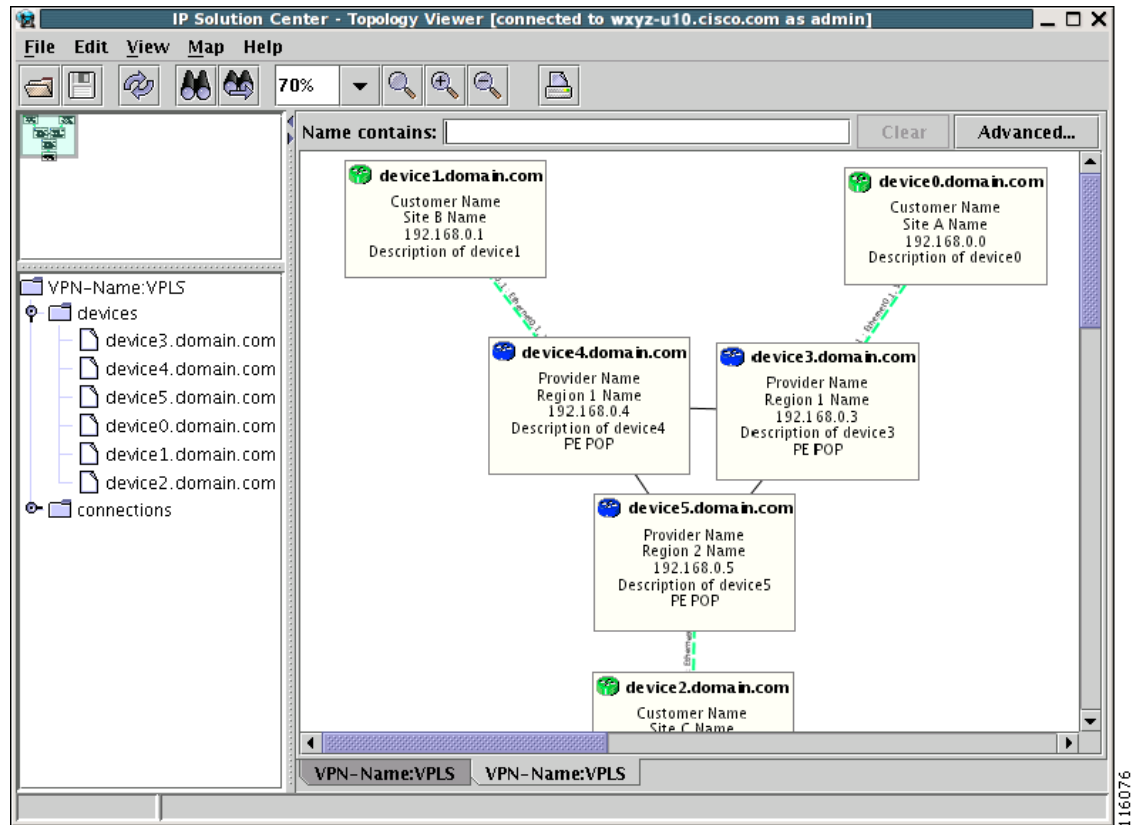
In the case of a VPLS topology, you can access an Attachment Circuit View or an Emulated Circuit View. The Attachment Circuit View corresponds to a logical view in other types of VPNs. It shows customer devices connected to a virtual private LAN, as shown in Figure 3-14, “Attachment Circuit View.”

Figure 3-14 Attachment Circuit View



The Emulated Circuit View shows the physical connectivity details omitted in the Attachment Circuit View. Connectivity between provider devices and customer devices connected to provider devices, as shown in [Figure 3-15, “Emulated Circuit View.”](#)

Figure 3-15 Emulated Circuit View



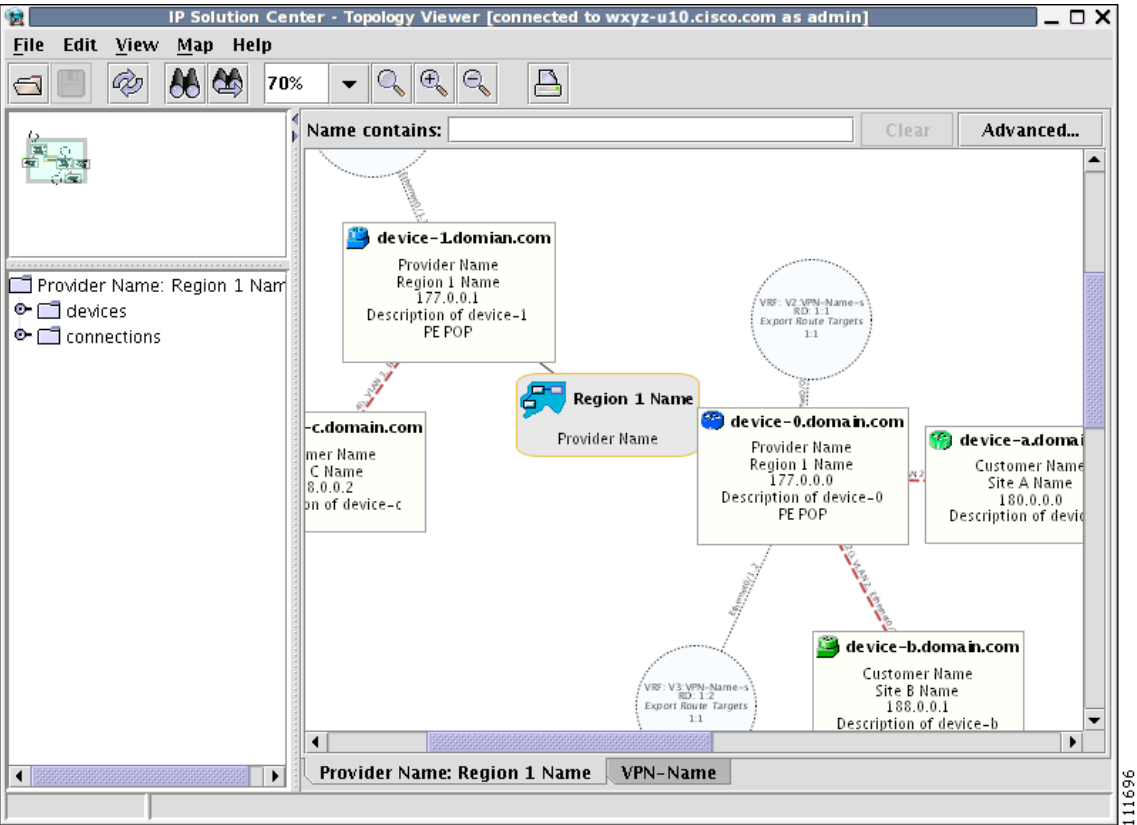
Logical View

The logical view shows connectivity, created through service requests, between PEs and CPEs of a given region.

To activate the logical view, use the following steps:

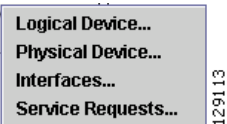
- Step 1** In the menu bar, select **File > Open**.
or
click the **Open** button in the tool bar.
The Folder View window in [Figure 3-11](#) appears.
 - Step 2** Navigate to the desired VPN's folder and double-click on the desired folder. Any logical and physical views associated with that VPN are displayed.
 - Step 3** To open the logical view for the selected VPN, do one of the following:
Single-click the **Logical View** icon and click **Open**
or
Double-click the **Logical View** icon.
- This creates a logical view for the chosen VPN, as shown in [Figure 3-16](#).

Figure 3-16 Logical View

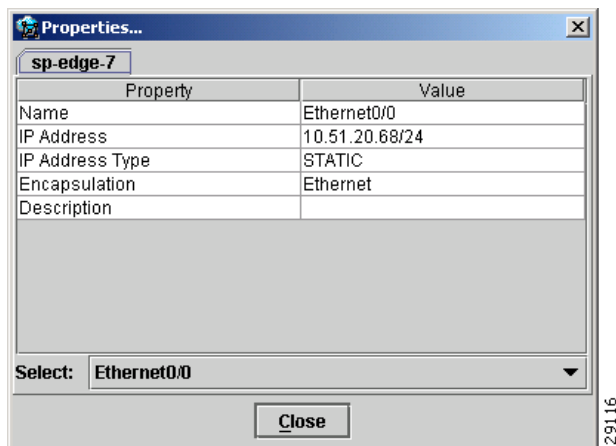


In a created view, the node, usually located in the center of the graph, is the node representing a given region of a provider. The node is annotated with the name of the region and the name of the provider. Each node directly connected to the regional node represents a PE. The icon of a node depends on the type and the role of the device it represents (see the “Conventions” section on page 3-9). Each PE is annotated with the fully-qualified device name, provider name, region name, management IP address, description, and role. A right-click on a node displays the details of the logical and physical device, interfaces, and service requests (SR) associated with the node, as shown in Figure 3-17. For the regional node, details are shown in a tabulated form.

Figure 3-17 Device Properties



The various node and link properties are described in detail in Viewing Device and Link Properties, page 3-23. Likewise, you can right-click on a link to learn about its link properties. For example, when selecting Interfaces... for a sample serial link, a Properties window like the one in Figure 3-18 appears.

Figure 3-18 Interface Details Table

Each PE can be logically connected to one or more CPEs. Such connections are created by either MPLS VPN links, Layer 2 Logical Links, or IPsec service request tunnels (**IPsec is not supported in this release.**). Each such connection is represented by an edge linking the given PE to a CPE. If there are more connections between a particular PE and CPE, all of them are shown. Depending on the state of a connection, the edge is drawn using a solid line (for functioning connections), dotted line (for broken connections), or dashed line (for connections yet to be established).

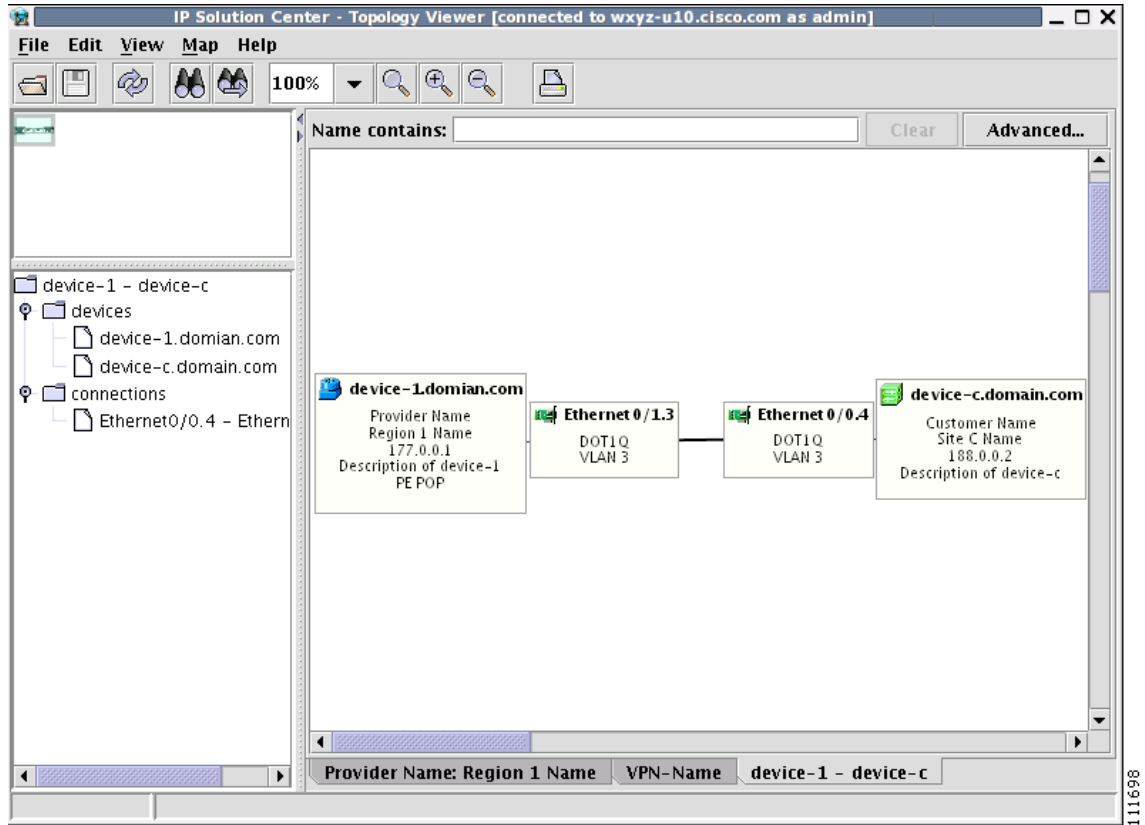
Depending on the connection type, the connection is drawn as described in [Table 3-3](#) and [Table 3-4](#). Each connection is annotated with the PE Interface Name (IP address), VLAN ID number, CPE Interface Name (IP address).

In the Overview area, a direct connection is drawn between a CPE and a PE, even if a number of devices are forming such a connection.

For more about viewing device properties, see [Viewing Device and Link Properties](#), page 3-23.

To view the details of a connection, right-click on it and select the **Expand** option from a pop-up menu. The expanded view, displayed in a new tab, shows all devices and interfaces making a given PE to CPE connection, as shown in [Figure 3-19](#).

Figure 3-19 Detailed Connection View



Physical View

A physical view shows all named physical circuits defined for PEs in a given region. Each named physical circuit is represented as a sequence of connections leading from a PE through its interfaces to interfaces of CLEs or CPEs. All physical links between PEs of a given region and their CLEs or CPEs are shown. Since physical links are assumed to be in a perfect operational order, edges are always drawn with solid lines.

To activate the physical view, use the following steps:

- Step 1** In the menu bar, select **File > Open**.
or
click the **Open** button in the tool bar.
The Folder View window in [Figure 3-11](#) appears.
- Step 2** Navigate to the desired VPN's folder and double-click on the desired folder. Any logical and physical views associated with that VPN are displayed.

Step 3 To open the physical view for the selected VPN, do one of the following:

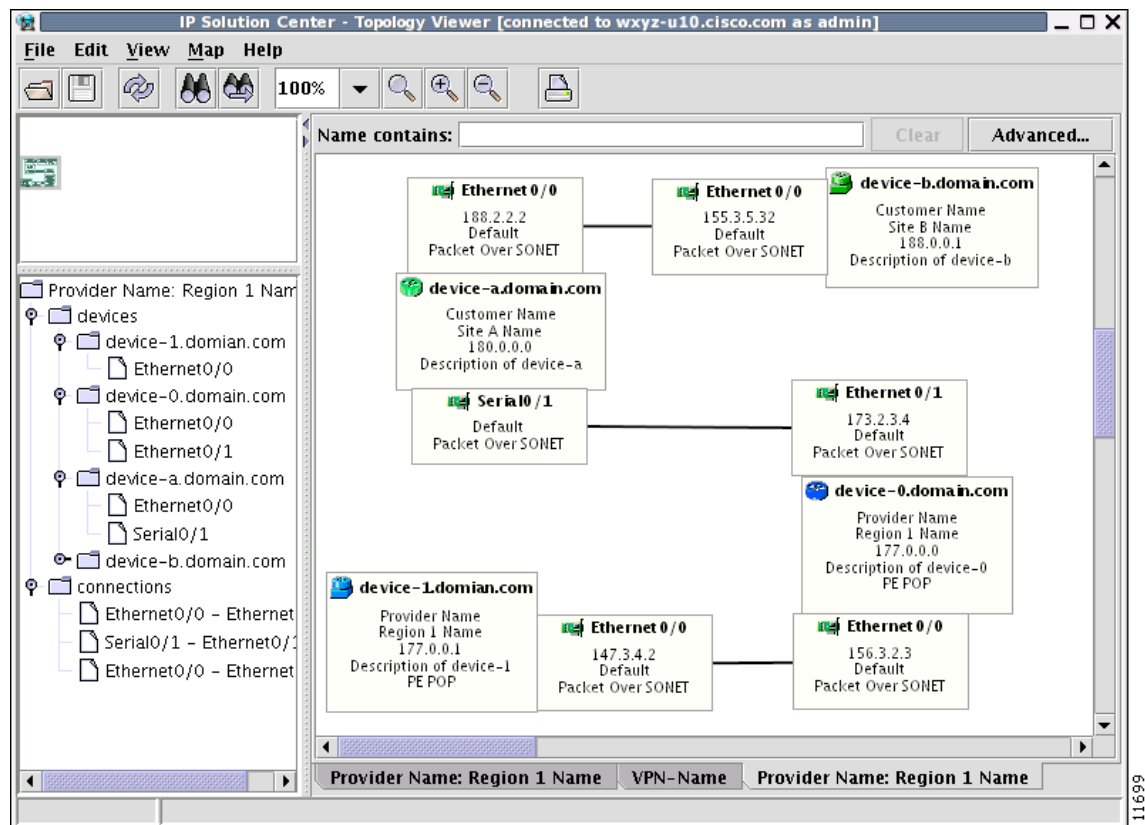
Single-click the **Physical View** icon and click **Open**

or

Double-click the **Physical View** icon.

This creates a physical view for the chosen VPN, as shown in [Figure 3-20](#).

Figure 3-20 Physical View



In this view, each device is connected with a thin line to the interfaces it owns. Interfaces are connected to other interfaces with thick lines. If there is more than one connection between two interfaces, they are spaced to show all of them.

The tree shows devices and connections. Each device can be a folder, holding all interfaces connected to it.

Viewing Device and Link Properties

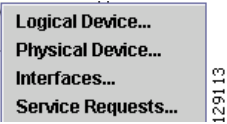
In the logical view, you can view the properties of both devices and links. In the physical view, only properties of physical devices are accessible.

Thus, device properties can be viewed in both the logical and physical views.

Device Properties

To view the properties of a device, right-click the device. The Device Properties menu in [Figure 3-17](#) appears.

Figure 3-21 Device Properties



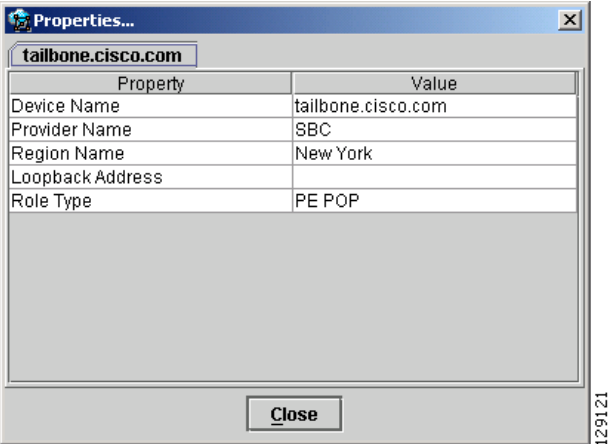
The following properties are available:

- Logical Device...**—View the logical properties of the device.
- Physical Device...**—View the physical properties of the device.
- Interfaces...**—View interface properties of the device.
- Service Requests...**—View service request properties associated with the device.

Logical Device

When right-clicking a device and selecting **Logical Device...**, the logical device properties window in [Figure 3-22](#) appears.

Figure 3-22 Logical Device Properties



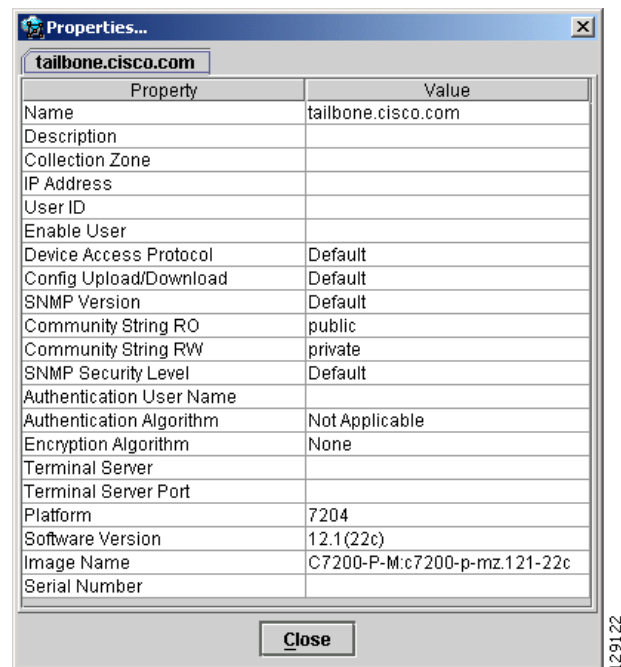
The logical properties window displays the following information:

- Device Name**—Name of the device.
- Provider Name**—Name of the provider whom the device is serving.
- Region Name**—Name of the provider region.
- Loopback Address**—IP address of the loopback address.
- Role Type**—Role assigned to the device.

Physical Device

When right-clicking a device and selecting **Physical Device...**, the physical device properties window in [Figure 3-23](#) appears.

Figure 3-23 Physical Device Properties



The physical properties window displays the following information:

Name—Name of the device.

Description—User-defined description of the device.

Collection Zone—Collection zone for device data.

IP Address—IP address of the interface used in the topology.

User ID—User ID for the interface.

Enable User—Password for the interface.

Device Access Protocol—Protocol used to communicate with the device.

Config Upload/Download—Upload/download method for the configuration file.

SNMP Version—Simple Network Management Protocol (SNMP) version on the device.

Community String RO—**public** or **private**

Community String RW—**public** or **private**

SNMP Security Level—Simple Network Management Protocol (SNMP) security level.

Authentication User Name—User name for performing authentication on the device.

Authentication Algorithm—Algorithm used to perform authentication.

Encryption Algorithm—Encryption algorithm used for secure communication.

Terminal Server—Name of the terminal server.

Terminal Server Port—Port number used by the terminal server.

Platform—Hardware platform.

Software—IOS version or other management software on the device.

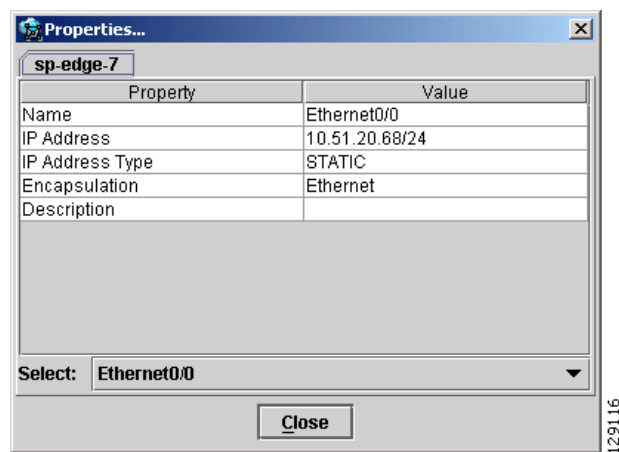
Image Name—Boot image for device initialization.

Serial Number—Serial number of the device.

Interfaces

When right-clicking a device and selecting **Interfaces...**, the interface properties window in [Figure 3-24](#) appears.

Figure 3-24 Device Interface Properties



The interface properties window displays the following information:

Name—Name of the device.

IP Address—IP address of the device.

IP Address Type—STATIC or DYNAMIC.

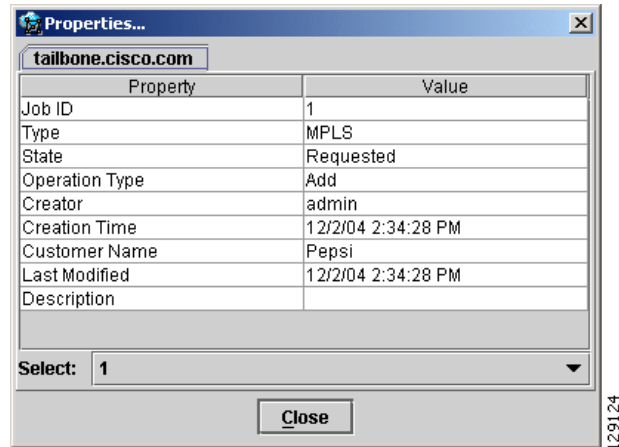
Encapsulation—Encapsulation used on the interface traffic.

Description—Description assigned to the interface, if any.

Select (link)—If a connection is attached to the interface, a drop-down list at the bottom of the window allows you to choose between the interfaces available on the device.

Service Requests

When right-clicking a device and selecting **Service Requests...**, the service request (SR) properties window in [Figure 3-25](#) appears.

Figure 3-25 Service Request Properties

The service request properties window displays the following information:

Job ID—SR identifier.

Type—Protocol type used in the SR.

State—SR state.

Operation Type—Encapsulation used on the interface traffic.

Creator—Description assigned to the interface, if any.

Creation Time—Date and time when the SR was created.

Customer Name—Name of customer associated with the SR.

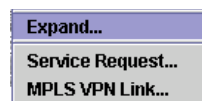
Last Modified—Date and time when the SR was last modified.

Description—User-defined description of the SR.

Select (SR)—If more than one SR is associated with the interface, the drop-down list at the bottom of the window allows you to choose between these SRs.

Link Properties

To view the properties of a given link, right-click the link. The Link Properties menu in [Figure 3-26](#) appears.

Figure 3-26 Link Properties

The following options are available:

Expand...—View link details, including devices local to the link not shown in the general topology.

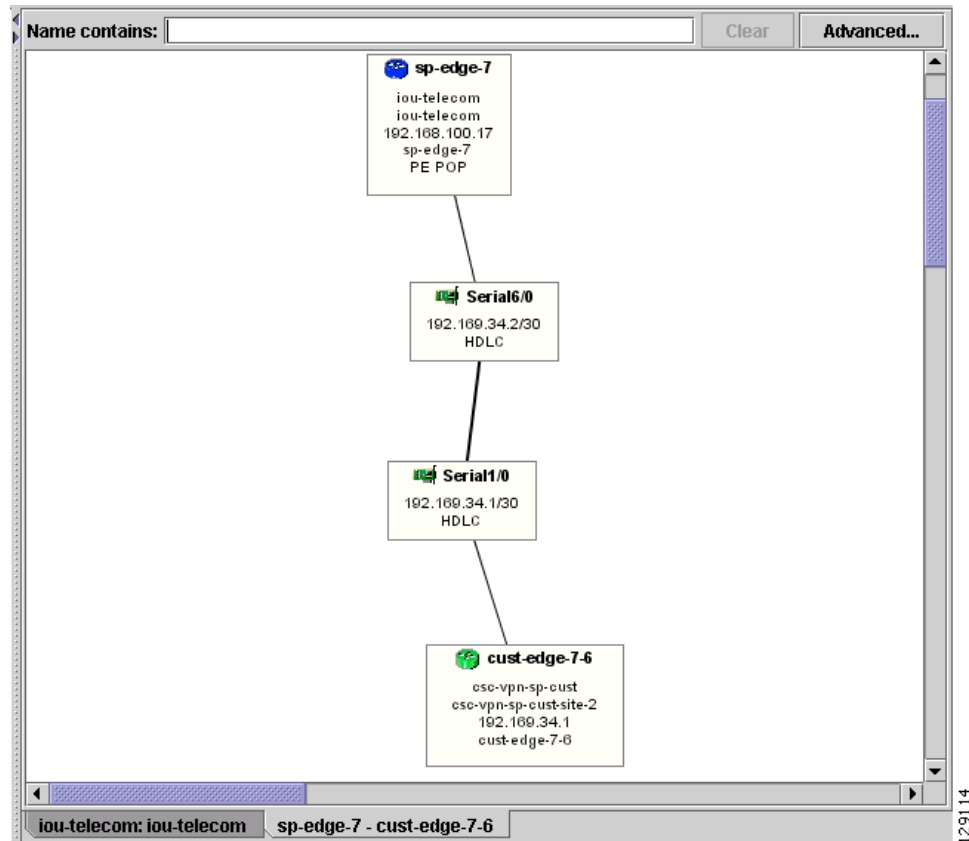
Service Request...—View service request properties associated with the link.

MPLS VPN...—View the MPLS VPN properties of the link. Other link protocol properties than MPLS VPN are currently not available.

Expand

When right-clicking a link and selecting **Expand...**, the Topology Display will display any devices and connections local to that link. An Expand Link window similar to the one in [Figure 3-25](#) will appear.

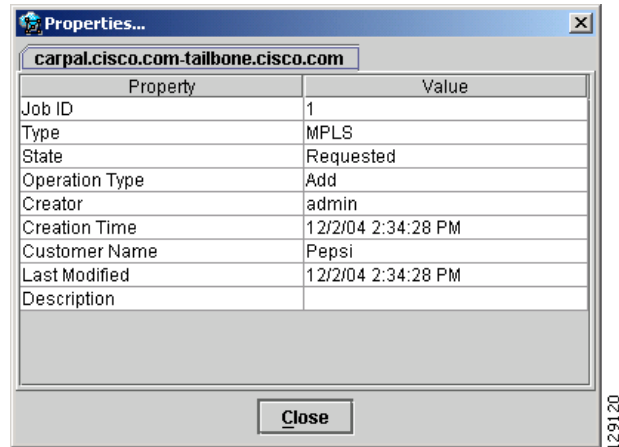
Figure 3-27 Expand Link



Properties information for devices and links can only be obtained in the master view as described earlier in this section.

Service Request

When right-clicking a link and selecting **Service Requests...**, the service request (SR) properties window in [Figure 3-28](#) appears.

Figure 3-28 Link Service Request Properties

The service request properties window displays the following information:

Job ID—SR identifier.

Type—Protocol type used in the SR.

State—SR state.

Operation Type—Encapsulation used on the interface traffic.

Creator—Description assigned to the interface, if any.

Creation Time—Date and time when the SR was created.

Customer Name—Name of customer associated with the SR.

Last Modified—Date and time when the SR was last modified.

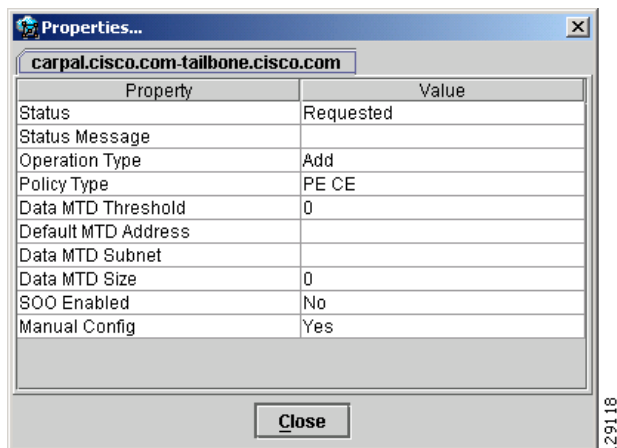
Description—User-defined description of the SR.

Select (SR)—If more than one SR is associated with the interface, the drop-down list at the bottom of the window allows you to choose between these SRs.

MPLS VPN

When right-clicking a link that is configured for MPLS VPN and selecting **MPLS VPN...**, the MPLS VPN properties window in [Figure 3-29](#) appears.

Figure 3-29 Link MPLS VPN Properties



The service request properties window displays the following information:

Status—Status of the MPLS VPN link.

Status Message—Displays any error or warning messages.

Operation Type—MPLS operation type.

Policy Type—The policy type applied to the link.

Data MTD Threshold—Memory Technology Driver (MTD) data threshold.

Default MTD Address—Default MTD IP address.

Data MTD Subnet—Data MTD subnet.

Data MTD Size—Data MTD size.

SOO Enabled—Yes or No.

Manual Config—Yes or No.

Filtering and Searching

On large graphs, the amount of detail can be overwhelming. In such cases, filtering might help eliminate unnecessary details, while searching can lead to a prompt location of a device you want to examine further.

Both advanced filtering and searching use the same dialog to enter conditions on nodes to be either filtered or located. The filtering area also allows you to quickly filter viewed objects by name.

Filtering

The topology view can be filtered in two ways, simple and advanced.

Simple Filtering

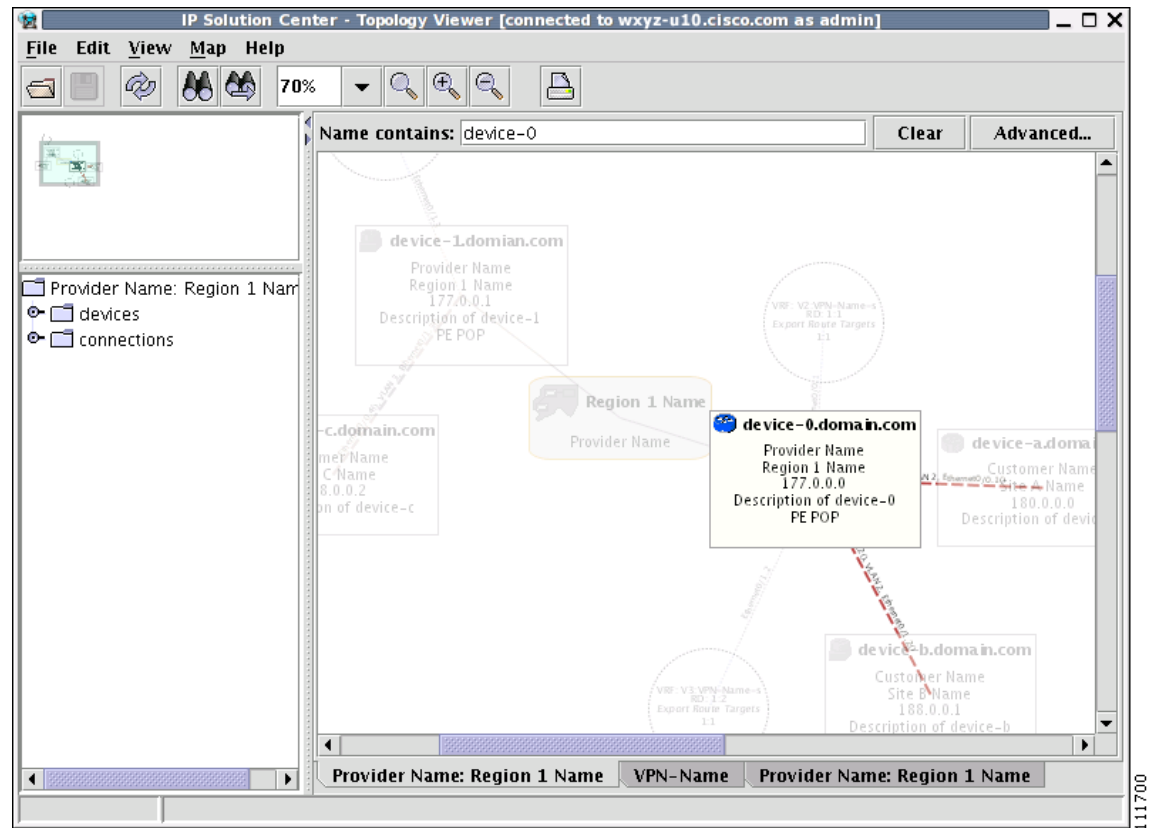
To perform simple filtering of the view, do as follows:

-
- Step 1** Enter a string in area (4) of the main window, as shown in [Figure 3-8 on page 3-12](#).

Step 2 Press **Enter** to dim all objects whose name does not contain the specified string.

For example, to locate nodes that contain string **router** in their name you would enter **router** in area (4) and click **Enter**. All objects whose name does not contain the entered string are dimmed, as shown in Figure 3-30.

Figure 3-30 Physical View with Dimmed Nodes



Note

Regular expressions are supported but only in the advanced dialog (click **Advanced...** button). For example, by entering `^foo.*a`, you only request nodes that have names starting with "foo" followed by arbitrary characters and containing the letter 'a' somewhere in the name. The regular expressions must follow the rules defined for Java regular expressions.

Advanced Filtering

To perform advanced filtering, do as follows:

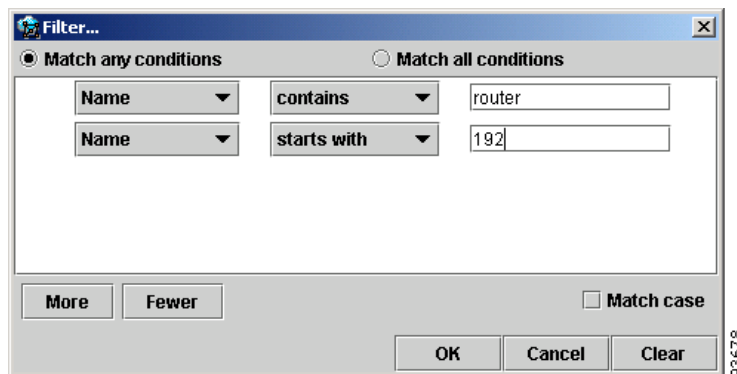
- Step 1** Open the advanced filtering dialog by clicking the **Advanced...** button. The Advanced Filter dialog appears, as shown in Figure 3-31.
- Step 2** Make the desired filtering elections.

The dialog allows you to enter one or more conditions on filtered nodes. The first drop-down menu allows you to specify the attribute by which the filtering is performed. The second allows you to decide how the matching between the value of the attribute and text entered in the third column is performed.

The following matching modes are supported from the drop-down menu:

- **contains**—The attribute value is fetched from the device and it is selected if it contains the string given by you. The string can be located at the start, end, or middle of the attribute for the match to succeed. For example, if the pattern is **cle** the following values match it in the **contains** mode: **clean**, **nucleus**, **circle**.
- **starts with**—The value of the attribute must start with the string given by you. For example, if the pattern is **foot**, **footwork** matches, but **afoot** does not.
- **ends with**—This is the reverse of the **starts with** case, when a given attribute matches only if the specified pattern is at the end of the attribute value. In this mode, for example, the pattern **foot** matches **afoot** but not **footwork**.
- **doesn't contain**—In this mode, only those strings that do not contain the given pattern match. The results are opposite to that of the **contains** mode. For example, if you specify **cle** in this mode, **clean**, **nucleus**, and **circle** are rejected, but **foot** is deemed to match, because it does not contain **cle**.
- **matches**—This is the most generic mode, in which you can specify a full or partial expression that defines which nodes you are interested in.

Figure 3-31 Advanced Filter dialog



By clicking one of the two radio buttons, **Match any conditions** or **Match all conditions**, you can request that any or all of the conditions are matched. In the first case, you can look for devices where, for example, the name contains **cisco** and the management IP address ends with **204**. When all conditions must be met, it is possible to look for devices that, for example, have a given name and platform.

Click **More** or **Fewer** to add more rows of conditions or remove existing rows of conditions.

By default, all matches are performed without regard for upper or lower case. However, in some cases it is beneficial to have a more exact matching that takes the case into account. To do so, select the **Match case** check box.

Step 3 Click **OK** to start the filtering process. Click **Cancel** to hide the dialog without any changes to the state of the filters.

The **Clear** button allows you to clear all conditions. Clicking **Clear** followed by **OK** effectively removes all filtering, restoring all nodes to their default brightness level. If filtering is active, the same can be achieved by clicking **Clear** in area (4) of the main window, as shown in [Figure 3-8 on page 3-12](#).

Searching

Searching can be conducted by using the menus or the tool bar. To perform a search, do as follows:

Step 1 Select **Find** in the **Edit** menu

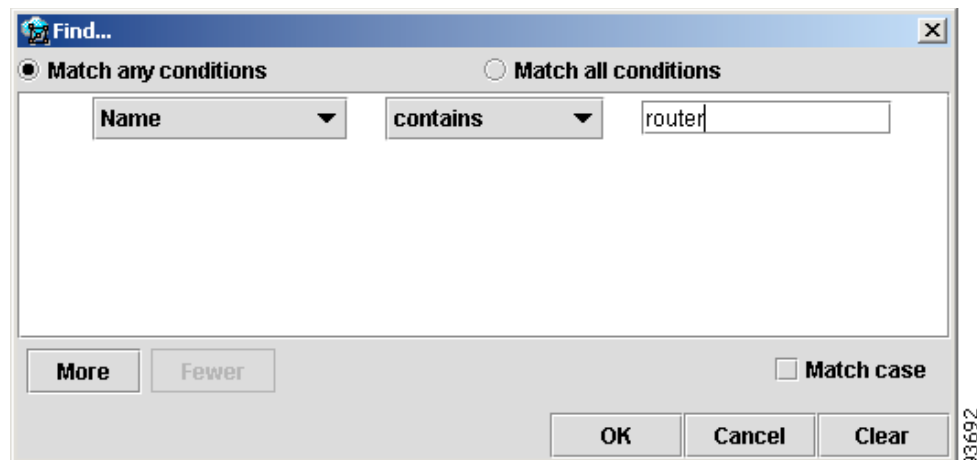
or

Click the **Find** icon in the main toolbar.

Both approaches bring up the same dialog box, as shown in [Figure 3-32](#).

Again, you can enter one or more conditions to locate the node.

Figure 3-32 Find Dialog Box



Step 2 Make the desired filtering selections. Match modes, case check box, and the radio button are used as described under [Advanced Filtering, page 3-31](#), as shown in [Figure 3-31](#).

Step 3 Click **OK** to start searching for the first node that matches the given criteria. If found, the node is highlighted and the view is shifted to make it appear in the currently viewed area of the main window.

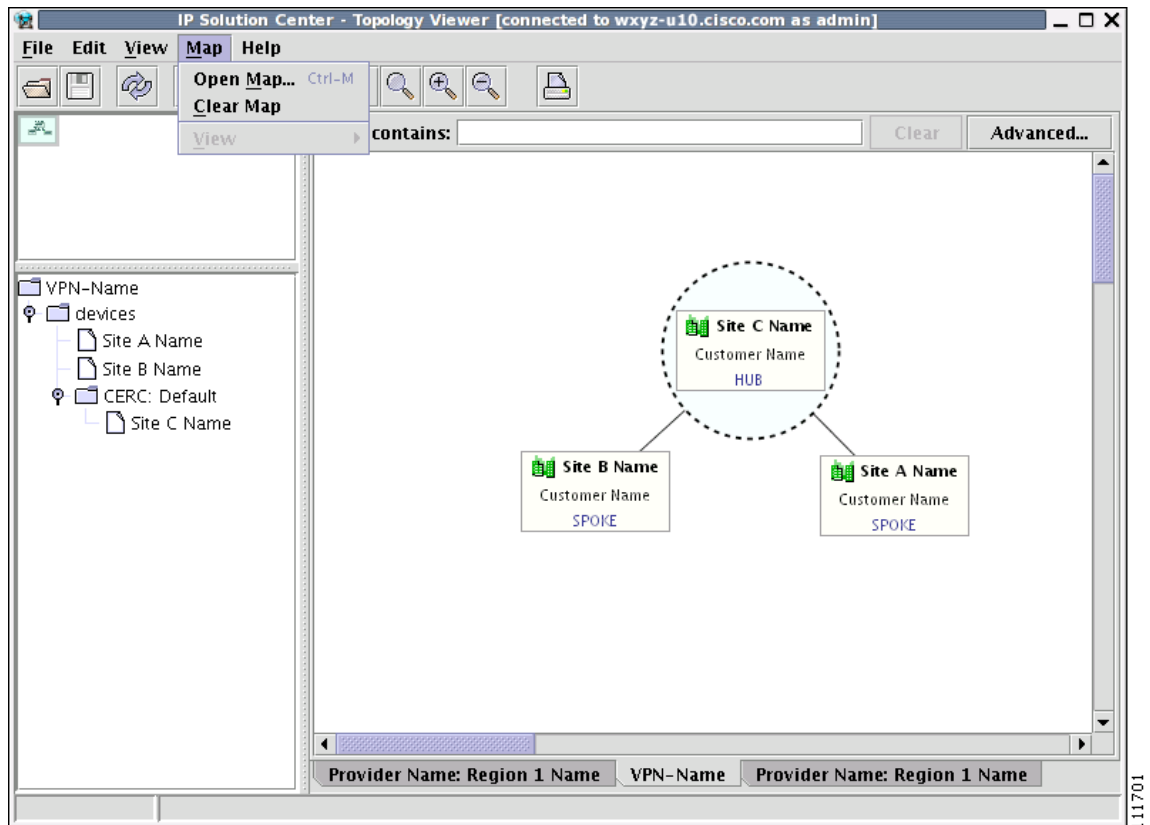
Step 4 After the first search, press **F3** or click the **Find Again** button to repeat the search. If more than one node matches the condition the **Find Again** function highlights each one of them. If no nodes match the entered criteria, the **Object Not Found** dialog box appears.

Using Maps

You can associate a map with each view. Currently, the topology viewer only supports maps in the Environmental Systems Research Institute, Inc. (ESRI) shape format. The following sections describe how to load maps and selectively view map layers and data associated with each map.

The map features are accessed from the **Map** menu shown in [Figure 3-33](#).

Figure 3-33 The Map Menu



The **Map** menu contains the following menu items:

- **Open Map...** Loads a map into the application
- **Clear Map** Clears the active map from the current view
- **View** Allows you to select which layers in the map should be displayed (for example, country, state, city).

Loading a map

You might want to set a background map showing the physical locations of the displayed devices. To load a map, use the following steps:

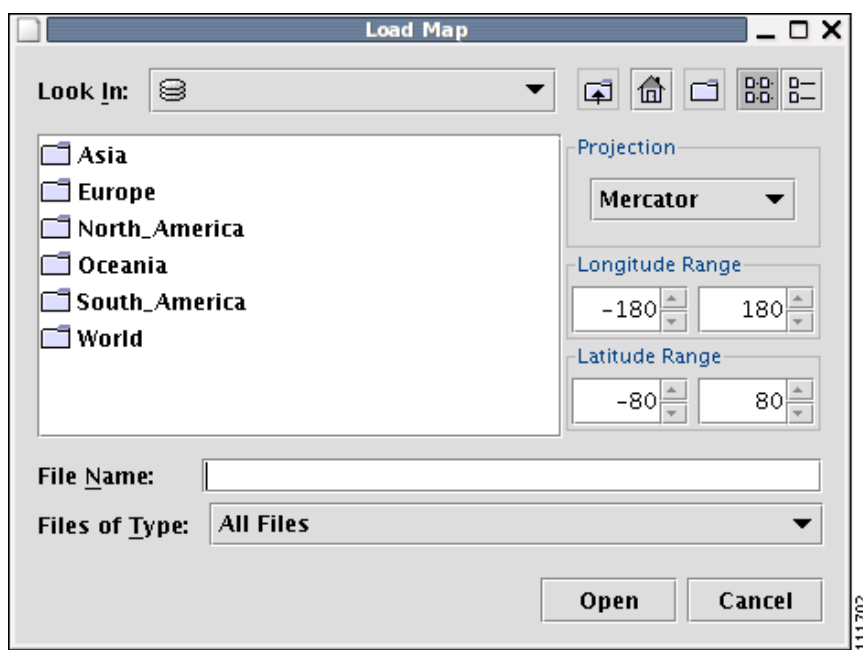
Step 1 In the menu bar, select **Map > Open Map....**

or

Press **Ctrl-M**

Providing the web map server is running and operational, the Load Map window appears, as shown in Figure 3-34.

Figure 3-34 Load Map Window



Step 2 Make your selections in the Load Map window.

The right-hand side of the window contains a small control panel, which allows you to select the projection in which a map is shown. A map projection is a projection that maps a sphere onto a plane. Typical projections are Mercator, Lambert, and Stereographic.

For more information on projections, consult the Map Projections section of Eric Weisstein's World of Mathematics at:

<http://mathworld.wolfram.com/topics/MapProjections.html>

For each projection, you can also select the region of the map to be shown. In most cases, the predefined values should be sufficient. The top level the file hierarchy should contain folders for all major regions, such as Europe, North America, Oceania, and so on.

If desired, make changes to the settings in the **Longitude Range** and **Latitude Range** fields.

Step 3 Navigate to the desired folder.

Each folder can contain either complete maps or folders for countries. Each map is clearly distinguished with the **Map** icon.

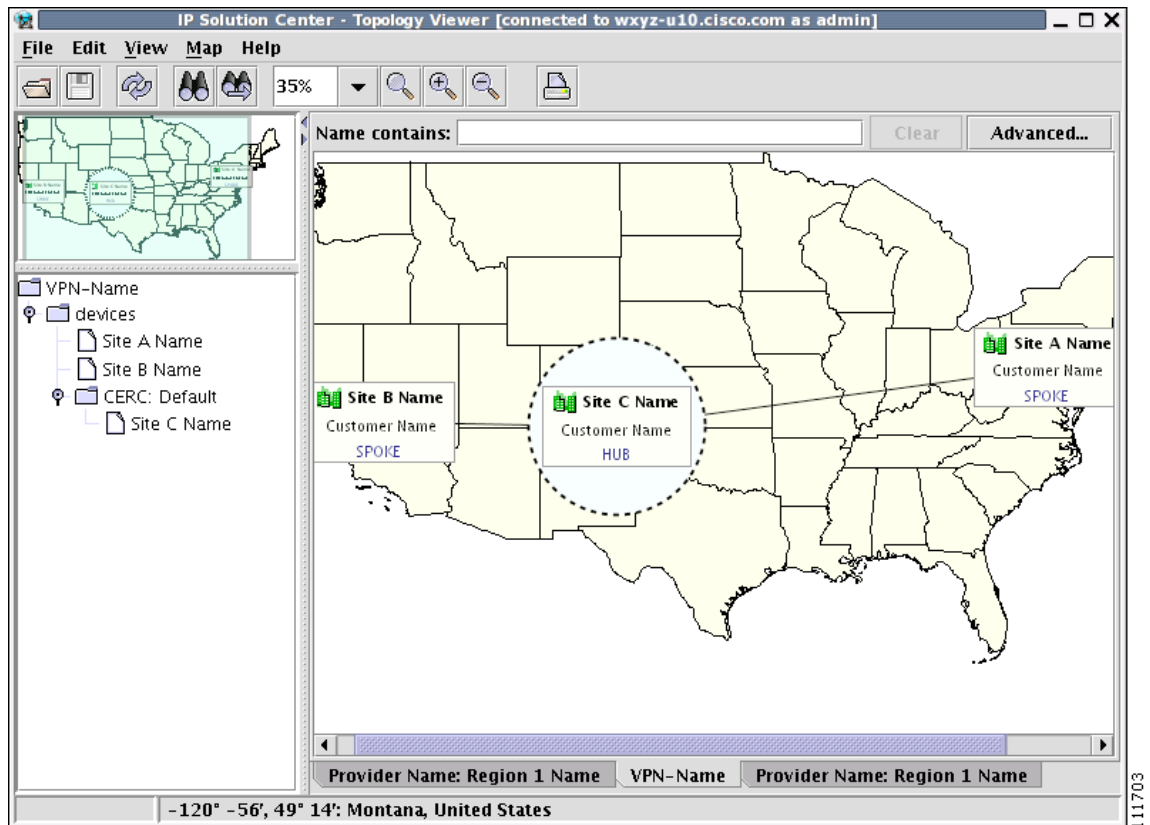
Step 4 Select a map file and click **Open** to load the map.

Selecting the map file and clicking the **Open** button starts loading it. Maps can consist of several components and thus a progress dialog is shown informing you which part of the map file is loaded.

Layers

Each map can contain several layers. For example most country maps have country, region, and city layers, as shown in [Figure 3-35](#).

Figure 3-35 Map Layers



After a map is loaded, the **View** submenu of the **Map** menu is automatically populated for you. A name of each available layer is shown together with the check box indicating visibility of the layer. If a given map shows too many details, you can turn off some or all layers by deselecting the corresponding check box(es). The same submenu can be used to restore visibility of layers.

If an incorrect map is loaded or the performance of the topology tool is unsatisfactory with the map loaded, you can clear the map entirely. To do this, select **Clear Map** from the **Map** menu. Maps are automatically cleared if another map is loaded.

Consequently if you want just to load another map, there is no need to clear the existing map. The act of loading a new map does this.

Map data

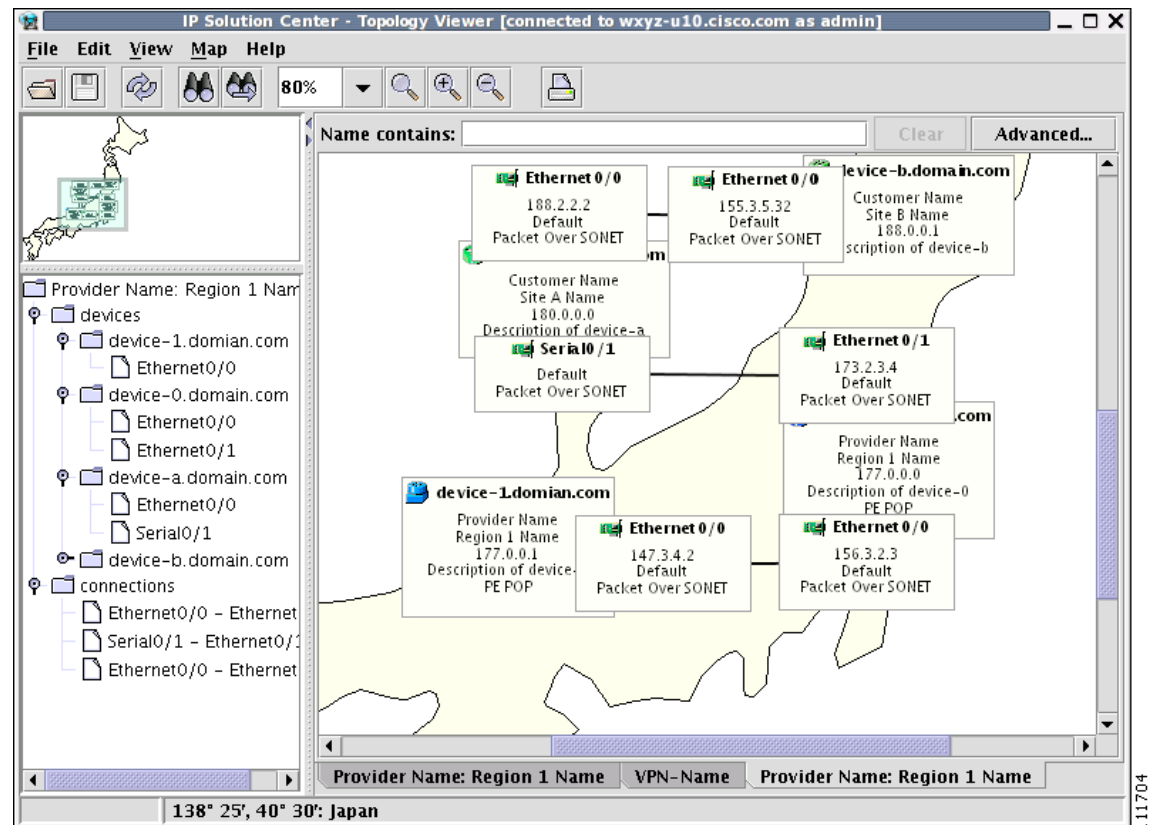
If map data files are successfully loaded with the map, the right field of the Status bar shows the longitude and latitude location of the cursor on the map. If map objects, such as cities, lakes, and so on, have data associated with them, their names are displayed after the longitude and latitude coordinates.

Node locations

After a map is successfully loaded, the view area is adjusted to fully accommodate it, as shown in [Figure 3-36](#). If nodes shown on the window had longitude and latitude information associated with them, they are moved to locations on the map corresponding to their geographical location. If not, their positions remain unchanged.

However, you can manually move them to the desired location and save the positions for future reference. The next time the image of a given network is loaded, node positions are restored and the map file is loaded.

Figure 3-36 Physical View with a Map of Japan



Adding new maps

You might want to add your own maps to the selection of maps available to the topology application. This is done by placing a map file in the desired directory within the ISC installation. To make this example more accessible, assume that you want to add a map of Toowong, a suburb of Brisbane, the capital of Queensland. The first step to do so is to obtain maps from a map vendor. All maps must be in the ESRI shape file format (as explained at the web site: <http://www.esri.com>). In addition, a data file might accompany each shape file. Data files contain information about objects whose shapes are contained within the shape file. Let us assume that the vendor provided four files:

- toowong_city.shp
- toowong_city.dbf
- toowong_street.shp
- toowong_street.dbf

We must create a map file that informs the topology application about layers of the map. In this case we have two layers: a city and a street layer. The map file, say, Toowong.map, would thus have the following contents:

```
toowong_city
toowong_street
```

It lists all layers that create a map of Toowong. The order is important, as the first file forms the background layer, with other layers placed on top of the preceding layers.

Having obtained shape and data files and having written the map file, decide on its location. As mentioned, Toowong is a suburb of Brisbane, located in Queensland, Australia. All map files must be located in or under the **\$ISC_HOME/resources/webserver/tomcat/webapps/ipsc-maps/data** directory. Since by default this directory contains a directory called **Oceania** intended for all maps from that region, simply create a path **Australia/Queensland/Brisbane** under the directory **Oceania**. Next, place all five files in this location. After this is done, the map is automatically accessible to the topology viewer.

Devices

Every network element that ISC manages must be defined as a device in the system. An element is any device from which ISC can collect information. In most cases, devices are Cisco IOS routers that function as edge routers in the IPsec VPN - **IPsec is NOT SUPPORTED in this release.** -, or as Provider Edge Routers (PEs) or Customer Edge Routers (CEs) in the MPLS VPN.



Note

To provision services with ISC, you must have IPv4 connectivity.

This section describes how to configure SSH, set up SNMP, manually enable an RTR responder, and create, edit, delete, and configure various types of supported devices. This section includes the following:

- [Configuring SSH, page 3-39](#)
- [Setting Up SNMP, page 3-41](#)
- [Manually Enabling RTR Responder on Cisco IOS Routers, page 3-43](#)
- [Accessing the Devices Window, page 3-44](#)
- [Creating a Device, page 3-45](#)

- [Editing a Device, page 3-73](#)
- [Deleting Devices, page 3-75](#)
- [Editing a Device Configuration, page 3-76](#)
- [E-mailing a Device's Owner, page 3-77](#)
- [Copying a Device, page 3-79](#)

Configuring SSH

ISC needs a mechanism to securely access and deploy configuration files on devices, which include routers, switches, Cisco VPN 3000 concentrators - **NOT SUPPORTED in this release.** -, and Cisco PIX Firewalls - **NOT SUPPORTED in this release.** -. And, to securely download a configlet and upload a configuration file from a device, SSH must be enabled.

The following sections describe how to configure SSH on a device.

Configuring SSH on Cisco IOS Routers

This Cisco IOS router configuration procedure assumes that the router's authentication database is stored locally on the router and not on a TACACS or RADIUS server.

The procedure for configuring SSH on a Cisco IOS router is as follows:.

	Command	Description
Step 1	Router# configure terminal	Enters global configuration mode.
Step 2	Router(config)# ip domain-name <i><domain_name></i>	Specifies the IP domain name.
Step 3	Router(config)# username <i><username></i> password <i><password></i>	Configures the user ID and password. Enter your ISC username and password. For example: username admin password iscpwd
Step 4	Router(config)# crypto key generate rsa	Generates keys for the SSH session.
Step 5	You will see the following prompt: Choose the size of the key modulus in the range of 360 to 2048 for your general purpose keys. How many bits in the modulus (nnn): Press Enter to accept the default number of bits.	Sets the number of bits.
Step 6	Router(config)# line vty 0 4	Enables SSH as part of the vty login transport.
Step 7	Router(config-line)# login local	The login local command indicates that the router stores the authentication information locally.
Step 8	Router(config-line)# transport input telnet ssh	Enables SSH transport.
Step 9	Router(config-line)# Ctrl+Z	Returns to Privileged Exec mode.
Step 10	Router# copy running startup	Saves the configuration changes to NVRAM.

Configuring SSH on VPN 3000 Concentrators

- NOT SUPPORTED in this release. -

The procedure for configuring SSH on a VPN 3000 concentrator is as follows:

-
- Step 1** Telnet to the VPN 3000 device through the console port. The command line appears.
 - Step 2** Select **Administration > Certificate Management > SSL Certificate**.
 - Step 3** Click **Generate**. The system uses parameters set on the Configuration > System > Management Protocols > SSL window and generates the certificate. The new certificate replaces any existing SSL certificate.
 - Step 4** If you must modify the SSH In and SSH Out Rules, select **Configuration > Policy Management > Traffic Management > Rules**. Select the rule you want to modify, and then click **Modify**.
 - Step 5** For SSH In and/or SSH Out, make any modifications that you require. Click **Apply** when you are finished making changes to a rule.
 - Step 6** Select **Configuration > Policy Management > Traffic Management > Filters**. You must assign the SSH In and SSH Out rules to the Public interface.
 - Step 7** Select Public from the **Filter List**.
 - Step 8** Click **Assign Rules to Filter**. The Configuration > Policy Management > Traffic Management > Assign Rules to Filter window appears.
 - Step 9** Select **SSH In** from the Available Filters list and then click << **Add**.
 - Step 10** Select **SSH Out** from the Available Filters list and then click << **Add**.
 - Step 11** Click **Done**.
 - Step 12** Go back to the main menu and then click **Logout**.
-

Configuring SSH on PIX Firewall Devices

- NOT SUPPORTED in this release. -

ISC needs a mechanism to securely deploy configuration files to PIX Firewall devices in the network.



Note

SSH permits up to 100 characters in a username, and up to 50 characters in a password.

To configure SSH on a PIX Firewall device, perform the following steps:

	Command	Description
Step 1	<code>Pix# configure terminal</code>	Enters global configuration mode.
Step 2	<code>Pix(config)# domain-name <domain_name></code>	Specifies the IP domain name.
Step 3	<code>Pix(config)# ca generate rsa key 1024</code>	Generates the RSA key pair for the SSH session. A modulus size of 1,024 bits is recommended for use with the Cisco IOS Software. Key generation could take several minutes.
Step 4	<code>Pix(config)# ca save all</code>	Saves the RSA key pair to Flash memory.

	Command	Description
Step 5	<code>Pix(config)# ssh <ip_address> <subnet_mask> <interface></code>	You can grant permission to one or more hosts to start an SSH session to the PIX Firewall through the specified interface (usually <code>outside</code> or <code>inside</code>). For example, with <code>ssh 128.107.128.108 255.255.255.255 outside</code> Also, you can permit all hosts in the specified subnet to establish an SSH session with the PIX Firewall through the specified interface. For example, <code>ssh 128.107.0.0 255.255.0.0 outside</code>
Step 6	<code>Pix(config)# write mem</code>	Saves the configuration changes.

When starting an SSH session, a dot (.) appears on the PIX Firewall console before the SSH user authentication prompt appears. For example:

```
pixfirewall(config)# .
```

The dot does not affect SSH functionality. The dot appears at the PIX Firewall console before authentication occurs when generating a server key or decrypting a message that uses private keys during an SSH exchange. These tasks can take up to two minutes or so. The dot is a progress indicator that verifies that the PIX Firewall is busy and not frozen.

Setting Up SNMP

To work with ISC, SNMP must be configured on each CPE device in the customer network. In ISC, SNMP is used to:

- collect from the Interface MIB
- provision and collect SLA data.

Two security models are available: SNMPv1/v2c and SNMPv3. [Table 3-5](#) identifies the combinations of security models and levels.

Table 3-5 SNMP Security Models and Levels

Model	Level	Authentication	Encryption	Description
v1/v2c	No Authentication/ No Encryption	Community String	No	Uses a community string match for authentication.
v3	No Authentication/ No Encryption	Username	No	Uses a username match for authentication.
v3	Authentication/ No Encryption	MD5 or SHA	No	Provides authentication based on the HMAC-MD5 or HMAC-SHA algorithms.
v3	Authentication/ Encryption	MD5 or SHA	DES	Provides authentication based on the HMAC-MD5 or HMAC-SHA algorithms, and provides DES 56-bit encryption in addition to authentication based on the CBC-DES (DES-56) standard.

SNMPv3 provides for both security models and security levels. A *security model* is an authentication strategy that is set up for a user and the group in which the user resides. A *security level* is the permitted level of security within a security model. A combination of a security model and a security level determines which security mechanism is employed when handling an SNMP packet.

The security features provided in SNMPv3 are as follows:

- Message integrity—Ensures that a packet has not been tampered with in-transit.
- Authentication—Determines the message is from a valid source.
- Encryption—Encoding the contents of a packet to prevent it from being read by an unauthorized source.

SNMPv3 objects have the following characteristics:

- Each user belongs to a group.
- The group defines the access policy for a set of users and determines the list of notifications its users can receive. The group also defines the security model and security level for its users.
- The access policy defines which SNMP objects can be accessed for reading, writing, or creation.

Setting Up SNMPv1/v2c on Cisco IOS Routers

To determine whether SNMP is enabled, and to set the SNMP community strings on a Cisco IOS router, perform the following steps for each router:

	Command	Description
Step 1	Router> enable Router> <enable_password>	Enters enable mode, and then enters the enable password.
Step 2	Router# show snmp	Check the output of the show snmp command to see whether the following statement is present: “SNMP agent not enabled.” If SNMP is not enabled, complete the steps in this procedure.
Step 3	Router# configure terminal	Enters global configuration mode.
Step 4	Router(config)# snmp-server community <userstring> RO	Sets the community read-only string.
Step 5	Router(config)# snmp-server community <userstring> RW	Sets the community read-write string.
Step 6	Router(config)# Ctrl+Z	Returns to Privileged Exec mode.
Step 7	Router# copy running startup	Saves the configuration changes to NVRAM.



Tip

The SNMP community strings defined in ISC for each target device must be identical to those configured on the device.

Setting SNMPv3 Parameters on Cisco IOS Routers

This section describes how to set the SNMPv3 parameters on Cisco IOS routers. SNMPv3 is only supported on IOS crypto images. For Authentication/Encryption, the IOS image must have DES56.

**Tip**

The SNMP users defined in ISC for each target device must be identical to those configured on the device.

To check the existing SNMP configuration, use these commands in the router terminal session:

- `show snmp group`
- `show snmp user`

To set the SNMPv3 server group and user parameters on a Cisco IOS router, perform the following steps.

**Note**

The group must be created first and then the user.

	Command	Description
Step 1	Router> <code>enable</code> Router> <code><enable_password></code>	Enters enable mode, then enter the enable password.
Step 2	Router# <code>configure terminal</code>	Enters global configuration mode.
Step 3	Router(config)# <code>snmp-server group</code> [<groupname> {v1 v2c v3 {auth noauth priv}}] [read <readview>] [write <writeview>] [notify <notifyview>] [access <access-list>]	The snmp-server group command configures a new SNMP group or a table that maps SNMP users to SNMP views. Each group belongs to a specific security level. Example: <code>snmp-server group v3auth v3 auth read vldefault write vldefault</code>
Step 4	Router(config)# <code>snmp-server user <username></code> [<groupname> remote <ip-address>] [udp-port <port>] {v1 v2c v3 [encrypted] [auth {md5 sha} <auth-password> [priv des56 <priv-password>]] [access <access-list>]}	The snmp-server user command configures a new user to an SNMP group. Example: <code>snmp-server user user1 v3auth v3 auth md5 user1Pass</code>
Step 5	Router(config)# <code>Ctrl+Z</code>	Returns to Privileged Exec mode.
Step 6	Router# <code>copy running startup</code>	Saves the configuration changes to NVRAM.

Manually Enabling RTR Responder on Cisco IOS Routers

**Note**

SNMP must be configured on the router.

To manually enable an RTR Responder on a Cisco IOS router, execute the following steps:

	Command	Description
Step 1	Router> <code>enable</code> Router> <code><enable_password></code>	Enters enable mode, and then enters the enable password.
Step 2	Router# <code>configure terminal</code>	Enters the global configuration mode.
Step 3	Router(config)# <code>rtr responder</code>	Enables the SA responder on the target router of SA Agent operations.
Step 4	Router(config)# <code>Ctrl+Z</code>	Returns to Privileged Exec mode.
Step 5	Router# <code>copy running startup</code>	Saves the configuration changes to NVRAM.

Accessing the Devices Window

The Devices feature is used to create, edit, delete, and configure devices, and e-mail the device owner. To access the Devices window, do the following:

- Step 1** Navigate **Service Inventory > Inventory and Connection Manager > Devices** to access the Devices window shown in [Figure 3-37](#).

Figure 3-37 *Devices List Window*



The Devices window contains the following:

- **Device Name** Lists the fully qualified host and domain name of the device. You can sort the list of devices by device name.
- **Management IP Address** Lists the management IP address or the IE2100 address. You can sort the list of devices by this field.
- **Type** Lists the type of the device. Types include: Cisco IOS Device, CatOs Device, Terminal Server, VPN 3000 - **NOT SUPPORTED in this release.** -, PIX Firewall - **NOT SUPPORTED in this release.** -, and IE2100.

In the Devices window, you can create, edit, delete, or configure devices or e-mail the device owner using the following buttons:

- **Create** Click to create new devices. Enabled only if no devices are selected.
- **Edit** Click to edit selected device (select device by clicking the corresponding box). Enabled only if a single device is selected.
- **Delete** Click to delete selected device (select device by clicking the corresponding box). Enabled only if one or more devices are selected.

- **Config** Click to change the selected device configuration (select device by clicking the corresponding box). Enabled only if a single device is selected.
- **E-mail** Click to send e-mail to the owner of selected device (select device by clicking the corresponding box). Enabled only if one or more devices are selected.

Creating a Device

From the Create window, you can define different types of devices.

To create a device, do the following:

- Step 1** Navigate **Service Inventory > Inventory and Connection Manager > Devices**.
- Step 2** Click the **Create** button.

The Create options appear, as shown in [Figure 3-38](#).

Figure 3-38 Create Options Window



The **Create** options include the following:

- **Catalyst Switch** A Catalyst device running the Catalyst Operating System.
- **Cisco IOS Device** Any router that runs the Cisco IOS. This includes Catalyst devices running Cisco IOS.
- **Terminal Server** A device that represents the workstation that can be used to provision edge routers.
- **VPN 3000** Any router in the Cisco VPN 3000 Series Concentrator family. - **NOT SUPPORTED in this release.** -
- **Firewall** Any Cisco PIX Firewall. - **NOT SUPPORTED in this release.** -
- **IE2100** Any Cisco Intelligence Engine (IE) 2100 series network device.

- Step 3** See the following sections for instructions on creating each type of device.

- [Creating a Catalyst Switch, page 3-46](#)

- [Creating a Cisco IOS Device, page 3-52](#)
- [Creating a Terminal Server, page 3-58](#)
- [Creating a VPN 3000, page 3-63](#)
- [Creating a Firewall, page 3-66](#)
- [Creating a Cisco CNS IE2100, page 3-72](#)

Creating a Catalyst Switch

To create a Catalyst switch, do the following:

- Step 1** Navigate **Service Inventory > Inventory and Connection Manager > Devices**.
- Step 2** Click the **Create** button.
- Step 3** Select **Catalyst Switch**.

The Create Catalyst Device window appears, as shown in [Figure 3-39](#).

Figure 3-39 Create Catalyst Device Window

The screenshot displays the 'Create Catalyst Device' window, which is organized into several sections:

- General:** Includes fields for 'Device Host Name' (marked with an asterisk), 'Device Domain Name', 'Description', 'Collection Zone' (set to 'None'), and 'Management IP Address'. There are 'Edit' buttons for 'Interfaces' and 'Associated Groups'.
- Operating System:** Features radio buttons for 'Catalyst OS' and 'Cisco IOS'.
- Catalyst Properties:** Includes a 'VNSM' field with an information icon and an 'Edit' button.
- Login and Password Information:** Contains fields for 'Login User', 'Login Password', 'Verify Login Password', 'Enable User', 'Enable Password', and 'Verify Enable Password'.
- Device and Configuration Access Information:** Includes dropdown menus for 'Terminal Session Protocol' (Default (Telnet)), 'Config Access Protocol' (Default (Terminal)), and 'SNMP Version' (Default (SNMP v1/v2c)).
- SNMP v1/v2c:** Includes fields for 'Community String RO' and 'Community String RW'.
- Additional Properties:** A section with an 'Edit' button.

At the bottom of the window are 'Save' and 'Cancel' buttons. A note at the bottom left states: 'Note: * - Required Field'. The number '116246' is visible in the bottom right corner of the window frame.

The General section of the Create Catalyst Device window contains the following fields:

- **Device Host Name** (required) Must begin with a letter, digit, or underscore followed by letters, digits, underscores, spaces, hyphens, or dots ending with a letter, digit, or underscore. This field must match the name configured on the target router device. Limited to 256 characters.
- **Device Domain Name** (optional) Must begin with a letter, digit, or underscore followed by letters, digits, underscores, spaces, hyphens, or dots ending with a letter, digit, or underscore. The name must match the domain name on the target router device.
- **Description** (optional) Limited to 80 characters. Can contain any pertinent information about the device such as the type of device, its location, or other information that might be helpful to service provider operators.
- **Collection Zone** (optional) Drop-down list of all collection zones within the ISC. Choices include: None and all collection zones within the ISC. Default: None.
- **Management IP Address** (optional) Valid IP address of the device that ISC uses to configure the target router device.
- **Interfaces** (optional) Click the **Edit** button to view, add, edit, and delete all interfaces associated with the device. See [Table 3-6](#) for a description of the Interfaces fields.

Table 3-6 Create Catalyst Device Interfaces Fields

Field	Description	Additional
Name	Name of this interface.	List can be sorted by this field. Limited to 80 characters.
Encapsulation	The Layer 2 Encapsulation for this device.	DEFAULT DOT1Q ETHERNET ISL FRAME_RELAY FRAME_RELAY_IETF HDLC PPP ATM AAL5SNAP AAL0 AAL5 AAL5MUX AAL5NLPID AAL2 ENCAP_QinQ GRE
IP Address	IP address associated with this interface.	

Table 3-6 Create Catalyst Device Interfaces Fields (continued)

Field	Description	Additional
Port Type		NONE ACCESS TRUNK ROUTED
VLAN ID	The VLAN ID to assign to this interface.	

- **Associated Groups** (optional) Click the **Edit** button to view, add, and remove all Device Group associations.
- **Operating System** (optional) Click the radio button for the operating system currently running on the CAT switch. Choices include: CatOs or IOS. Default: CatOs. When you choose the IOS operating system, VPNSM is available under the heading Catalyst Properties.
- **VPNSM** (optional) This is only available if you chose the Operating System radio button of **Cisco IOS**. If you click the **Edit** button, an Edit Device VPNSM Blades window (for VPN Service Modules) appears. This is the only place to create a VPNSM. It uses this IOS operating system of the catalyst switch as a parent device. You can do the following:
 - **Create** Click this button and a VPNSM Blade window appears. Here you can enter the following:
 - **Name** (optional)
 - **Module Number** (required) The default is 1.

After you enter this information, click **OK** and you return to the Edit Device VPNSM Blades window, which is updated to include the new information. (If you did not enter a Name, the default name is the <device host name>_VPNSM_<module number>.)

- **Edit** Select the check box next to the VPNSM that you want to edit and click the **Edit** button. You receive a window with the current information about this VPNSM that you can edit. Then click **OK**.
- **Delete** Select the check box(es) next to the VPNSM(s) you want to delete and click the **Delete** button. You receive a confirmation window in which you can click **OK** to complete the deletion or you can click **Cancel** to cancel the deletion.
- **OK** Click **OK** and you return to the Create Catalyst Device window and the created VPNSM(s) are listed.
- **Cancel** Click **Cancel** if you decide not to create a VPNSM.

The Login and Password Information section of the Create Catalyst Device window contains the following fields:

- **Login User** (optional) Not required by ISC. However, collection and upload/download will not function without the Login User and Login Password as ISC will not be able to access the device. Should match what is configured on the target router device. Limited to 80 characters.
- **Login Password** (optional) Displayed as stars (*). Not required by ISC. However, collection and upload/download will not function without the Login User and Login Password as ISC will not be able to access the device. Should match what is configured on the target router device. Limited to 80 characters.

- **Verify Login Password** (optional) Displayed as stars (*). Must match the Login Password field. Limited to 80 characters.
- **Enable User** (optional) Not required by ISC. However, collection and upload/download only function if the Login User has sufficient privileges to configure the router in EXEC mode. Should match what is configured on the target router device. Limited to 80 characters.
- **Enable Password** (optional) Displayed as stars (*). Not required by ISC. However, collection and upload/download only function if the Login User has sufficient privileges to configure the router in EXEC mode. Should match what is configured on the target router device. Limited to 80 characters.
- **Verify Enable Password** (optional) Displayed as stars (*). Must match the Enable Password field. Limited to 80 characters.

The Device and Configuration Access Information section of the Create Catalyst Device window contains the following fields:

- **Terminal Session Protocol** (optional) Configures the method of communication between ISC and the device. Choices include: Telnet, Secure Shell (SSH), and CNS. In previous versions of ISC, this field was called the Transport field. Default: The default set in the DCPL properties.
- **Config Access Protocol** (optional) Administers the access protocol for config upload and download. Choices include: Terminal, TFTP, and FTP. Default: The default set in the DCPL properties.
- **SNMP Version** (optional) Configures the version of SNMP to use when communicating with the device. Choices include: SNMP v1/v2c and SNMP v3. Default: The default set in the DCPL properties.

The SNMP v1/v2c section of the Create Catalyst Device window contains the following fields:

- **Community String RO** (optional) SNMP Read-Only Community String. Many tasks use SNMP to access the device. This field must match what is configured on the target router device. Limited to 80 characters.
- **Community String RW** (optional) SNMP Read-Write Community String. Many tasks use SNMP to access the device. This field must match what is configured on the target router device. Limited to 80 characters.

Step 4 Enter the desired information for the Catalyst device you are creating.

Step 5 To access the Additional Properties section of the **Create Catalyst Device**, click **Edit**.

The Catalyst Device Properties window appears, as shown in [Figure 3-40](#).

Figure 3-40 Catalyst Device Properties Window

Catalyst Device Properties

Device: device1

SNMP v3

SNMP Security Level: Default (No Authentication/No Encryption) ▼

Authentication User Name:

Authentication Password:

Verify Authentication Password:

Authentication Algorithm: None ▼

Encryption Password:

Verify Encryption Password:

Encryption Algorithm: None ▼

Terminal Server and CNS Options

Terminal Server: None ▼

Port:

Fully Managed: ☐

Device State: ACTIVE ▼

CNS Identification:

Device Event Identification: CNS_ID ▼

Most recent CNS event: None ▼

IE2100: None ▼

CNS Software Version: 1.3.2 ▼

CNS Device Transport: HTTP ▼

Device Platform Information

Platform:

Software Version:

Image Name:

Serial Number:

Device Owner's Email Address:

OK Cancel

101977

The SNMP v3 section of the Catalyst Device Properties window contains the following fields:

- **SNMP Security Level** (optional) Choices include: Default (<default_set_in_DCPL>), Authentication/No Encryption, and Authentication/Encryption. Default: Default (<default_set_in_DCPL>). Note: When you change the DCPL property, the <default_set_in_DCPL> variable changes.
- **Authentication User Name** (optional) User name configured on the specified device router. User must have permission to the object identification numbers (OIDs) specified in the security request (that is, write permission for a set request, and read permission for a get request). Should match what is configured on the target router device. Should be provisioned if the SNMP Security Level is Authentication/No Encryption or Authentication/Encryption. Limited to 80 characters.
- **Authentication Password** (optional) Displayed as stars (*). Should be provisioned if the SNMP Security Level is Authentication/No Encryption or Authentication/Encryption. Should match what is configured on the target router device. Limited to 80 characters.
- **Verify Authentication Password** (optional) Displayed as stars (*). Must match the Encryption Password field. Limited to 80 characters.

- **Authentication Algorithm** (optional) Should be provisioned if the SNMP Security Level is Authentication/No Encryption or Authentication/Encryption. Choices include: None, MD5, and SHA. Default: None.
- **Encryption Password** (optional) Displayed as stars (*). In previous versions of ISC, this field was called Privacy Password. Should match what is configured on the target router device. Should be provisioned if the SNMP Security Level is Authentication/Encryption. Limited to 80 characters.
- **Verify Encryption Password** (optional) Displayed as stars (*). Must match the Encryption Password field. Limited to 80 characters.
- **Encryption Algorithm** (optional) In previous versions of ISC, this field was called Privacy Protocol. Should be provisioned if the SNMP Security Level is Authentication/Encryption. Choices include: None and DES 56. Default: None.

The Terminal Server and CNS Options section of the Catalyst Device Properties window contains the following fields:

- **Terminal Server** (optional) Choices include: None and the list of existing Terminal Server names. Default: None.
- **Port** (optional) Disabled until a Terminal Server is selected. Range: 0-65535. Default: 0.
- **Fully Managed** (optional) If the Fully Managed check box is selected, the device becomes a fully managed device. ISC performs additional management actions only for fully managed devices. These actions include e-mail notifications upon receipt of device configuration changes originated outside ISC and the scheduling of enforcement audit tasks upon detection of possible intrusion. Default: Not selected and therefore not selected.
- **Device State** (optional) Choices include: ACTIVE and INACTIVE. ACTIVE indicates that the router has been plugged on the network and can be part of ISC tasks such as collect config and provisioning. INACTIVE indicates the router has not been plugged-in. Default: ACTIVE.
- **CNS Identification** Required if the Device Event Identification field is set to CNS_ID. Only valid characters that Cisco IOS allows are alphanumeric characters and (.) (-) (_).
- **Device Event Identification** (optional) Indicates whether the CNS Identification field contains a HOST_NAME or CNS_ID. Default: HOST_NAME.
- **Most Recent CNS event** (optional) Choices include: None, CONNECT, and DISCONNECT. Changing from the default of None is not recommended. Note: The last connect or disconnect CNS TIBCO event received by ISC for each CNS-enabled IOS device is automatically recorded.
- **IE2100** (optional) Disabled unless the Device State field is INACTIVE or the Terminal Session Protocol field is CNS. A valid IE2100 must be selected if the Terminal Session Protocol is CNS. Choices include: None and the list of existing IE2100 names. Default: None.
- **CNS Software Version** (optional) Choices include: 1.3, 1.3.1, and 1.3.2. This is the release version of Cisco CNS Configuration Engine that manages the IOS device. Default: 1.3.2.
- **CNS Device Transport** (optional) Choices include: HTTP and HTTPS. This field determines what will be the transport mechanism used by ISC to create, delete, or edit devices in the IE2100 repository. If HTTPS is used, the Cisco CNS Configuration Engine must be running in secure mode. Default: HTTP.

The Device Platform Information section of the Catalyst Device Properties window contains the following fields:

- **Platform** (optional) Should match what is configured on the target router device. Limited to 80 characters.
- **Software Version** (optional) Should match what is configured on the target router device. Limited to 80 characters.

- **Image Name** (optional) Should match what is configured on the target router device. Limited to 80 characters.
- **Serial Number** (optional) Should match what is configured on the target router device. Limited to 80 characters.
- **Device Owner's Email Address** (optional) Used in the To: field when the Email button is selected from the device list. Limited to 80 characters and must be valid Email format.

Step 6 Enter any desired Additional Properties information for the Catalyst device you are creating.

Step 7 Click **OK**.

Step 8 Click **Save**.

The Devices window reappears with the new Catalyst device listed.

Creating a Cisco IOS Device

To create a Cisco IOS device, do the following:

Step 1 Navigate **Service Inventory > Inventory and Connection Manager > Devices**.

Step 2 Click the **Create** button.

Step 3 Select **Cisco IOS Device**.

The Create Cisco IOS Device window appears, as shown in [Figure 3-41](#).

Figure 3-41 Create Cisco IOS Device Window

Create Cisco IOS Device

General	
Device Host Name *	
Device Domain Name:	
Description:	
Collection Zone:	None ▾
Management IP Address:	
Interfaces:	Edit
Associated Groups:	Edit
Login and Password Information	
Login User:	
Login Password:	
Verify Login Password:	
Enable User:	
Enable Password:	
Verify Enable Password:	
Device and Configuration Access Information	
Terminal Session Protocol:	Default (Telnet) ▾
Config Access Protocol:	Default (Terminal) ▾
SNMP Version:	Default (SNMP v1/v2c) ▾
SNMP v1/v2c	
Community String RO:	
Community String RW:	
Additional Properties:	Edit
Save Cancel	

Note: * - Required Field

93777

The General section of the Create Cisco IOS Device window contains the following fields:

- **Device Host Name** Must begin with a letter, digit, or underscore followed by letters, digits, underscores, spaces, hyphens, or dots ending with a letter, digit, or underscore. This field is required and must match the name configured on the target router device. Limited to 256 characters.
- **Device Domain Name** (optional) Must begin with a letter, digit, or underscore followed by letters, digits, underscores, spaces, hyphens, or dots ending with a letter, digit, or underscore. The name must match the domain name on the target router device.
- **Description** (optional) Limited to 80 characters. Can contain any pertinent information about the device such as the type of device, its location, or other information that might be helpful to service provider operators.
- **Collection Zone** (optional) Drop-down list of all collection zones within the ISC. Choices include: None and all collection zones within the ISC. Default: None.
- **Management IP Address** (optional) Valid IP address of the device that ISC uses to configure the target router device.
- **Interfaces** (optional) Click the Edit button to view, add, edit, and delete all interfaces associated with the device. See [Table 3-7](#) for a description of the Interface fields.

Table 3-7 Create Cisco IOS Device Interface Fields

Field	Description	Additional
Name	Name of this interface.	List can be sorted by this field. Limited to 80 characters.
Encapsulation	The Layer 2 Encapsulation for this device.	DEFAULT DOT1Q ETHERNET ISL FRAME_RELAY FRAME_RELAY_IETF HDLC PPP ATM AAL5SNAP AAL0 AAL5 AAL5MUX AAL5NLPID AAL2 ENCAP_QinQ GRE
IP Address	IP address associated with this interface.	

- **Associated Groups** (optional) Click the **Edit** button to view, add, and remove all Device Group associations.

The Login and Password Information section of the Create Cisco IOS Device window contains the following fields:

- **Login User** (optional) Not required by ISC. However, collection and upload/download will not function without the Login User and Login Password as ISC will not be able to access the device. Should match what is configured on the target router device. Limited to 80 characters.
- **Login Password** (optional) Displayed as stars (*). Not required by ISC. However, collection and upload/download will not function without the Login User and Login Password as ISC will not be able to access the device. Should match what is configured on the target router device. Limited to 80 characters.
- **Verify Login Password** (optional) Displayed as stars (*). Must match the Login Password field. Limited to 80 characters.
- **Enable User** (optional) Not required by ISC. However, collection and upload/download only function if the Login User has sufficient privileges to configure the router in EXEC mode. Should match what is configured on the target router device. Limited to 80 characters.
- **Enable Password** (optional) Displayed as stars (*). Not required by ISC. However, collection and upload/download only function if the Login User has sufficient privileges to configure the router in EXEC mode. Should match what is configured on the target router device. Limited to 80 characters.
- **Verify Enable Password** (optional) Displayed as stars (*). Must match the Enable Password field. Limited to 80 characters.

The Device and Configuration Access Information section of the Create Cisco IOS Device window contains the following fields:

- **Terminal Session Protocol** (optional) Configures the method of communication between ISC and the device. Choices include: Telnet, Secure Shell (SSH), and CNS. In previous versions of ISC this
- **Config Access Protocol** (optional) Administers the access protocol for config upload and download. Choices include: Terminal, TFTP, and FTP. Default: The default set in the DCPL properties.
- **SNMP Version** (optional) Configures the version of SNMP to use when communicating with the device. Choices include: SNMP v1/v2c and SNMP v3. Default: The default set in the DCPL properties.

The SNMP v1/v2c section of the Create Cisco IOS Device window contains the following fields:

- **Community String RO** (optional) SNMP Read-Only Community String. Many tasks use SNMP to access the device. This field must match what is configured on the target router device. Limited to 80 characters.
- **Community String RW** (optional) SNMP Read-Write Community String. Many tasks use SNMP to access the device. This field must match what is configured on the target router device. Limited to 80 characters.

Step 4 Enter the desired information for the Cisco IOS device you are creating.

Step 5 To access the Additional Properties section of the **Create Cisco IOS Device**, click **Edit**.

The Cisco IOS Device Properties window appears, as shown in [Figure 3-42](#).

Figure 3-42 Cisco IOS Device Properties Window

The SNMP v3 section of the Cisco IOS Device Properties window contains the following fields:

- **SNMP Security Level** (optional) Choices include: Default (<default_set_in_DCPL>), Authentication/No Encryption, and Authentication/Encryption. Default: Default (<default_set_in_DCPL>). Note: When you change the DCPL property, the <default_set_in_DCPL> variable changes.
- **Authentication User Name** (optional) User name configured on the specified device router. User must have permission to the object identification numbers (OIDs) specified in the security request (that is, write permission for a set request, and read permission for a get request). Should match what is configured on the target router device. Should be provisioned if the SNMP Security Level is Authentication/No Encryption or Authentication/Encryption. Limited to 80 characters.
- **Authentication Password** (optional) Displayed as stars (*). Should be provisioned if the SNMP Security Level is Authentication/No Encryption or Authentication/Encryption. Should match what is configured on the target router device. Limited to 80 characters.
- **Verify Authentication Password** (optional) Displayed as stars (*). Must match the Encryption Password field. Limited to 80 characters.
- **Authentication Algorithm** (optional) Should be provisioned if the SNMP Security Level is Authentication/No Encryption or Authentication/Encryption. Choices include: None, MD5, and SHA. Default: None.
- **Encryption Password** (optional) Displayed as stars (*). In previous versions of ISC, this field was called Privacy Password. Should match what is configured on the target router device. Should be provisioned if the SNMP Security Level is Authentication/Encryption. Limited to 80 characters.

- **Verify Encryption Password** (optional) Displayed as stars (*). Must match the Encryption Password field. Limited to 80 characters.
- **Encryption Algorithm** (optional) In previous versions of ISC, this field was called Privacy Protocol. Should be provisioned if the SNMP Security Level is Authentication/Encryption. Choices include: None and DES 56. Default: None.

The Terminal Server and CNS Options section of the Cisco IOS Device Properties window contains the following fields:

- **Terminal Server** (optional) Choices include: None and the list of existing Terminal Server names. Default: None.
- **Port** (optional) Disabled until a Terminal Server is selected. Range: 0-65535. Default: 0.
- **Fully Managed** (optional) If the Fully Managed check box is selected, the device becomes a fully managed device. ISC performs additional management actions only for fully managed devices. These actions include e-mail notifications upon receipt of device configuration changes originated outside ISC and the scheduling of enforcement audit tasks upon detection of possible intrusion. Default: Not selected and therefore not selected.
- **Device State** (optional) Choices include: ACTIVE and INACTIVE. ACTIVE indicates that the router has been plugged on the network and can be part of ISC tasks such as collect config and provisioning. INACTIVE indicates the router has not been plugged-in. Default: ACTIVE.
- **CNS Identification** Required if the Device Event Identification field is set to CNS_ID. Only valid characters that Cisco IOS allows are alphanumeric characters and (.) (-) (_).
- **Device Event Identification** (optional) Indicates whether the CNS Identification field contains a HOST_NAME or CNS_ID. Default: HOST_NAME.
- **Most Recent CNS event** (optional) Choices include: None, CONNECT, and DISCONNECT. Changing from the default of None is not recommended. Note: The last connect or disconnect CNS TIBCO event received by ISC for each CNS-enabled IOS device is automatically recorded.
- **IE2100** (optional) Disabled unless the Device State field is INACTIVE or the Terminal Session Protocol field is CNS. A valid IE2100 must be selected if the Terminal Session Protocol is CNS. Choices include: None and the list of existing IE2100 names. Default: None.
- **CNS Software Version** (optional) Choices include: 1.3, 1.3.1, 1.3.2, and 1.4. This is the release version of Cisco CNS Configuration Engine that manages the IOS device. Default: 1.3.2.
- **CNS Device Transport** (optional) Choices include: HTTP and HTTPS. This field determines what will be the transport mechanism used by ISC to create, delete, or edit devices in the IE2100 repository. If HTTPS is used, the Cisco CNS Configuration Engine must be running in secure mode. Default: HTTP.

The Device Platform Information section of the Cisco IOS Device Properties window contains the following fields:

- **Platform** (optional) Should match what is configured on the target router device. Limited to 80 characters.
- **Software Version** (optional) Should match what is configured on the target router device. Limited to 80 characters.
- **Image Name** (optional) Should match what is configured on the target router device. Limited to 80 characters.

- **Serial Number** (optional) Should match what is configured on the target router device. Limited to 80 characters.
- **Device Owner's Email Address** (optional) Used in the To: field when the Email button is selected from the device list. Limited to 80 characters and must be valid Email format.

Step 6 Enter any desired Additional Properties information for the Cisco IOS device you are creating.

Step 7 Click **OK**.

Step 8 Click **Save**.

The Devices window reappears with the new Cisco IOS device listed.

Creating a Terminal Server

To create a Terminal Server device, do the following:

Step 1 Navigate **Service Inventory > Inventory and Connection Manager > Devices**.

Step 2 Click the **Create** button.

Step 3 Select **Terminal Server**.

The Create Terminal Server window appears, as shown in [Figure 3-43](#).

Figure 3-43 Create Terminal Server Window

Create Terminal Server

General

Device Host Name *:

Device Domain Name:

Description:

Collection Zone:

Management IP Address:

Interfaces:

Associated Groups:

Login and Password Information

Login User:

Login Password:

Verify Login Password:

Enable User:

Enable Password:

Verify Enable Password:

Device and Configuration Access Information

Terminal Session Protocol:

Config Access Protocol:

SNMP Version:

SNMP v1/v2c

Community String RO:

Community String RW:

Additional Properties:

Note: * - Required Field

93781

The General section of the Create Terminal Server window contains the following fields:

- **Device Host Name** (required) Must begin with a letter, digit, or underscore followed by letters, digits, underscores, spaces, hyphens, or dots ending with a letter, digit, or underscore. This field must match the name configured on the target router device. Limited to 256 characters.
- **Device Domain Name** (optional) Must begin with a letter, digit, or underscore followed by letters, digits, underscores, spaces, hyphens, or dots ending with a letter, digit, or underscore. The name must match the domain name on the target router device.
- **Description** (optional) Limited to 80 characters. Can contain any pertinent information about the device such as the type of device, its location, or other information that might be helpful to service provider operators.
- **Collection Zone** (optional) Drop-down list of all collection zones within the ISC. Choices include: None and all collection zones within the ISC. Default: None.
- **Management IP Address** (optional) Valid IP address of the device that ISC uses to configure the target router device.

- **Interfaces** (optional) Click the **Edit** button to view, add, edit, and delete all interfaces associated with the device. See [Table 3-8](#) for a description of the Interfaces fields.

Table 3-8 Create Terminal Server Device Interfaces Fields

Field	Description	Additional
Name	Name of this interface.	List can be sorted by this field. Limited to 80 characters.
Encapsulation	The Layer 2 Encapsulation for this device.	DEFAULT DOT1Q ETHERNET ISL FRAME_RELAY FRAME_RELAY_IETF HDLC PPP ATM AAL5SNAP AAL0 AAL5 AAL5MUX AAL5NLPID AAL2 ENCAP_QinQ GRE
IP Address	IP address associated with this interface.	

- **Associated Groups** (optional) Click the **Edit** button to view, add, and remove all Device Group associations.

The Login and Password Information section of the Create Terminal Server window contains the following fields:

- **Login User** (optional) Not required by ISC. However, collection and upload/download will not function without the Login User and Login Password as ISC will not be able to access the device. Should match what is configured on the target router device. Limited to 80 characters.
- **Login Password** (optional) Displayed as stars (*). Not required by ISC. However, collection and upload/download will not function without the Login User and Login Password as ISC will not be able to access the device. Should match what is configured on the target router device. Limited to 80 characters.
- **Verify Login Password** (optional) Displayed as stars (*). Must match the Login Password field. Limited to 80 characters.

- **Enable User** (optional) Not required by ISC. However, collection and upload/download only function if the Login User has sufficient privileges to configure the router in EXEC mode. Should match what is configured on the target router device. Limited to 80 characters.
- **Enable Password** (optional) Displayed as stars (*). Not required by ISC. However, collection and upload/download only function if the Login User has sufficient privileges to configure the router in EXEC mode. Should match what is configured on the target router device. Limited to 80 characters.
- **Verify Enable Password** (optional) Displayed as stars (*). Must match the Enable Password field. Limited to 80 characters.

The Device and Configuration Access Information section of the Create Terminal Server window contains the following fields:

- **Terminal Session Protocol** (optional) Configures the method of communication between ISC and the device. Choices include: Telnet, Secure Shell (SSH), CNS, and RSH. In previous versions of ISC, this field was called the Transport field. Default: The default set in the DCPL properties.
- **Config Access Protocol** (optional) Administers the access protocol for config upload and download. Choices include: Terminal, TFTP, FTP, and RCP. Default: The default set in the DCPL properties.
- **SNMP Version** (optional) Configures the version of SNMP to use when communicating with the device. Choices include: SNMP v1/v2c and SNMP v3. Default: The default set in the DCPL properties.

The SNMP v1/v2c section of the Create Terminal Server window contains the following fields:

- **Community String RO** (optional) SNMP Read-Only Community String. Many tasks use SNMP to access the device. This field must match what is configured on the target router device. Limited to 80 characters.
- **Community String RW** (optional) SNMP Read-Write Community String. Many tasks use SNMP to access the device. This field must match what is configured on the target router device. Limited to 80 characters.

Step 4 Enter the desired information for the Terminal Server you are creating.

Step 5 To access the Additional Properties section of the **Create Terminal Server**, click **Edit**.

The Terminal Server Device Properties window appears, as shown in [Figure 3-44](#).

Figure 3-44 Terminal Server Device Properties Window

The SNMP v3 section of the Terminal Server Device Properties window contains the following fields:

- **SNMP Security Level** (optional) Choices include: Default (<default_set_in_DCPL>), Authentication/No Encryption, and Authentication/Encryption. Default: Default (<default_set_in_DCPL>). Note: When you change the DCPL property, the <default_set_in_DCPL> variable changes.
- **Authentication User Name** (optional) User name configured on the specified device router. User must have permission to the object identification numbers (OIDs) specified in the security request (that is, write permission for a set request, and read permission for a get request). Should match what is configured on the target router device. Should be provisioned if the SNMP Security Level is Authentication/No Encryption or Authentication/Encryption. Limited to 80 characters.
- **Authentication Password** (optional) Displayed as stars (*). Should be provisioned if the SNMP Security Level is Authentication/No Encryption or Authentication/Encryption. Should match what is configured on the target router device. Limited to 80 characters.
- **Verify Authentication Password** (optional) Displayed as stars (*). Must match the Encryption Password field. Limited to 80 characters.
- **Authentication Algorithm** (optional) Should be provisioned if the SNMP Security Level is Authentication/No Encryption or Authentication/Encryption. Choices include: None, MD5, and SHA. Default: None.
- **Encryption Password** (optional) Displayed as stars (*). In previous versions of ISC, this field was called Privacy Password. Should match what is configured on the target router device. Should be provisioned if the SNMP Security Level is Authentication/Encryption. Limited to 80 characters.

- **Verify Encryption Password** (optional) Displayed as stars (*). Must match the Encryption Password field. Limited to 80 characters.
- **Encryption Algorithm** (optional) In previous versions of ISC, this field was called Privacy Protocol. Should be provisioned if the SNMP Security Level is Authentication/Encryption. Choices include: None and DES 56. Default: None.

The Device Platform Information section of the Terminal Server Device Properties window contains the following fields:

- **Platform** (optional) Should match what is configured on the target router device. Limited to 80 characters.
- **Software Version** (optional) Should match what is configured on the target router device. Limited to 80 characters.
- **Image Name** (optional) Should match what is configured on the target router device. Limited to 80 characters.
- **Serial Number** (optional) Should match what is configured on the target router device. Limited to 80 characters.
- **Device Owner's Email Address** (optional) Used in the To: field when the Email button is selected from the device list. Limited to 80 characters and must be valid Email format.

Step 6 Enter any desired Additional Properties information for the Terminal Server device you are creating.

Step 7 Click **OK**.

Step 8 Click **Save**.

The Devices window reappears with the new Terminal Server device listed.

Creating a VPN 3000

- NOT SUPPORTED in this release. -

To create a VPN 3000 device, do the following:

Step 1 Navigate **Service Inventory > Inventory and Connection Manager > Devices**.

Step 2 Click the **Create** button.

Step 3 Select **VPN 3000**.

The Create VPN 3000 Device window appears, as shown in [Figure 3-45](#).

Figure 3-45 Create VPN 3000 Device Window

Create VPN 3000 Device

General

Device Host Name *:

Device Domain Name:

Description:

Collection Zone:

Management IP Address:

Interfaces:

Associated Groups:

Login and Password Information

Login User:

Login Password:

Verify Login Password:

Device Platform Information

Platform:

Software Version:

Image Name:

Serial Number:

Device Owner's Email Address:

Note: * - Required Field

93783

The General section of the Create VPN 3000 Device window contains the following fields:

- **Device Host Name** (required) Must begin with a letter, digit, or underscore followed by letters, digits, underscores, spaces, hyphens, or dots ending with a letter, digit, or underscore. This field must match the name configured on the target router device. Limited to 255 characters.
- **Device Domain Name** (optional) Must begin with a letter, digit, or underscore followed by letters, digits, underscores, spaces, hyphens, or dots ending with a letter, digit, or underscore. The name must match the domain name on the target router device.
- **Description** (optional) Limited to 80 characters. Can contain any pertinent information about the device such as the type of device, its location, or other information that might be helpful to service provider operators.
- **Collection Zone** (optional) Drop-down list of all collection zones within the ISC. Choices include: None and all collection zones within the ISC. Default: None.
- **Management IP Address** (optional) Valid IP address of the device that ISC uses to configure the target router device.

- **Interfaces** (optional) Click the **Edit** button to view, add, edit, and delete all interfaces associated with the device. See [Table 3-9](#) for a description of the Interfaces fields.

Table 3-9 Create VPN 3000 Device Interfaces Fields

Field	Description	Additional
Name	Name of this interface.	List can be sorted by this field. Limited to 80 characters.
Encapsulation	The Layer 2 Encapsulation for this device.	DEFAULT DOT1Q ETHERNET ISL FRAME_RELAY FRAME_RELAY_IETF HDLC PPP ATM AAL5SNAP AAL0 AAL5 AAL5MUX AAL5NLPID AAL2 ENCAP_QinQ GRE
IP Address	IP address associated with this interface.	

- **Associated Groups** (optional) Click the **Edit** button to view, add, and remove all Device Group associations.

The Login and Password Information section of the Create VPN 3000 Device window contains the following fields:

- **Login User** (optional) Not required by ISC. However, collection and upload/download will not function without the Login User and Login Password as ISC will not be able to access the device. Should match what is configured on the target router device. Limited to 80 characters.
- **Login Password** (optional) Displayed as stars (*). Not required by ISC. However, collection and upload/download will not function without the Login User and Login Password as ISC will not be able to access the device. Should match what is configured on the target router device. Limited to 80 characters.
- **Verify Login Password** (optional) Displayed as stars (*). Must match the Login Password field. Limited to 80 characters.

The Device Platform Information section of the Create VPN 3000 Device window contains the following fields:

- **Platform** (optional) Should match what is configured on the target router device. Limited to 80 characters.
- **Software Version** (optional) Should match what is configured on the target router device. Limited to 80 characters.
- **Image Name** (optional) Should match what is configured on the target router device. Limited to 80 characters.
- **Serial Number** (optional) Should match what is configured on the target router device. Limited to 80 characters.
- **Device Owner's Email Address** (optional) Used in the To: field when the Email button is selected from the device list. Limited to 80 characters and must be valid Email format.

Step 4 Enter the desired information for the VPN 3000 device you are creating.

Step 5 Click **Save**.

The Devices window reappears with the new VPN 3000 device listed.

Creating a Firewall

- NOT SUPPORTED in this release. -

To create a PIX Firewall, do the following:

Step 1 Navigate **Service Inventory > Inventory and Connection Manager > Devices**.

Step 2 Click the **Create** button.

Step 3 Select **Firewall**.

The Create PIX Firewall window appears, as shown in [Figure 3-46](#).

Figure 3-46 Create PIX Firewall Window

Create PIX Firewall

General

Device Host Name *:

Device Domain Name:

Description:

Collection Zone:

Management IP Address:

Interfaces:

Associated Groups:

Login and Password Information

Login User:

Login Password:

Verify Login Password:

Enable User:

Enable Password:

Verify Enable Password:

Device and Configuration Access Information

Terminal Session Protocol:

Config Access Protocol:

SNMP Version:

SNMP v1/v2c

Community String RO:

Community String RW:

Additional Properties:

Note: * - Required Field

93784

The General section of the Create PIX Firewall window contains the following fields:

- **Device Host Name** (required) Must begin with a letter, digit, or underscore followed by letters, digits, underscores, spaces, hyphens, or dots ending with a letter, digit, or underscore. This field must match the name configured on the target router device. Limited to 256 characters.
- **Description** (optional) Limited to 80 characters. Can contain any pertinent information about the device such as the type of device, its location, or other information that might be helpful to service provider operators.
- **Collection Zone** (optional) Drop-down list of all collection zones within the ISC. Choices include: None and all collection zones within the ISC. Default: None.
- **Management IP Address** (optional) Valid IP address of the device that ISC uses to configure the target router device.

- **Interfaces** (optional) Click the **Edit** button to view, add, edit, and delete all interfaces associated with the device. See [Table 3-10](#) for a description of the Interfaces fields.

Table 3-10 Create PIX Firewall Device Interfaces Fields

Field	Description	Additional
Name	Name of this interface.	List can be sorted by this field. Limited to 80 characters.
Encapsulation	The Layer 2 Encapsulation for this device.	DEFAULT DOT1Q ETHERNET ISL FRAME_RELAY FRAME_RELAY_IETF HDLC PPP ATM AAL5SNAP AAL0 AAL5 AAL5MUX AAL5NLPID AAL2 ENCAP_QinQ GRE
IP Address	IP address associated with this interface.	

- **Associated Groups** (optional) Click the **Edit** button to view, add, and remove all Device Group associations.

The Login and Password Information section of the Create PIX Firewall window contains the following fields:

- **Login User** (optional) Not required by ISC. However, collection and upload/download will not function without the Login User and Login Password as ISC will not be able to access the device. Should match what is configured on the target router device. Limited to 80 characters.
- **Login Password** (optional) Displayed as stars (*). Not required by ISC. However, collection and upload/download will not function without the Login User and Login Password as ISC will not be able to access the device. Should match what is configured on the target router device. Limited to 80 characters.
- **Verify Login Password** (optional) Displayed as stars (*). Must match the Login Password field. Limited to 80 characters.

- **Enable User** (optional) Not required by ISC. However, collection and upload/download only function if the Login User has sufficient privileges to configure the router in EXEC mode. Should match what is configured on the target router device. Limited to 80 characters.
- **Enable Password** (optional) Displayed as stars (*). Not required by ISC. However, collection and upload/download only function if the Login User has sufficient privileges to configure the router in EXEC mode. Should match what is configured on the target router device. Limited to 80 characters.
- **Verify Enable Password** (optional) Displayed as stars (*). Must match the Enable Password field. Limited to 80 characters.

The Device and Configuration Access Information section of the Create PIX Firewall window contains the following fields:

- **Terminal Session Protocol** (optional) Configures the method of communication between ISC and the device. Choices include: Telnet, Secure Shell (SSH), and CNS. In previous versions of ISC, this field was called the Transport field. Default: The default set in the DCPL properties.
- **Config Access Protocol** (optional) Administers the access protocol for config upload and download. Choices include: Terminal, TFTP, and FTP. Default: The default set in the DCPL properties.
- **SNMP Version** (optional) Configures the version of SNMP to use when communicating with the device. Choices include: SNMP v1/v2c and SNMP v3. Default: The default set in the DCPL properties.

The SNMP v1/v2c section of the Create PIX Firewall window contains the following fields:

- **Community String RO** (optional) SNMP Read-Only Community String. Many tasks use SNMP to access the device. This field must match what is configured on the target router device. Limited to 80 characters.
- **Community String RW** (optional) SNMP Read-Write Community String. Many tasks use SNMP to access the device. This field must match what is configured on the target router device. Limited to 80 characters.

Step 4 Enter the desired information for the PIX Firewall device you are creating.

Step 5 To access the Additional Properties section of the **Create PIX Firewall**, click **Edit**.

The PIX Device Properties window appears, as shown in [Figure 3-47](#).

Figure 3-47 PIX Device Properties Window

The screenshot shows the 'PIX Device Properties' window with the following sections and fields:

- Device:** (Header)
- SNMP v3:**
 - SNMP Security Level: Default (No Authentication/No Encryption) [dropdown]
 - Authentication User Name: [text field]
 - Authentication Password: [text field]
 - Verify Authentication Password: [text field]
 - Authentication Algorithm: None [dropdown]
 - Encryption Password: [text field]
 - Verify Encryption Password: [text field]
 - Encryption Algorithm: None [dropdown]
- Terminal Server Options:**
 - Terminal Server: None [dropdown]
 - Port: [text field]
- Failover Options:**
 - Failover Type: ☒ None ☐ Normal ☐ Stateful
 - LAN Based Failover: ☐
 - Failover LAN Key: [text field]
- Device Platform Information:**
 - Platform: [text field]
 - Software Version: [text field]
 - Image Name: [text field]
 - Serial Number: [text field]
 - Device Owner's Email Address: [text field]
- Buttons:** OK, Cancel

93785

The SNMP v3 section of the PIX Device Properties window contains the following fields:

- **SNMP Security Level** (optional) Choices include: Default (<default_set_in_DCPL>), Authentication/No Encryption, and Authentication/Encryption. Default: Default (<default_set_in_DCPL>). Note: When you change the DCPL property, the <default_set_in_DCPL> variable changes.
- **Authentication User Name** (optional) User name configured on the specified device router. User must have permission to the object identification numbers (OIDs) specified in the security request (that is, write permission for a set request, and read permission for a get request). Should match what is configured on the target router device. Should be provisioned if the SNMP Security Level is Authentication/No Encryption or Authentication/Encryption. Limited to 80 characters.
- **Authentication Password** (optional) Displayed as stars (*). Should be provisioned if the SNMP Security Level is Authentication/No Encryption or Authentication/Encryption. Should match what is configured on the target router device. Limited to 80 characters.
- **Verify Authentication Password** (optional) Displayed as stars (*). Must match the Encryption Password field. Limited to 80 characters.
- **Authentication Algorithm** (optional) Should be provisioned if the SNMP Security Level is Authentication/No Encryption or Authentication/Encryption. Choices include: None, MD5, and SHA. Default: None.

- **Encryption Password** (optional) Displayed as stars (*). In previous versions of ISC, this field was called Privacy Password. Should match what is configured on the target router device. Should be provisioned if the SNMP Security Level is Authentication/Encryption. Limited to 80 characters.
- **Verify Encryption Password** (optional) Displayed as stars (*). Must match the Encryption Password field. Limited to 80 characters.
- **Encryption Algorithm** (optional) In previous versions of ISC, this field was called Privacy Protocol. Should be provisioned if the SNMP Security Level is Authentication/Encryption. Choices include: None and DES 56. Default: None.

The Terminal Server Options section of the PIX Device Properties window contains the following fields:

- **Terminal Server** (optional) Choices include: None and the list of existing Terminal Server names. Default: None.
- **Port** (optional) Disabled until a Terminal Server is selected. Range: 0-65535. Default: 0.

The Failover Options section of the PIX Device Properties window contains the following fields:

- **Failover Type** Determines whether failover is enabled for this PIX device. Choices: None, Normal, and Stateful. Default: None.
- **LAN Based Failover** (optional) Enabled only if the Failover Type is Normal or Stateful.
- **Failover LAN Key** (optional) The key used in LAN based Failover. Limited to 20 characters.

The Device Platform Information section of the PIX Device Properties window contains the following fields:

- **Platform** (optional) Should match what is configured on the target router device. Limited to 80 characters.
- **Software Version** (optional) Should match what is configured on the target router device. Limited to 80 characters.
- **Image Name** (optional) Should match what is configured on the target router device. Limited to 80 characters.
- **Serial Number** (optional) Should match what is configured on the target router device. Limited to 80 characters.
- **Device Owner's Email Address** (optional) Used in the To: field when the Email button is selected from the device list. Limited to 80 characters and must be valid Email format.

Step 6 Enter any desired Additional Properties information for the PIX Firewall device you are creating.

Step 7 Click **OK**.

Step 8 Click **Save**.

The Devices window reappears with the new PIX Firewall device listed.

Creating a Cisco CNS IE2100



Note

To use the Cisco CNS IE2100 functionality on ISC, you must first set up the Cisco CNS IE2100 appliance and the ISC workstation as explained in Appendix B, “Setting Up Cisco CNS IE2100 Appliances Running Cisco CNS Configuration Engine 1.3 Software with ISC” in *Cisco IP Solution Center Installation Guide*. You must also create a Cisco IOS device to communicate with the Cisco CNS IE2100 appliance. See Appendix A, “Setting Up Oracle for ISC,” in *Cisco IP Solution Center Installation Guide*.

To create a Cisco CNS IE2100 appliance, do the following:

- Step 1** Navigate **Service Inventory > Inventory and Connection Manager > Devices**.
- Step 2** Click the **Create** button.
- Step 3** Select **IE2100**.

The Create IE2100 Device window appears, as shown in [Figure 3-48](#).

Figure 3-48 Create IE2100 Device Window

The screenshot shows a window titled 'Create IE2100 Device Window'. The 'General' section contains four text input fields: 'Device Host Name *', 'Device Domain Name', 'Description', and 'IP Address'. The 'Device Host Name' field has a small asterisk next to it. At the bottom right of the form are 'Save' and 'Cancel' buttons. Below the form, a note states: 'Note: * - Required Field'. A small number '96322' is visible in the bottom right corner of the window frame.

The General section of the Create IE2100 Device window contains the following fields:

- **Device Host Name** (required) Must begin with a letter, digit, or underscore followed by letters, digits, underscores, spaces, hyphens, or dots ending with a letter, digit, or underscore. This field must match the name configured on the target router device. Limited to 256 characters.
- **Device Domain Name** (optional) Must begin with a letter, digit, or underscore followed by letters, digits, underscores, spaces, hyphens, or dots ending with a letter, digit, or underscore. The name must match the domain name on the target router device.
- **Description** (optional) Limited to 80 characters. Can contain any pertinent information about the device such as the type of device, its location, or other information that might be helpful to service provider operators.
- **IP Address** (optional) Valid IP address of the Cisco CNS IE2100 device that ISC uses to configure the target router device.

Step 4 Enter the desired information for the Cisco CNS IE2100 device you are creating.

Step 5 Click **Save**.

The Devices window reappears with the new Cisco CNS IE2100 device listed.

Editing a Device

From the Edit window, you can modify the fields that have been specified for a particular device.

To access the Edit window, do the following:

Step 1 Navigate **Service Inventory > Inventory and Connection Manager > Devices** to access the Devices window shown in [Figure 3-49](#).

Figure 3-49 *Devices List Window*



Step 2 Select a single device to edit by selecting the box to the left of the Device Name. You can also select a device to edit by clicking on the hyper link of the device name.

Step 3 Click the **Edit** button. This button is only enabled if a device is selected.

The Edit window appropriate to the type of device selected appears. For example, if you selected a Cisco IOS device the Edit Cisco IOS Device window appears, as shown in [Figure 3-50](#).

Figure 3-50 Editing a Device Window

Edit Cisco IOS Device

General

Device Host Name :

ence132

Device Domain Name:

Description:

Collection Zone:

None

Management IP Address:

192.168.115.116

Interfaces:

192.168.129.93/30, 192.168.115.116/32

Edit

Associated Groups

Edit

Login and Password Information

Login User:

Login Password:

xxxx

Verify Login Password:

xxxx

Enable User:

Enable Password:

xxxx

Verify Enable Password:

xxxx

Device and Configuration Access Information

Terminal Session Protocol:

Default (Telnet)

Config Access Protocol:

Default (Terminal)

SNMP Version:

Default (SNMP v1/v2c)

SNMP v1/v2c

Community String RO:

public

Community String RW:

private

Additional Properties

Edit

Save

Cancel

Note: * - Required Field

116248

Step 4 Enter the changes you want to make to the selected device.

Step 5 Click **Save**.

The changes are saved and the Devices window reappears.

Cisco IP Solution Center Infrastructure Reference, 4.0

3-74

OL-6370-01

Deleting Devices

From the Delete window, you can remove selected devices from the database.

To access the Delete window, do the following:

- Step 1** Navigate **Service Inventory > Inventory and Connection Manager > Devices** to access the Devices window shown in [Figure 3-51](#).

Figure 3-51 *Devices List Window*

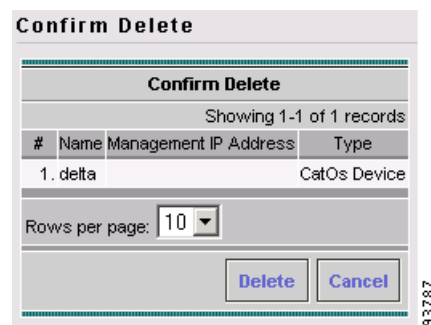


- Step 2** Select one or more devices to delete by selecting the check box(es) to the left of the Device Name(s).

- Step 3** Click the **Delete** button. This button is only enabled if one or more devices are selected.

The Confirm Delete window appears, as shown in [Figure 3-52](#).

Figure 3-52 *Confirm Delete Window*



- Step 4** Click the **Delete** button to confirm that you want to delete the device(s) listed.
The Devices window reappears with the specified device(s) deleted.

Editing a Device Configuration

From the Config window, you can edit the configuration for a specified device.

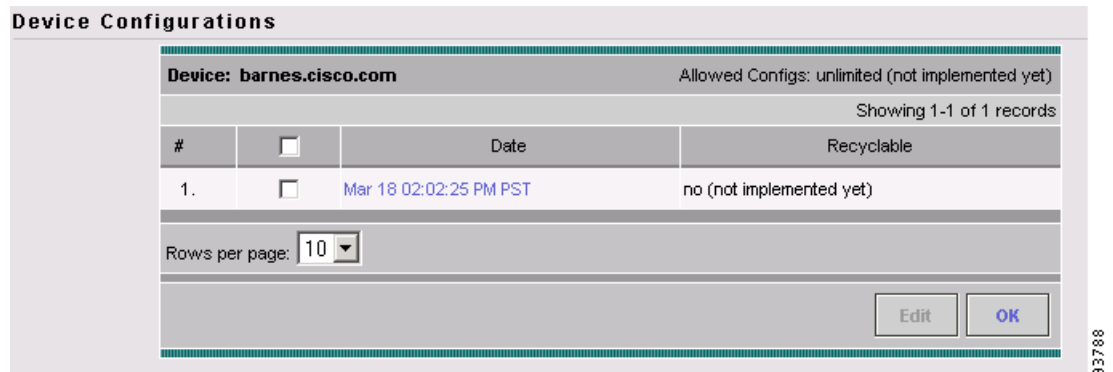
To access the Config window, do the following:

- Step 1** Navigate **Service Inventory > Inventory and Connection Manager > Devices** to access the Devices window shown in [Figure 3-53](#).

Figure 3-53 *Devices List Window*

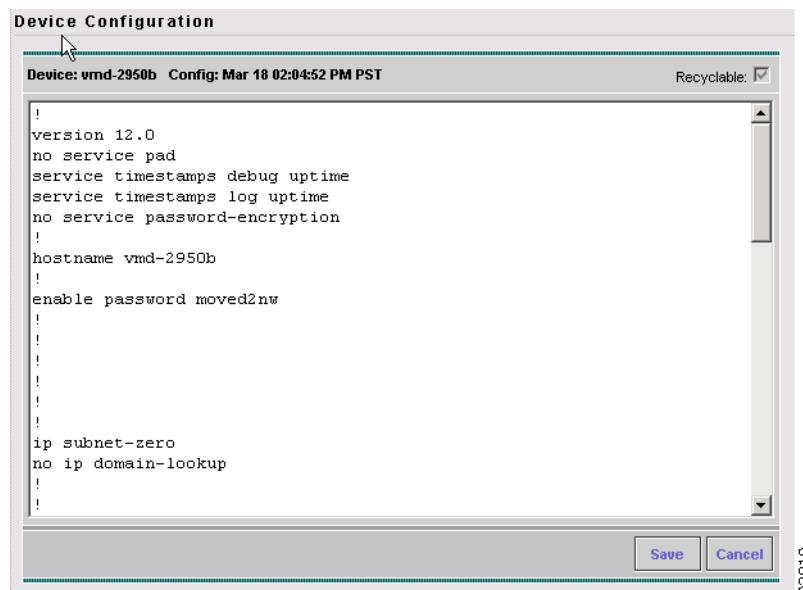


- Step 2** Select a single device to modify by selecting the check box to the left of the Device Name.
- Step 3** Click the **Config** button.
- The Device Configurations window for the selected device appears, as shown in [Figure 3-54](#).

Figure 3-54 Device Configurations Window

- Step 4** Select the box to the left of the Date for the configuration that you want to modify and click the **Edit** button. This button is only enabled if a device is selected.

The Device Configuration window for the selected device appears, as shown in [Figure 3-55](#).

Figure 3-55 Device Configuration Window

- Step 5** Enter the changes you want to make to the selected device configuration.

- Step 6** Click **Save**.

The changes are saved and the Device Configurations window reappears.

- Step 7** Click **OK** to return to the Devices window.

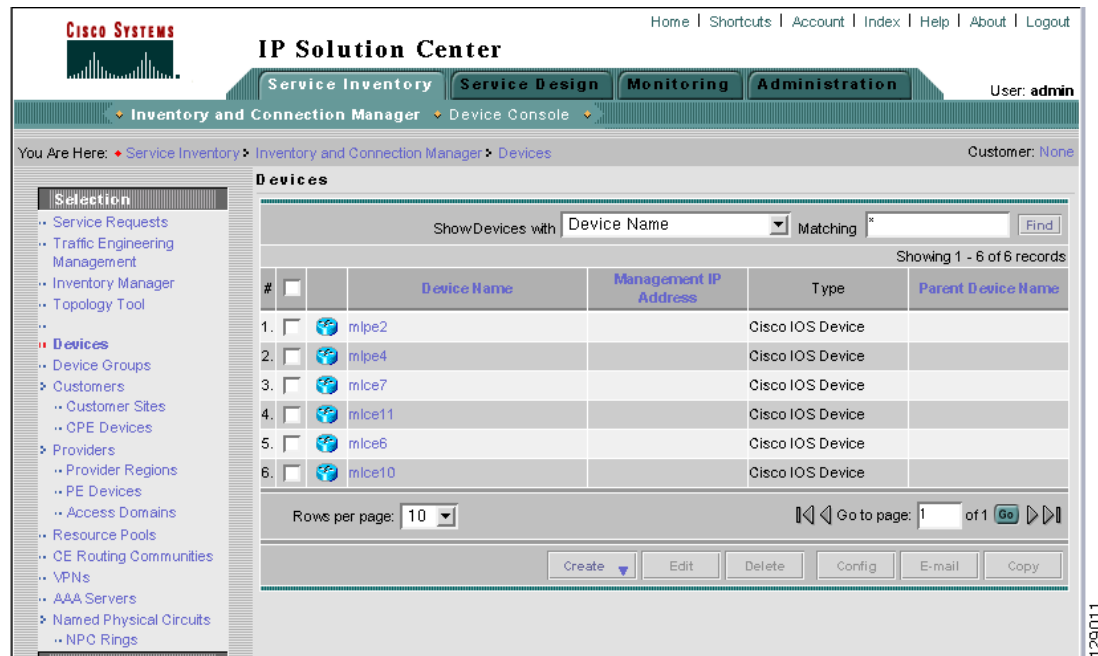
E-mailing a Device's Owner

From the E-mail window, you can send a device report via e-mail to the owners of specified devices.

To access the E-mail window, do the following:

- Step 1** Navigate **Service Inventory > Inventory and Connection Manager > Devices** to access the Devices window shown in [Figure 3-56](#).

Figure 3-56 *Devices List Window*



- Step 2** Select the devices for which you want to send a device report by selecting the check box(es) to the left of the Device Name(s).
- Step 3** Click the **E-Mail** button. This button is only enabled if one or more devices are selected.
- The Send Mail to Device Owners window appears, as shown in [Figure 3-57](#).

Figure 3-57 Send Mail to Device Owners Window

Send Mail to Device owners

Please separate E-mail addresses using comma.

To:

CC:

Subject: Device Report

Message:

Send Cancel

93789

Step 4 Compose the e-mail that you want to send to the selected device owners.

Step 5 Click **Send**.

The e-mail is sent and the Devices window reappears.

Copying a Device

From the Copy window, you receive a copy of the chosen device and can name it and change values.

To access the Copy window, do the following:

Step 1 Navigate **Service Inventory > Inventory and Connection Manager > Devices** to access the Devices window shown in [Figure 3-58](#).

Figure 3-58 Devices List Window



Step 2 Select a single device to copy by selecting the check box to the left of the Device Name.

Step 3 Click the **Copy** button. This button is only enabled if a device is selected.

A window appropriate to the type of device selected to copy appears. You receive an exact copy of the selected device but the Name, Management IP Address, all Interfaces, and VPNSM blades for a Catalyst Switch running Cisco IOS are blanked out and you must fill in the required information and save this new device. See the “[Creating a Device](#)” section on [page 3-45](#) for specifics.

Device Groups

Every network element that ISC manages must be defined as a device in the system. After you have defined your network elements as devices, you can organize the devices into groups for collection and management purposes.

This section describes how to create, edit, and delete device groups and e-mail device group owners. This section includes the following:

- [Accessing the Device Groups Window, page 3-81](#)
- [Creating a Device Group, page 3-81](#)
- [Editing a Device Group, page 3-84](#)
- [Deleting Device Groups, page 3-84](#)
- [E-mailing a Device Group, page 3-85](#)

Accessing the Device Groups Window

The Device Groups feature is used to create, edit, and delete device groups and e-mail device group owners.

To access the Device Groups window, do the following:

- Step 1** Navigate **Service Inventory > Inventory and Connection Manager > Device Groups** to access the Device Groups window shown in [Figure 3-59](#).

Figure 3-59 Device Groups Window

The screenshot shows the 'Device Groups' window. At the top, there is a search bar with the text 'Show Device Groups with' followed by a dropdown menu set to 'Device Group Name', the word 'matching', and a text input field with an asterisk. A 'Find' button is to the right. Below the search bar, it says 'Showing 1-4 of 4 records'. The main area contains a table with two columns: '# Device Group Name' and 'Description'. The table has four rows, each with a checkbox and a device group name: 1. group1, 2. Device Group 1, 3. Device Group B, and 4. DeviceC. Below the table, there is a 'Rows per page' dropdown set to '10'. At the bottom right, there are four buttons: 'Create', 'Edit', 'Delete', and 'Email'.

The Device Groups window contains the following:

- **Device Group Name** Lists the name of the device group. You can sort the list by device group name.
- **Description** Lists the description of the device group.

From the Device Groups window, you can create, edit, or delete device groups or e-mail device group owners using the following buttons:

- **Create** Click to create new device groups. Enabled only if no device group is selected.
- **Edit** Click to edit a selected device group (select device group by clicking the corresponding box). Enabled only if a single device group is selected.
- **Delete** Click to delete selected device group(s) (select device group by clicking the corresponding box). Enabled only if one or more device groups are selected.
- **E-mail** Click to send e-mail to the owner of a selected device group (select device group by clicking the corresponding box). Enabled only if one or more device groups are selected.

Creating a Device Group

From the Create Device Group window, you can create different device groups.

To create a device group, do the following:

- Step 1** Navigate **Service Inventory > Inventory and Connection Manager > Device Groups**.

Step 2 Click the **Create** button.

The Create Device Group window appears, as shown in [Figure 3-60](#).

Figure 3-60 Create Device Group Window

Create Device Group

Name *

Description:

Devices:

#	Name	Description
Rows per page: 10 Go to page: 1 of 1 Go Previous Next		

Note: * - Required Field

117443

The Create Device Group window contains the following fields:

- **Name** (required) Must begin with a letter, digit, or underscore followed by letters, digits, underscores, spaces, hyphens, or dots ending with a letter, digit, or underscore. Limited to 80 characters.
- **Description** (optional) Any pertinent information about the device group that could be helpful to service provider operators. Limited to 512 characters.

Step 3 Enter the name and the description of the Device Group that you are creating.

Step 4 Click **Edit**.

The Select Group Members window appears, as shown in [Figure 3-61](#).

Figure 3-61 Select Group Members Window

Select Group Members

Members of the Device Group <>>

Show with matching

Showing 1-10 of 26 records

#	☐	Name	Type
1.	☐	ipsec-cpe-london.cisco.com	Cisco IOS Device
2.	☐	ipsec-cpe-paris.cisco.com	Cisco IOS Device
3.	☐	ence11	Cisco IOS Device
4.	☐	ence132	Cisco IOS Device
5.	☐	ence21	Cisco IOS Device
6.	☐	ence51	Cisco IOS Device
7.	☐	ence61	Cisco IOS Device
8.	☐	ipsec-cpe-london	Cisco IOS Device
9.	☐	ipsec-cpe-ny	Cisco IOS Device
10.	☐	barnes.cisco.com	Cisco IOS Device

Rows per page: Page 1 of 3 | 2 | 3 |

93822

Step 5 Select the devices that you want to be group members by selecting the check box to the left of the device name.

Step 6 Click **OK**.

The Create Device Group window appears listing the selected devices, as shown in [Figure 3-62](#).

Figure 3-62 Create Device Group Window

Create Device Group

Name *:

Description:

Devices:

#	Name	Description
1.	a2100	
2.	ats-18.cisco.com	

Rows per page: Go to page: of 1

Note: * - Required Field

117444

Step 7 Click **Save**.

The Device Groups window reappears with the new device group listed.

Editing a Device Group

From the Edit Device Group window, you can modify the fields that have been specified for a particular device group.

To access the Edit Device Group window, do the following:

Step 1 Navigate **Service Inventory > Inventory and Connection Manager > Device Groups**.

Step 2 Select a single device group to modify by selecting the check box to the left of the Device Group Name.

Step 3 Click the **Edit** button. This button is only enabled if a device group is selected.

The Edit Device Group window appears, as shown in [Figure 3-63](#).

Figure 3-63 Edit Device Group Window

Edit Device Group

Name * : group2

Description:

Devices:

#	Name	Description
Rows per page: 10 Go to page: 1 of 1 Go		

Save Cancel

Note: * - Required Field

117445

Step 4 Enter the changes you want to make to the selected device group.

Step 5 Click **Save**.

The changes are saved and the Device Groups window reappears.

Deleting Device Groups

From the Delete window, you can remove selected device groups from the database.

To access the Delete window, do the following:

Step 1 Navigate **Service Inventory > Inventory and Connection Manager > Device Groups**.

- Step 2** Select one or more device groups to delete by selecting the check box(es) to the left of the Device Group Names.
- Step 3** Click the **Delete** button. This button is only enabled if one or more device groups are selected. The Confirm Delete window appears, as shown in [Figure 3-64](#).

Figure 3-64 Confirm Delete Window

The screenshot shows a window titled "Confirm Delete". Inside, there is a table with the following data:

#	Name	Description	Associated Devices
1.	San Jose	Devices located in San Jose.	ence51, ence61

Below the table, it says "Showing 1-1 of 1 records". There is a "Rows per page:" dropdown menu set to "10". At the bottom right, there are two buttons: "Delete" and "Cancel".

- Step 4** Click the **Delete** button to confirm that you want to delete the device group(s) listed. The Device Groups window reappears with the specified device group(s) deleted.

E-mailing a Device Group

From the E-mail window, you can send a device report via e-mail to the owners of specified device groups.

To access the E-mail window, do the following:

- Step 1** Navigate **Service Inventory > Inventory and Connection Manager > Device Groups**.
- Step 2** Select the device groups for which you want to send a device report by selecting the check box to the left of the Device Group Name.
- Step 3** Click the **E-Mail** button. This button is only enabled if one or more device groups are selected. The Send Mail to Device owners of selected groups window appears, as shown in [Figure 3-65](#).

Figure 3-65 Send Mail to Device Owners of Selected Groups Window

Step 4 Compose the e-mail that you want to send to the selected device group owners.

Step 5 Click **Send**.

The e-mail is sent and the Device Groups window reappears.

Customers

A customer site is a set of IP systems with mutual IP connectivity between them without the use of a VPN. Each customer site belongs to exactly one customer. A customer site can contain one or more (for load balancing) edge device routers. This section describes how to create, edit, and delete customers. This section includes the following:

- [Accessing the Customers Window, page 3-86](#)
- [Creating a Customer, page 3-87](#)
- [Editing a Customer, page 3-88](#)
- [Deleting Customers, page 3-89](#)
- [Creating Customer Sites, page 3-90](#)
- [CPE Devices, page 3-91](#)

Accessing the Customers Window

The Customers feature is used to create, edit, and delete customers.

To access the Customers window, do the following:

- Step 1** Navigate **Service Inventory > Inventory and Connection Manager > Customers** to access the Customers window shown in [Figure 3-66](#).

Figure 3-66 Customers Window

The screenshot shows the 'Customers' window. At the top, there is a search bar with the text 'Show Customers with Customer Name matching' followed by an asterisk and a text input field. To the right of the input field is a 'Find' button. Below the search bar, it says 'Showing 1-3 of 3 records'. The main area contains a table with three columns: '#', a checkbox, and 'Customer Name'. The table has three rows of data: 1. [checkbox] Customer01, 2. [checkbox] Customer1, and 3. [checkbox] Customer2. Below the table, there is a 'Rows per page:' label with a dropdown menu set to '10'. At the bottom right, there are three buttons: 'Create', 'Edit', and 'Delete'. A vertical text '95238' is visible on the right side of the window.

The Customers window contains the following:

- **Customer Name** Lists the names of customers. You can sort the list by customer name.

From the Customers window, you can create, edit, or delete customers using the following buttons:

- **Create** Click to create new customers.
- **Edit** Click to edit selected customer (select by clicking the corresponding box). Enabled only if a single customer is selected.
- **Delete** Click to delete selected customer (select customer by clicking the corresponding box). Enabled only if one or more customers are selected.

Creating a Customer

From the Create Customer window, you can create different customers.

To create a customer, do the following:

- Step 1** Navigate **Service Inventory > Inventory and Connection Manager > Customers**.

- Step 2** Click the **Create** button.

The Create Customer window appears, as shown in [Figure 3-67](#).

Figure 3-67 Create Customer Window

The Create Customer window contains the following fields:

- **Name** (required) Must begin with a letter. Can contain letters, numbers, and these punctuation characters: period, underscore, and dash. Limited to 80 characters.
- **Customer Abbreviation** This field is used only for L2VPN and L2TPv3 Frame Relay service requests. The entry in this field is used to construct a connect name. When this field is left blank, DLCI switching is the transport mode used. Limited to 10 characters.
- **Customer Information** (optional) Any pertinent information about the customer that could be helpful to service provider operators. Limited to 5256 characters.
- **Site of Origin Enabled** (optional) This check box appears only when you have MPLS permissions. Select this check box to enable the site of origin.

Step 3 Enter the name and information for the Customer that you are creating. Select the **Site of Origin Enabled** check box if you want this enabled.

Step 4 Click **Save**.

The Customers window reappears with the new customer listed.

Editing a Customer

From the Edit Customer window, you can modify the fields that have been specified for a particular customer.

To access the Edit Customer window, do the following:

Step 1 Navigate **Service Inventory > Inventory and Connection Manager > Customers**.

Step 2 Select a single customer to modify by selecting the check box to the left of the Customer Name.

Step 3 Click the **Edit** button. This button is only enabled if a customer is selected.

The Edit Customer window appears, as shown in [Figure 3-68](#).

Figure 3-68 Edit Customer Window

Edit Customer

Name * : Customer1

Customer Abbreviation: CUST1

Contact Information:

Enable Site of Origin: ☐

Save Cancel

Note: * - Required Field

129012

Step 4 Enter the changes you want to make to the selected customer.

Step 5 Click **Save**.

The changes are saved and the Customers window reappears.

Deleting Customers

From the Delete window, you can remove selected customers from the database.

To access the Delete window, do the following:

Step 1 Navigate **Service Inventory > Inventory and Connection Manager > Customers**.

Step 2 Select one or more customers to delete by selecting the check box to the left of the Customer Name.

Step 3 Click the **Delete** button. This button is only enabled if one or more customers are selected.

The Confirm Delete window appears, as shown in [Figure 3-69](#).

Figure 3-69 Confirm Delete Window

Delete Customer

Confirm Delete

Showing 1-1 of 1 records

#	Name
1.	Customer2

Rows per page: 10

Delete
Cancel

- Step 4** Click the **Delete** button to confirm that you want to delete the customer(s) listed. The Customers window reappears with the specified customer(s) deleted.

Creating Customer Sites

To access the Customer Sites window, do the following:

- Step 1** Navigate **Service Inventory > Inventory and Connection Manager**.
- Step 2** Click on **Customer Sites** listed in the Inventory and Connection Manager tree in the left column as shown in Figure 3-70.
- The Customer Sites window appears.

Figure 3-70 Customer Sites Window

Cisco Systems
IP Solution Center

Service Inventory
Service Design
Monitoring
Administration

Inventory and Connection Manager
Device Console

You Are Here: Service Inventory > Inventory and Connection Manager > Customers > Customer Sites
Customer: None

Selection

- Service Requests
- Traffic Engineering Management
- Inventory Manager
- Topology Tool
- Devices
- Device Groups
- Customers
 - Customer Sites
 - CPE Devices
- Providers
 - Provider Regions
 - PE Devices
 - Access Domains
- Resource Pools
- CE Routing Communities
- VPNs
- AAA Servers
- Named Physical Circuits
 - NPC Rings

Show Sites with Site Name Matching
Find

Showing 1 - 2 of 2 records

#	Site Name	Customer Name
1.	NY	Customer1
2.	SF	Customer1

Rows per page: 10

Go to page: 1 of 1 Go

Create
Edit
Delete

The Customer Sites window contains the following:

- **Site Name** Lists the names of sites. The first character must be a letter. Can contain letters, numbers, and these punctuation characters: period, underscore, and dash. Limit: 80 characters. You can sort the list by site name.
- **Customer Name** Lists the names of customer. The first character must be a letter. Can contain letters, numbers, and these punctuation characters: period, underscore, and dash. Limit: 80 characters. You can sort the list by customer name.

From the Customer Sites window, you can create, edit, or delete customer sites using the following buttons:

- **Create** Click to create new customer sites. Enabled only if no customer site is selected.
- **Edit** Click to edit selected customer sites (select by clicking the corresponding box). Enabled only if a single customer site is selected.
- **Delete** Click to delete selected customer site(s) (select by clicking the corresponding box). Enabled only if one or more customer sites are selected.

CPE Devices

The CPE feature provides a list of CPEs that have been associated with a site through the CPE editor or Inventory Manager. To access the CPE Devices window, do the following:

- Step 1** Navigate **Service Inventory > Inventory and Connection Manager**.
- Step 2** Click on **CPE Devices** listed in the Inventory and Connection Manager tree in the left column, as shown in [Figure 3-71](#).

The CPE Devices window appears.

Figure 3-71 CPE Devices Window

The screenshot displays the Cisco IP Solution Center interface. The main window is titled "CPE Devices" and shows a table of devices. The table has the following columns: #, Device Name, Customer Name, Site Name, Management Type, and Service Request. The data rows are:

#	Device Name	Customer Name	Site Name	Management Type	Service Request
1.	mlce7	Customer1	SF	Managed	L2VPN
2.	mlce11	Customer1	NY	Managed	L2VPN
3.	mlce6	Customer1	SF	Managed	L2VPN
4.	mlce10	Customer1	NY	Managed	L2VPN

The interface also includes a search bar at the top with "Show CPEs with" and "Device Name" selected, and a "Find" button. Below the table, there are controls for "Rows per page" (set to 10) and "Go to page" (set to 1 of 1). At the bottom right, there are buttons for "Create", "Edit", "Deploy", and "Delete".

129038

The CPE Devices window contains the following:

- **Device Name** Lists the names of devices. The first character must be a letter. Can contain letters, numbers, and these punctuation characters: period, underscore, and dash. Limit: 80 characters. You can sort the list by device name.
- **Customer Name** Lists the names of customer. The first character must be a letter. Can contain letters, numbers, and these punctuation characters: period, underscore, and dash. Limit: 80 characters. You can sort the list by customer name.
- **Site Name** Lists the names of sites. The first character must be a letter. Can contain letters, numbers, and these punctuation characters: period, underscore, and dash. Limit: 80 characters. You can sort the list by site name.
- **Management Type** When associating a CE with a customer site, you can select Managed or Unmanaged. Other choices are available (see below), but they should not be confused with this primary choice.
 - **Managed**—A managed CE can be provisioned directly by the provider using ISC. The CE must be reachable from an ISC server.
 - **Unmanaged** —An unmanaged CE cannot be provisioned directly by the provider. If Unmanaged is selected, the provider can use ISC to generate a configuration, and then send the configuration to the customer for placement on the CE.
 - **Managed - Management LAN** —A managed Management LAN or Management CE (MCE) is configured like a managed CE router, but it resides in the provider space. Normally, an MCE acts as the network operations center (NOC) gateway router.
 - **Unmanaged - Management LAN** —An unmanaged Management LAN or MCE is configured like an unmanaged CE router, but it resides in the provider space. Normally, an MCE acts as the network operations center (NOC) gateway router.
 - **Directly Connected** —In most cases, the CE is connected to a PE router. In this case, the CE is connected to a workstation or other device.
 - **Directly Connected Management Host** —In most cases, the CE is connected to a PE router. In this case, the CE is connected to a workstation or other device, on which ISC resides.
 - **Multi-VRF** —A multi-VRF CE (MVRFCPE) is owned by the customer, but resides in the provider space. It is used to off load traffic from the PE.
 - **Unmanaged Multi-VRF**—An unmanaged multi-VRF CE is provisioned like an unmanaged CE (configurations are not uploaded or downloaded to the device by the provider). It is owned by the customer and resides in the provider space.

Create CPE Device

Click **Create** to create new CPE devices. Enabled only if no customer site is selected. The resulting window is shown in [Figure 3-72](#), “[Create CPE Device](#).”

Figure 3-72 Create CPE Device

Create CPE Device

Device Name *		Select
Site Name *		Select
Management Type:	Managed	▼

Save Cancel

Note: * - Required Field

116250

Edit CPE Device

Click **Edit** to edit a single CPE device selected in [Figure 3-71](#). The result is a window as shown in the example in [Figure 3-73](#), “[Edit CPE Device](#).”

Figure 3-73 Edit CPE Device

Edit CPE Device

Device Name:ence51

Site Name:Site-ence51

Customer Name:Customer1

Management Type:Managed

Pre-shared Keys:

IPsec High Availability Options:

None

Normal Failover

Stateful Failover

IPsec Public IP Address:

IP Address Ranges10.5.5.0/30, 192.168.129.136/30

Edit

Show Interfaces withNameMatchingFind

Showing 1 - 6 of 6 records

#	Interface Name	IP Address	IP Address Type	Encapsulation	Description	IPsec	Firewall	NAT	QoS Candidate
1.	Ethernet0	192.168.129.137/30	STATIC	UNKNOWN	Link to ensu3 (192.168.129.138) ! DON'T MODIFY or REMOVE !	None	None	Inside	None
2.	Ethernet1	10.5.5.1/30	STATIC	UNKNOWN	GRE Tunnel Unnumbered Interface ! DON'T MODIFY or REMOVE !	None	Inside	Outside	None
3.	FastEthernet0		STATIC	UNKNOWN		None	Outside	None	None
4.	Loopback0	192.168.115.81/32	STATIC	UNKNOWN	DNS entry for ence51 ! DON'T MODIFY or REMOVE !	None	None	None	None
5.	Loopback1	11.11.11.1/32	STATIC	UNKNOWN	IPSec Secured Tunnel Endpoint ! DON'T MODIFY or REMOVE !	None	None	None	None
6.	Loopback2	12.12.12.1/32	STATIC	UNKNOWN	IPSec Secured Tunnel Endpoint ! DON'T MODIFY or REMOVE !	None	None	None	None

Rows per page:All

Go to page:1 of 1Go

Save

Cancel

116251

Deploy CPE Device

- NOT SUPPORTED in this release. -

To deploy CPE Device(s), follow these steps:


Note

This **Deploy** button is supported for Site-to-Site VPN, Remote Access VPN, NAT, and Firewall services *only*. The only way to use this **Deploy** button with other services is to find the available Service Requests for the CPE, as explained in [Step 3](#).

- Step 1

In [Figure 3-71](#), select one or more check boxes for the CPE(s) you want to Deploy.
- Step 2

Click the **Deploy** button and you receive a window, as shown in [Figure 3-74](#), “[Service Deployment Task](#).”

Figure 3-74 Service Deployment Task

Service Deployment Task

Deployment Task: 2004-02-22 23:16:15.07

Service Requests *: 12 Select/Deselect

Options:

- ☐ Force Deployment
- ☒ Provision and Audit
- ☐ Regenerate IPsec Pre-shared Keys

Schedule:

- ☒ Now
- ☐ Later
- ☐ None

Later Schedule * Edit

Task Owner:

- ☒ Customer
- ☐ Provider
- ☐ None

Submit Cancel

Note: * - Required Field

- Step 3** In **Service Requests** in [Figure 3-74](#), click the **Select/Deselect** button and you will receive a window from which you can select and deselect Service Requests you want to deploy.

**Caution**

Be sure to only select IPsec, IPsec Remote Access, NAT, or Firewall Service Requests. If you are using a service other than these, go no further.

- Step 4** Click **Select**.
- Step 5** In **Options**, choose: **Force Deployment**; **Provision and Audit**; or **Regenerate IPsec Pre-shared Keys**
- Step 6** In **Schedule**, choose **Now**; **Later**; or **None**. If you choose **Later**, a **Later Schedule** category appears. Click that **Edit** button and you will receive a Task Schedule window from which you can choose how often to deploy the chosen Service Requests and when to start and stop this process. Make your choices and click **OK**.
- Step 7** For Task Owner, choose **Customer**; **Provider**; or **None**.
- Step 8** Click **Submit**.

Delete CPE Device

Click to delete selected CPE device(s) (select by clicking the corresponding box). Enabled only if one or more CPE devices are selected.

Providers

This section describes how to create and manage providers. This section includes the following:

- [Accessing the Providers Window, page 3-96](#)

- [Creating a Provider, page 3-97](#)
- [Editing a Provider, page 3-97](#)
- [Deleting Providers, page 3-98](#)
- [Creating Provider Regions, page 3-99](#)
- [Creating PE Devices, page 3-100](#)
- [Creating Access Domains, page 3-101](#)

Accessing the Providers Window

The Providers feature is used to create and manage providers.

To access the Providers window, do the following:

- Step 1** Navigate **Service Inventory > Inventory and Connection Manager > Providers** to access the Providers window shown in [Figure 3-75](#).

Figure 3-75 Providers Window

The screenshot shows the 'Providers' window. At the top, there is a search bar with the text 'Show Providers with Provider Name matching' and a 'Find' button. Below the search bar, it says 'Showing 1-3 of 3 records'. The main part of the window is a table with the following data:

#	☐	Provider Name	BGP AS
1.	☐	Provider1	100
2.	☐	Provider2	200
3.	☐	ProviderA	300

Below the table, there is a 'Rows per page' dropdown menu set to '10'. At the bottom right, there are three buttons: 'Create', 'Edit', and 'Delete'.

The Providers window contains the following:

- **Provider Name** Lists the names of providers. You can sort the list by provider name.
- **BGP AS** The Unique number assigned to each BGP autonomous system.

From the Providers window, you can create, edit, or delete providers using the following buttons:

- **Create** Click to create new providers. Enabled only if no customer is selected.
- **Edit** Click to edit selected provider (select the corresponding box). Enabled only if a single provider is selected.
- **Delete** Click to delete a selected provider (select the corresponding box). Enabled only if one or more providers are selected.

Creating a Provider

From the Create Provider window, you can create different providers.

To create a provider, do the following:

Step 1 Navigate **Service Inventory > Inventory and Connection Manager > Providers**.

Step 2 Click the **Create** button.

The Create Provider window appears, as shown in [Figure 3-76](#).

Figure 3-76 Create Provider Window

The Create Provider window contains the following fields:

- **Name** (required) Must begin with a letter. Can contain letters, numbers, and these punctuation characters: period, underscore, and dash. Limited to 80 characters.
- **BGP AS** (required) Each BGP autonomous system is assigned a unique 16-bit number by the same central authority that assigns IP network numbers. Range: 1 to 65535.
- **Contact Information** (optional) Any pertinent information about the provider that could be helpful to service provider operators. Limited to 256 characters.

Step 3 Enter the name, BGP AS, and any contact information for the Provider that you are creating.

Step 4 Click **Save**.

The Providers window reappears with the new provider listed.

Editing a Provider

From the Edit Provider window, you can modify the fields that have been specified for a particular provider.

To access the Edit Provider window, do the following:

- Step 1** Navigate **Service Inventory > Inventory and Connection Manager > Providers**.
- Step 2** Select a single provider to modify by selecting the check box to the left of the Provider Name.
- Step 3** Click the **Edit** button. This button is only enabled if a customer is selected.

The Edit Provider window appears, as shown in [Figure 3-77](#).

Figure 3-77 Edit Provider Window

- Step 4** Enter the changes you want to make to the selected provider.
- Step 5** Click **Save**.

The changes are saved and the Providers window reappears.

Deleting Providers

From the Delete window, you can remove selected providers from the database.

To access the Delete window, do the following:

- Step 1** Navigate **Service Inventory > Inventory and Connection Manager > Providers**.
- Step 2** Select provider(s) to delete by selecting the check box to the left of the Provider Name.
- Step 3** Click the **Delete** button. This button is only enabled if one or more Providers are selected.

The Confirm Delete window appears, as shown in [Figure 3-78](#).

Figure 3-78 Confirm Delete Window

The screenshot shows a window titled "Delete Provider(s)". Inside, there is a section titled "Confirm Delete" with a sub-header "Showing 1-1 of 1 records". Below this is a table with two columns: "#" and "Name". The table contains one row with the value "1." in the "#" column and "ProviderA" in the "Name" column. Below the table, there is a "Rows per page:" label followed by a dropdown menu set to "10". At the bottom right of the window, there are two buttons: "Delete" and "Cancel". A small number "95246" is visible in the bottom right corner of the window frame.

#	Name
1.	ProviderA

Rows per page: 10

Delete Cancel

- Step 4** Click the **Delete** button to confirm that you want to delete the provider(s) listed. The Providers window reappears with the specified provider(s) deleted.

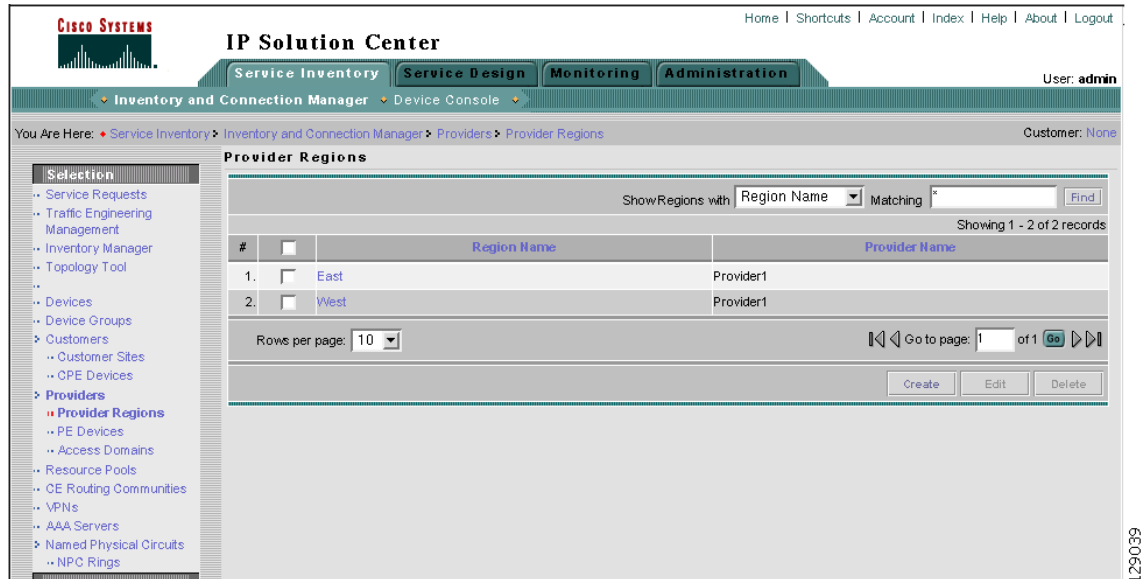
Creating Provider Regions

A Provider Region is considered to be a group of provider edge routers (PEs) within a single BGP autonomous system. The primary objective for defining Provider Regions is to allow a provider to employ unique IP address pools in large Regions, such as Europe, Asia Pacific, and so forth.

To access the Provider Regions window, do the following:

- Step 1** Navigate **Service Inventory > Inventory and Connection Manager**.
- Step 2** Click on **Provider Regions** listed in the Inventory and Connection Manager tree in the left column, as shown in [Figure 3-79](#).
- The Provider Regions window appears.

Figure 3-79 Provider Regions Window



The Provider Regions window contains the following:

- **Region Name** Lists the names of regions. Must begin with a letter. Can contain letters, numbers, and these punctuation characters: period, underscore, and dash. Limited to 80 characters. You can sort the list by region name.
- **Provider Name** Lists the names of providers. Must begin with a letter. Can contain letters, numbers, and these punctuation characters: period, underscore, and dash. Limited to 80 characters. You can sort the list by provider name.

From the Provider Regions window, you can create, edit, or delete provider regions using the following buttons:

- **Create** Click to create new provider regions. Enabled only if no customer is selected.
- **Edit** Click to edit selected provider regions (select the corresponding box). Enabled only if a single provider region is selected.
- **Delete** Click to delete selected provider regions (select the corresponding box). Enabled only if one or more provider regions are selected.

Creating PE Devices

The PE Devices feature provides a list of provider edge routers (PEs) that have been associated with the region, either through the PE editor or Inventory Manager.

To access the PE Devices window, do the following:

- Step 1** Navigate **Service Inventory > Inventory and Connection Manager**.
- Step 2** Click on **PE Devices** listed in the Inventory and Connection Manager tree in the left column, as shown in [Figure 3-80](#).

The PE Devices window appears.

Figure 3-80 PE Devices Window



The PE Devices window contains the following:

- **Device Name** Lists the names of devices. The first character must be a letter. Can contain letters, numbers, and these punctuation characters: period, underscore, and dash. Limit: 80 characters. You can sort the list by device name.
- **Provider Name** Lists the names of providers. Must begin with a letter. Can contain letters, numbers, and these punctuation characters: period, underscore, and dash. Limited to 80 characters. You can sort the list by provider name.
- **Region Name** Lists the names of regions. Must begin with a letter. Can contain letters, numbers, and these punctuation characters: period, underscore, and dash. Limited to 80 characters. You can sort the list by region name.
- **Role Type** Choices include: PE_POP, PE_CLE, PE_CORE, PE_MVRF.

From the PE Devices window, you can create, edit, or delete providers using the following buttons:

- **Create** Click to create new PE device. Enabled only if no PE device is selected.
- **Edit** Click to edit selected PE device (select the corresponding box). Enabled only if a single PE device is selected.
- **Delete** Click to delete selected PE device(s) (select the corresponding box). Enabled only if one or more PE devices are selected.

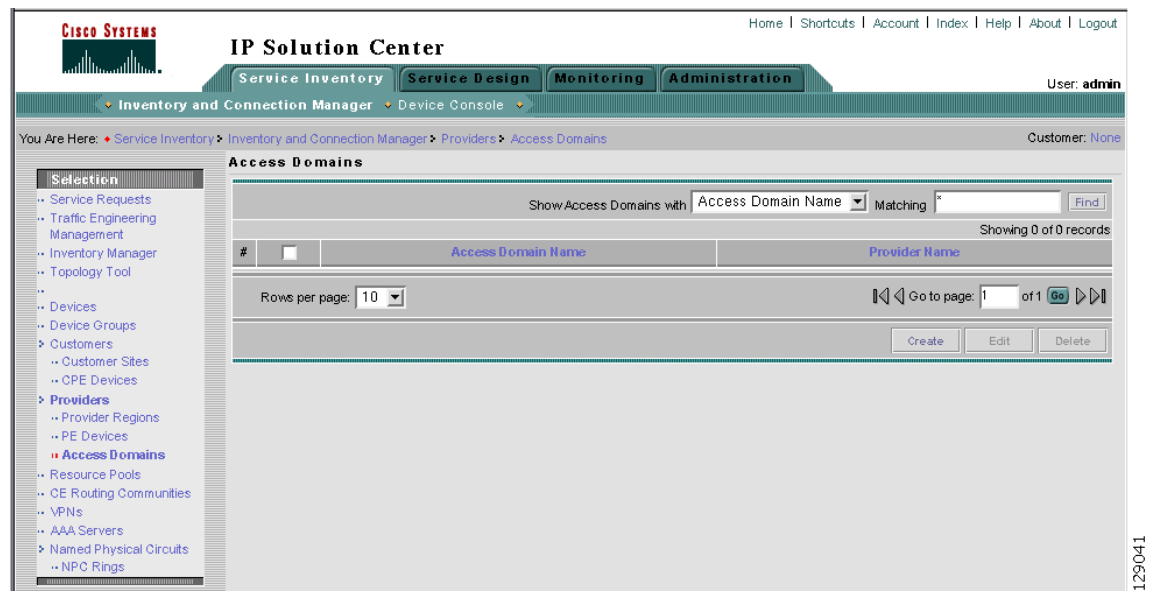
Creating Access Domains

To access the Access Domains window, do the following:

- Step 1** Navigate **Service Inventory > Inventory and Connection Manager**.
- Step 2** Click on **Access Domains** listed in the Inventory and Connection Manager tree in the left column, as shown in Figure 3-81.

The Access Domains window appears.

Figure 3-81 Access Domains Window



The Access Domains window contains the following:

- **Access Domain Name** Lists the names of access domain. The first character must be a letter. Can contain letters, numbers, and these punctuation characters: period, underscore, and dash. Limit: 80 characters. You can sort the list by access domain name.
- **Provider Name** Lists the names of providers. Must begin with a letter. Can contain letters, numbers, and these punctuation characters: period, underscore, and dash. Limited to 80 characters. You can sort the list by provider name.

From the Access Domains window, you can create, edit, or delete access domains using the following buttons:

- **Create** Click to create new access domain. Enabled only if no access domain is selected.
- **Edit** Click to edit selected access domain (select the corresponding box). Enabled only if a single access domain is selected.
- **Delete** Click to delete selected access domain(s) (select the corresponding box). Enabled only if one or more access domains are selected.

Resource Pools

Cisco IP Solution Center enables multiple pools to be defined and used during operations. The following resource pools are available:

- **IP address pool:** The IP address pool can be defined and assigned to regions or VPNs. This feature gives the service operator the flexibility to manage the allocation of all IP addresses in the network.
- **Multicast pool:** The Multicast pool is used for Multicast MPLS VPNs.

- *Route Target (RT) pool*: A route target is the MPLS mechanism that informs PEs as to which routes should be inserted into the appropriate VRFs. Every VPN route is tagged with one or more route targets when it is exported from a VRF and offered to other VRFs. The route target can be considered a VPN identifier in MPLS VPN architecture. RTs are a 64-bit number.
- *Route Distinguisher (RD) pool*: The IP subnets advertised by the CE routers to the PE routers are augmented with a 64-bit prefix called a route distinguisher (RD) to make them unique. The resulting 96-bit addresses are then exchanged between the PEs, using a special address family of Multiprotocol BGP (referred to as MP-BGP). The RD pool is a pool of 64-bit RD values that Cisco IP Solution Center uses to make sure the IP addresses in the network are unique.
- *Site of origin pool*: The pool of values for the site-of-origin (SOO) attribute. The site-of-origin attribute prevents routing loops when a site is multihomed to the MPLS VPN backbone. This is achieved by identifying the site from which the route was learned, based on its SOO value, so that it is not readvertised back to that site from a PE in the MPLS VPN network.
- *VC ID pool*: VC ID pools are defined with a starting value and a size of the VC ID pool. (VC ID is a 32-bit unique identifier that identifies a circuit/port.) A given VC ID pool is not attached to any Inventory object. During the deployment of an Ethernet Service (EWS, ERS for example), VC ID is auto-allocated from the VC ID pool.
- *VLAN ID pool*: VLAN ID pools are defined with a starting value and a size of the VLAN pool. A given VLAN ID pool can be attached to an Access Domain. During the deployment an Ethernet Service (EWS, ERS for example), VLAN ID can be auto-allocated from the Access Domain's VLAN pools. This gives the Service Provider a tighter control of VLAN ID allocation.

All these resources, that are made available to the service provider, enable the automation of service deployment.

This section describes how you can create and manage pools for various types of resources. This section includes the following:

- [Accessing the Resource Pools Window, page 3-103](#)
- [Creating an IP Address Pool, page 3-104](#)
- [Creating a Multicast Pool, page 3-105](#)
- [Creating a Route Distinguisher and Route Target Pool, page 3-106](#)
- [Creating a Site of Origin Pool, page 3-109](#)
- [Creating a VC ID Pool, page 3-111](#)
- [Creating a VLAN Pool, page 3-112](#)
- [Deleting Resource Pools, page 3-113](#)

Accessing the Resource Pools Window

The Resource Pools feature is used to create and manage various types of resource pools.

To access the Resource Pools window, do the following:

-
- Step 1** Navigate **Service Inventory > Inventory and Connection Manager > Resource Pools** to access the Resource Pools window shown in [Figure 3-82](#).

Figure 3-82 Resource Pools Window

Resource Pools

Pool Type: IP Address

Show IP Address Pools with Pool Name matching * of type All Find

Showing 1-6 of 6 records

#	☐	Start	Pool Mask	Pool Size	Status	Type	Pool Name
1.	☐	2.0.0.0	32	16777216	Available	VPN	Customer2:VPN-1
2.	☐	10.10.10.0	30	1	Available	Region	Provider1:US
3.	☐	10.10.10.4	30	1	Allocated	Region	Provider1:US
4.	☐	10.10.10.8	30	62	Available	Region	Provider1:US
5.	☐	10.10.20.0	32	256	Available	Region	Provider1:US
6.	☐	1.0.0.0	30	4194304	Available	Region	Provider2:Western

Rows per page: 10

Create Delete

96247

From the Resource Pools window, you have access to the following buttons:

- **Pool Type** Choices include: IP Address, Multicast Address, Route Distinguisher, Route Target, Site of Origin, VC ID, and VLAN. The fields displayed in the Resource Pools window vary depending on the pool type selected.
- **Create** Click to create new resource pools. Enabled only if no resource pool is selected.
- **Delete** Click to delete selected resource pools (select by clicking the corresponding box). Enabled only if one or more resource pools are selected.

Creating an IP Address Pool

ISC uses IP address pools to automatically assign IP addresses to PEs and CEs. Each Region has an IP address pool to use for IP numbered addresses (/30 pools) and a separate IP address pool for IP unnumbered addresses (/32 loopback address pools).

Within a VPN or extranet, all IP addresses must be unique. Customer IP addresses must not overlap with the provider's IP addresses. Overlapping IP addresses are only possible when two devices cannot see each other—that is, when they are in isolated VPNs.

From the Create IP Address Pool window, you can create IP address pools.

To create an IP address pool, do the following:

- Step 1** Navigate **Service Inventory > Inventory and Connection Manager > Resource Pools**.
- Step 2** Select **IP address** from the **Pool Type** in the upper left of the Resource Pools window.
- Step 3** Click the **Create** button.

The Create IP Address Pool window appears, as shown in [Figure 3-83](#).

Figure 3-83 Create IP Address Pool Window

Create IP Address Pool

IP Address Pool * : (IP Address / Mask)

Pool Mask (bits) * : ☐ 30 ☐ 32

Pool Association * : Region

Note: * - Required Field

96306

The Create IP Address Pool window contains the following fields:

- **IP Address Pool** (required) Text field in the format a.b.c.d/mask, for example 172.0.0.0/8.
- **Pool Mask (bits)** (required) Choices include: **30** and **32**
where:
 30 is used for IP numbered address pools (/30)
 32 is used for IP unnumbered loopback address pools (/32).
- **Pool Association** (required) Choices include: Region and VPN.



Note If you choose **VPN**, an additional optional field appears, **Pool Name Suffix**, when you return to [Figure 3-83](#). This field allows the creation of multiple address pools within the same VPN. If you are creating this address pool for DMVPN usage, the recommendation is to use this field to specify a suffix.

Step 4 Enter the required information for the IP address pool you are creating.

Step 5 Click **Save**.

The Resource Pools window reappears with the new IP address pool listed.

Creating a Multicast Pool

From the Create Multicast Pool window, you can create multicast pools. These pools are global and are not associated with any provider or customer.

To create a multicast pool, do the following:

Step 1 Navigate **Service Inventory > Inventory and Connection Manager > Resource Pools**.

Step 2 Select **Multicast** from the **Pool Type** in the upper left of the Resource Pools window.

Step 3 Click the **Create** button.

The Create Multicast Pool window appears, as shown in [Figure 3-84](#).

Figure 3-84 Create Multicast Pool Window

Create Multicast Pool

Multicast Address*: (IP Address / Mask)

Use for Default MDT: ☒

Use for Data MDT: ☒

Save Cancel

Note: * - Required Field

96303

The Create Multicast Pool window contains the following fields:

- **Multicast Address** (required) Text field in the format a.b.c.d/mask, for example 239.0.0.0/8. Range: 224.0.1.0/8 to 239.255.255.255/32.
- **Use for default MDT** (optional) This is a check box. Default: selected.
- **Use for Data MDT** (optional) This is a check box. The *data MDT* contains a range of multicast group addresses and a bandwidth threshold. Thus, whenever a CE behind a multicast-VRF exceeds that bandwidth threshold while sending multicast traffic, the PE sets up a new data MDT for the multicast traffic from that source. The PE informs the other PEs about this data MDT and, if they have receivers for the corresponding group, the other PEs join this data MDT. Default: selected.

Step 4 Enter the required information for the multicast pool you are creating.

Step 5 Click **Save**.

The Resource Pools window reappears with the new multicast pool listed.

Creating a Route Distinguisher and Route Target Pool

MPLS-based VPNs employ Border Gateway Protocol (BGP) to communicate between PEs to facilitate customer routes. This is made possible through extensions to BGP that carry addresses other than IPv4 addresses. A notable extension is called the route distinguisher (RD).

The purpose of the route distinguisher (RD) is to make the prefix value unique across the network backbone. Prefixes should use the same RD if they are associated with the same set of route targets (RTs) and anything else that is used to select routing policy. The community of interest association is based on the route target (RT) extended community attributes distributed with the Network Layer Reachability Information (NLRI). The RD value must be a globally unique value to avoid conflict with other prefixes.

The MPLS label is part of a BGP routing update. The routing update also carries the addressing and reachability information. When the RD is unique across the MPLS VPN network, proper connectivity is established even if different customers use non-unique IP addresses.

For the RD, every CE that has the same overall role should use a VRF with the same name, same RD, and same RT values. The RDs and RTs are only for route exchange between the PEs running BGP. That is, for the PEs to do MPLS VPN work, they have to exchange routing information with more fields than usual for IPv4 routes; that extra information includes (but is not limited to) the RDs and RTs.

From the Create Route Distinguisher Pool window, you can create route distinguisher pools.

To create a route distinguisher pool, do the following:

- Step 1** Navigate **Service Inventory > Inventory and Connection Manager > Resource pools**.
- Step 2** Select **Route Distinguisher** from the **Pool Type** in the upper left of the Resource Pools window.
- Step 3** Click the **Create** button.

The Create Route Distinguisher Pool window appears, as shown in [Figure 3-85](#).

Figure 3-85 Create Route Distinguisher Pool Window

Create Route Distinguisher Pool

RD Pool Start*: 0 (0 - 2147483646)

RD Pool Size*: 0 (1 - 2147483647)

Provider*:

Note: * - Required Field

The Create Route Distinguisher Pool window contains the following fields:

- **RD Pool Start** (required) Range: 0 to 2147483646.
- **RD Pool Size** (required) Range: 1 to 2147483647.
- **Provider** (required)

- Step 4** Enter the **RD Pool Start** and **Size** information for the route distinguisher pool you are creating.
- Step 5** Click the **Select** button.

The Provider for new Resource Pool window appears, as shown in [Figure 3-86](#).

Figure 3-86 Provider for New Resource Pool Window

Provider for new Resource Pool

Show Providers with Provider Name matching *

Showing 1-3 of 3 records

#	Select	Name
1.	☐	prov
2.	☐	ServiceProvider1
3.	☐	Telia_Sonera

Rows per page: 10

Step 6 Select one of the providers listed and click **Select**.

Step 7 Click **Save**.

The Resource Pools window reappears with the new route distinguisher pool listed.

To create a Route Target Pool, do the following:

Step 1 Navigate **Service Inventory > Inventory and Connection Manager > Resource pools**.

Step 2 Select **Route Target** from the **Pool Type** in the upper left of the Resource Pools window.

Step 3 Click the **Create** button.

The Create Route Target Pool window appears, as shown in [Figure 3-87](#).

Figure 3-87 Create Route Target Pool Window

Create Route Target Pool

RT Pool Start *	0	(0 - 2147483646)
RT Pool Size *	0	(1 - 2147483647)
Provider *		Select

Save Cancel

Note: * - Required Field

96299

The Create Route Target Pool window contains the following fields:

- **RT Pool Start** (required) Range: 0 to 2147483646.
- **RT Pool Size** (required) Range: 1 to 2147483647.
- **Provider** (required)

Step 4 Enter the **RT Pool Start** and **Size** information for the route target pool you are creating.

Step 5 Click the **Select** button.

The Provider for new Resource Pool window appears, as shown in [Figure 3-88](#).

Figure 3-88 Provider for New Resource Pool Window

#	Select	Name
1.	☐	prov
2.	☐	ServiceProvider1
3.	☐	Telia_Sonera

Step 6 Select one of the providers listed and click **Select**.

Step 7 Click **Save**.

The Resource Pools window reappears with the new route target pool listed.

Creating a Site of Origin Pool

In MPLS VPN, CE sites use private/public AS numbers and when one AS number is used for each VPN, all sites belonging to the same VPN share the same private/public AS number. The default BGP behavior is to drop any prefix if its own AS number is already in the AS path. As a result, a customer site does not learn prefixes of a remote site in this situation. AS-OVERRIDE must be configured (if there are hub sites involved, ALLOWAS-IN must be configured) to allow those prefixes to be sent by PE routers but a routing loop can occur.

For example, CE1 and CE2 belong to the same customer VPN and have the same AS number 65001. The AS path between two customer sites is 65001 - 1234 - 65001 and prefixes cannot be exchanged between customer sites because AS 65001 is already in the path. To solve this problem, AS-OVERRIDE options are configured on PE routers; but it introduces a routing loop into the network without using extended community site of origin attributes.

Site of origin is a concept in MPLS VPN architecture that prevents routing loops in sites that are multi-homed to the MPLS VPN backbone and in sites using AS-OVERRIDE in conjunction. Site of origin is a type of BGP extended community attribute used to identify a prefix that originated from a site so that the re-advertisement of that prefix back to the site can be prevented. This attribute uniquely identifies the site from which the PE router learned the route. Site of origin is tagged at PE in peering with BGP neighbors using an inbound route-map and works in conjunction with BGP CE-PE routing protocol.

Site of origin must be unique per customer site per VPN/customer (when these sites are multi-homed). Therefore, the same value of site of origin must be used on PE routers connected to the same CE router or to the same customer site.

**Note**

Each time a customer site is created, ISC generates a unique site of origin value from the selected site of origin provider pool if Site of Origin is enabled. This site of origin value must be unique per customer site per customer/VPN.

From the Create Site of Origin Pool window, you can create site of origin pools.

To create a site of origin pool, do the following:

- Step 1** Navigate **Service Inventory > Inventory and Connection Manager > Resource pools**.
- Step 2** Select **Site of Origin** from the **Pool Type** in the upper left of the Resource Pools window.
- Step 3** Click the **Create** button.

The Create Site of Origin Pool window appears, as shown in [Figure 3-89](#).

Figure 3-89 Create Site of Origin Pool Window

Create Site of Origin Pool

SOO Pool Start *	0	(0 - 2147483646)
SOO Pool Size *	0	(1 - 2147483647)
Provider *		Select

Save Cancel

Note: * - Required Field

96300

The Create Site of Origin Pool window contains the following fields:

- **SOO Pool Start** (required) Range: 0 to 2147483646.
- **SOO Pool Size** (required) Range: 1 to 2147483647.
- **Provider** (required)

- Step 4** Enter the **SOO Pool Start** and **Size** information for the site of origin pool you are creating.
- Step 5** Click the **Select** button.

The Provider for new Resource Pool window appears, as shown in [Figure 3-90](#).

Figure 3-90 Provider for New Resource Pool Window

Step 6 Select one of the providers listed and click **Select**.

Step 7 Click **Save**.

The Site of Origin pools window reappears with the new route target pool listed.

Creating a VC ID Pool

From the Create VC ID Pool window, you can create VC ID pools. These pools are global and are not associated with any provider or customer

To create a VC ID pool, do the following:

Step 1 Navigate **Service Inventory > Inventory and Connection Manager > Resource pools**.

Step 2 Select **VC ID** from the **Pool Type** in the upper left of the Resource Pools window.

Step 3 Click the **Create** button.

The Create VC ID Pool window appears, as shown in [Figure 3-91](#).

Figure 3-91 Create VC ID Pool Window

The Create VC ID Pool window contains the following fields:

- **VC Pool Start** (required) Range: 1 to 2147483646.
- **VC Pool Size** (required) Range: 1 to 2147483647.

Step 4 Enter the required information for the site of origin pool you are creating.

Step 5 Click **Save**.

The VC ID Pools window reappears with the new VC ID pool listed.

Creating a VLAN Pool

From the Create VLAN Pool window, you can create VLAN pools.

To create a VLAN pool, do the following:

Step 1 Navigate **Service Inventory > Inventory and Connection Manager > Resource pools**.

Step 2 Select **VLAN** from the **Pool Type** in the upper left of the Resource Pools window.

Step 3 Click the **Create** button.

The Create VLAN Pool window appears, as shown in [Figure 3-92](#).

Figure 3-92 Create VLAN Pool Window

Create VLAN Pool

VLAN Pool Start *	0	(1 - 4094)
VLAN Pool Size *	0	(1 - 4094)
Access Domain *	Select	

Save **Cancel**

Note: * - Required Field

95302

The Create VLAN Pool window contains the following fields:

- **VLAN Pool Start** (required) Range: 1 to 4094.
- **VLAN Pool Size** (required) Range: 1 to 4094.
- **Access Domain** (required)

Step 4 Enter the **VLAN Pool Start** and **Size** information for the VLAN pool you are creating.

Step 5 Click the **Select** button.

The Access Domain for new VLAN Pool window appears, as shown in [Figure 3-93](#).

Figure 3-93 Access Domain for new VLAN Pool Window

#	Select	Access Domain Name	Provider Name
1.	☐	Sonera_Access	Telia_Sonera

Step 6 Select one of the access domains listed and click **Select**.

Step 7 Click **Save**.

The VLAN Pools window reappears with the new VLAN pool listed.

Deleting Resource Pools

From the Resource Pool window, you can delete specific resource pools.

To delete resource pools, do the following:

Step 1 Navigate **Service Inventory > Inventory and Connection Manager > Resource pools**.

Step 2 Select a pool type from the **Pool Type** in the upper left of the Resource Pools window.

Step 3 Select one or more resource pools to delete by selecting the check box to the left of the resource pool(s).

Step 4 Click the **Delete** button.

The Confirm Delete window appears, as shown in [Figure 3-94](#).

Figure 3-94 Confirm Delete Window

#	IP Address Pool	Mask	Size	Type	Pool Name
1.	18.0.0.4	30	4194303	Region	ServiceProvider1:Region1

- Step 5** Click the **Delete** button to confirm that you want to delete the resource pool(s) listed. The Resource Pools window reappears with the specified pool(s) deleted.
-

CE Routing Communities

A VPN can be organized into subsets called *CE routing communities*, or CERCs. A CERC describes how the CEs in a VPN communicate with each other. Thus, CERCs describe the logical topology of the VPN. Cisco IP Solution Center can be employed to form a variety of VPN topologies between CEs by building hub and spoke or full mesh CE routing communities. CERCs are building blocks that allow you to form complex VPN topologies and CE connectivity.

The most common types of VPNs are *hub-and-spoke* and *full mesh*.

- A hub-and-spoke CERC is one in which one or a few CEs act as hubs, and all spoke CEs talk only to or through the hubs, never directly to each other.
- A full mesh CERC is one in which every CE connects to every other CE.

These two basic types of VPNs—full mesh and hub and spoke—can be represented with a single CERC. Whenever you create a VPN, the Cisco IP Solution Center software creates one default CERC for you. This means that until you need advanced customer layout methods, you will not need to define new CERCs. Up to that point, you can think of a CERC as standing for the VPN itself—they are one and the same. If, for any reason, you must override the software's choice of route target values, you can do so only at the time you create a CERC in the Cisco IP Solution Center software.

To build very complex topologies, it is necessary to break down the required connectivity between CEs into groups, where each group is either fully meshed, or has a hub and spoke pattern. (Note that a CE can be in more than one group at a time, if each group has one of the two basic patterns.) Each subgroup in the VPN wants its own CERC. Any CE that is only in one group just joins the corresponding CERC (as a spoke if necessary). If a CE is in more than one group, then you can use the Advanced Setup choice during provisioning to add the CE to all the relevant groups in one service request. Given this information, the provisioning software does the rest, assigning route target values and VRF tables to arrange exactly the connectivity the customer requires. You can use the Topology tool to double-check the CERC memberships and resultant VPN connectedness.

Cisco IP Solution Center supports multiple CEs per site and multiple sites connected to the same PE. Each CERC has unique route targets (RT), route distinguisher (RD), and VPN Routing and Forwarding instance (VRF) naming. After provisioning a CERC, it is a good idea to run the audit reports to verify the CERC deployment and view the topologies created by the service requests. The product supports linking two or more CE routing communities in the same VPN.

This section describes how you can create and manage CE routing communities. This section includes the following:

- [Accessing the CE Routing Communities Window, page 3-115](#)
- [Creating CE Routing Communities, page 3-115](#)
- [Deleting CE Routing Communities, page 3-117](#)

Accessing the CE Routing Communities Window

The CE Routing Communities feature is used to create and manage CERCs.

To access the CE Routing Communities window, do the following:

- Step 1** Navigate **Service Inventory > Inventory and Connection Manager > CE Routing Communities** to access the CE Routing Communities window shown in [Figure 3-95](#).

Figure 3-95 CE Routing Communities Window

The screenshot shows the 'CE Routing Communities' window. At the top, there is a search bar with the text 'Show CERCs with' followed by a dropdown menu set to 'Name', a text input field with an asterisk, and a 'Find' button. Below the search bar, it says 'Showing 1-3 of 3 records'. The main area contains a table with the following columns: '#', 'Name', 'HRT', 'SRT', 'Provider', and 'VPN'. There are three rows of data, each with a checkbox in the '#' column. Below the table, there is a 'Rows per page:' dropdown set to '10'. At the bottom right, there are three buttons: 'Create', 'Edit', and 'Delete'.

#	Name	HRT	SRT	Provider	VPN
1. ☐	CERC1	10:100	10:200	ServiceProvider1	VPN1
2. ☐	Default	100:5987	100:5988	Telia_Sonera	Telia-Sonera-VPN
3. ☐	Telia_Cerc	12121:23243	12311:34142	Telia_Sonera	

From the CE Routing Communities window, you can create, edit, or delete CE routing communities using the following buttons:

- **Create** Click to create new CE routing communities. Enabled only if no CE routing community is selected.
- **Edit** Click to edit selected CE routing communities (select by clicking the corresponding box). Enabled only if one CE routing community is selected.
- **Delete** Click to delete selected CE routing communities (select by clicking the corresponding box(es)). Enabled only if one or more CE routing communities are selected.

Creating CE Routing Communities

When you create a VPN, the Cisco IP Solution Center software creates one default CE routing community (CERC) for you. But if your network topology and configuration require customized CERC definitions, you can define CERCs customized for your network.



Tip

Customized CERCs should be defined only in consultation with the VPN network administrator. To build complex topologies, it is necessary to break down the required connectivity between CEs into groups, where each group is either fully meshed or has a hub-and-spoke pattern. A CE can be in more than one group at a time, as long as each group has one of the two basic configuration patterns.

Each subgroup in the VPN wants its own CERC. Any CE that is only in one group just joins the corresponding CERC (as a spoke if necessary). If a CE is in more than one group, then you can use the Advanced Setup choice during provisioning to add the CE to all the relevant groups in one service request. Given this information, Cisco IP Solution Center does the rest, assigning route target values and VRF tables to arrange the precise connectivity the customer requires.

To create a CE routing community, do the following:

- Step 1** Navigate **Service Inventory > Inventory and Connection Manager > CE Routing Communities**.
- Step 2** Click **Create**.

The Create CE Routing Community window appears, as shown in [Figure 3-96](#).

Figure 3-96 Create CE Routing Community Window

- Step 3** Complete the CERC fields as required for the CE Routing Community:
- Provider** (required) To specify the service provider associated with this CERC, click **Select**.
The Select Provider dialog box is displayed.
 - Choose the name of the service provider, then click **Select**.
 - Name** (required) Enter the name of the CERC.
 - CERC Type** Specify the CERC type: Hub and Spoke or Fully Meshed.
 - Auto-Pick Route Target Values** Choose to either let Cisco IP Solution Center automatically set the route target (RT) values or set the RT values manually.
By default, the **Auto-pick route target values** check box is selected. If you deselect the check box, you can enter the Route Target values manually.



Caution

If you choose to bypass the **Auto-pick route target values** option and set the route target (RT) values manually, note that the RT values cannot be edited after they have been defined in the ISC software.

- Step 4** When you have finished entering the information in the Create CE Routing Community dialog box, click **Save**.

After creating the CERC, you can add it to the VPN.

Deleting CE Routing Communities

From the CE Routing Community window, you can delete specific CERCs.

To delete CERC(s), do the following:

-
- Step 1** Navigate **Service Inventory > Inventory and Connection Manager > CE Routing Communities**

- Step 2** Select CERC(s) to delete by selecting the check box(es) to the left of the CERC name.

- Step 3** Click the **Delete** button.

The Confirm Delete window appears.

- Step 4** Click **OK** to confirm that you want to delete the CERC(s) listed.

The CE Routing Communities window reappears with the specified CERC(s) deleted.

VPNs

At its simplest, a virtual private network (VPN) is a collection of sites that share the same routing table. A VPN is also a framework that provides private IP networking over a public infrastructure such as the Internet. In Cisco IP Solution Center: MPLS VPN Management, a VPN is a set of customer sites that are configured to communicate through a VPN service. A VPN is defined by a set of administrative policies.

A VPN is a network in which two sites can communicate over the provider's network in a private manner; that is, no site outside the VPN can intercept their packets or inject new packets. The provider network is configured such that only one VPN's packets can be transmitted through that VPN—that is, no data can come in or out of the VPN unless it is specifically configured to allow it. There is a physical connection from the provider edge network to the customer edge network, so authentication in the conventional sense is not required.

This section describes how you can create and manage pools for various types of resources. This section includes the following:

- [Accessing the VPNs Window, page 3-118](#)
- [Creating a VPN, page 3-118](#)
- [Deleting VPNs, page 3-120](#)

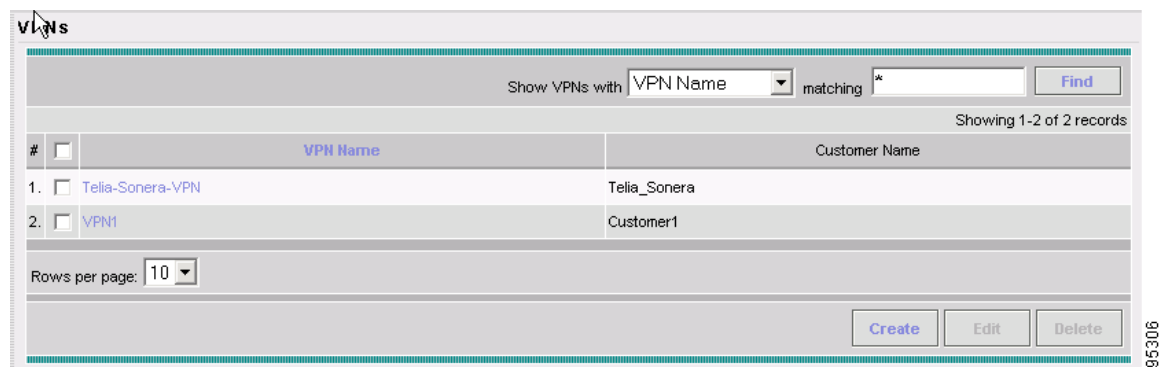
Accessing the VPNs Window

The VPN feature is used to create and manage various types of VPNs.

To access the VPN window, do the following:

- Step 1** Navigate **Service Inventory > Inventory and Connection Manager > VPN** to access the VPN window shown in [Figure 3-97](#).

Figure 3-97 VPNs Window



From the VPNs window, you can create, edit, or delete VPNs using the following buttons:

- **Create** Click to create new VPNs. Enabled only if no VPN is selected.
- **Edit** Click to edit selected VPNs (select the corresponding box). Enabled only if one VPN is selected.
- **Delete** Click to delete selected VPNs (select the corresponding box). Enabled only if one or more VPNs is selected.

Creating a VPN

To create a VPN, do the following:

- Step 1** Navigate **Service Inventory > Inventory and Connection Manager > VPN**.
- Step 2** Click **Create**.

The Create VPN window appears, as shown in [Figure 3-98](#).

Figure 3-98 Create VPN Window

Step 3 Complete the fields as required for the VPN:

- a. **Name** (required) Enter the name of the VPN.
- b. **Customer** (required) To select the customer associated with this VPN, choose **Select**.
- c. From the list of customers, select the appropriate customer, then click **Select**.
- d. If you want MPLS attributes, the optional fields for that are in e. to j.
- e. **Create Default CE Routing Community** (optional) To create a default CE routing community, select the **Create Default CE Routing Community** check box and select a provider.
- f. **Enable Multicast** To enable multicast VPN routing, select the **Enable Multicast** check box.

An IP address that starts with the binary prefix *1110* is identified as a *multicast group address*. There can be more than one sender and receiver at any time for a given multicast group address. The senders send their data by setting the group address as the destination IP address. It is the responsibility of the network to deliver this data to all the receivers in the network who are listening to that group address.



Note Before you can create a VPN with multicast enabled, you must define one or more multicast resource pools.

- g. **Data MDT Size** (optional) If **Enable Multicast** is set on, **Data MDT Size** is required. From the drop-down list, select the data MDT size.

MDT refers to a *multicast distribution tree* (MDT). The MDT defined here carries multicast traffic from customer sites associated with the multicast domain.

- h. **Data MDT Threshold** (optional) If **Enable Multicast** is set on, **Data MDT Threshold** is required. Enter the bandwidth threshold for the data multicast distribution tree.

The *data MDT* contains a range of multicast group addresses and a bandwidth threshold. Thus, whenever a CE behind a multicast-VRF exceeds that bandwidth threshold while sending multicast traffic, the PE sets up a new data MDT for the multicast traffic from that source. The PE informs the other PEs about this data MDT and, if they have receivers for the corresponding group, the other PEs join this data MDT.

- i. **CE Routing Communities** (optional) If **Enable Multicast** is set on, **CE Routing Communities** is required. If you do not choose to enable the default CERC, you can select a customized CERC that you have already created in ISC. From the CE Routing Communities pane, click **Select**.

The Select CE Routing Communities dialog box is displayed.

- j. Select the check box for the CERC you want used for this service policy, then click **Select**.

You return to the Create VPN dialog box, where the new CERC selection is displayed, along with its *hub route target (HRT)* and *spoke route target (SRT)* values.

- k. If you want VPLS attributes, the optional fields for that are in l. to m.

- l. **Enable VPLS** (optional) Select this check box to enable VPLS.

- m. **Service Type** (optional) Click the drop-down menu and choose from ERS (Ethernet Relay Service) or EWS (Ethernet Wire Service).

- n. **Topology** (optional) Select the VPLS topology from the drop-down menu: Full Mesh (each CE will have direct connections to every other CE) or Hub and Spoke (only the Hub CE has connection to each Spoke CE and the Spoke CEs do not have direct connection to each other).

Step 4 When satisfied with the settings for this VPN, click **Save**.

You have successfully created a VPN, as shown in the **Status** display in the lower left corner of the VPNs dialog box.

Deleting VPNs

From the VPNs window, you can delete specific VPNs.

To delete VPN(s), do the following:

Step 1 Navigate **Service Inventory > Inventory and Connection Manager > VPN**.

Step 2 Select VPN(s) to delete by selecting the check box to the left of the VPN name.

Step 3 Click the **Delete** button.

The Confirm Delete window appears.

Step 4 Click **OK** to confirm that you want to delete the VPN(s) listed.

The VPNs window reappears with the specified VPN(s) deleted.

AAA Servers

This section describes how you can create and manage AAA servers. An AAA server is only required when you want remote access VPN service and Easy VPN service and the user authentication or authorization is not done internally but by an external AAA server, such as RADIUS, TACACS+, NT Domain, or SDI. In this case, ISC sets up aspects of AAA on CPE devices for the remote access services, based on the external AAA server information in the repository. When the Service Request is scheduled to be deployed, the configlet of AAA is generated and downloaded to the CPE devices.

This section includes the following:

- [Accessing the AAA Servers Window, page 3-121](#)
- [Defining an AAA Server, page 3-121](#)
- [Deleting AAA Servers, page 3-123](#)

Accessing the AAA Servers Window

The AAA Servers feature is used to create or delete AAA servers that communicate with CPE devices and edit their parameters.

To access the AAA Servers window, do the following:

- Step 1** Navigate **Service Inventory > Inventory and Connection Manager > AAA Servers** to access the AAA Servers window shown in [Figure 3-99](#).

Figure 3-99 AAA Servers Window

The screenshot shows the 'AAA Servers' window. At the top, there is a search bar with the text 'Show AAA Servers with' followed by a dropdown menu set to 'AAA Server Name', a 'matching' label, an asterisk '*' in a text box, and a 'Find' button. Below the search bar, it says 'Showing 0 of 0 records'. There is a table with two columns: 'AAA Server Name' and 'Customer Name'. The table is currently empty. Below the table, there is a 'Rows per page:' dropdown set to '10'. At the bottom right, there are three buttons: 'Create', 'Edit', and 'Delete'.

From the AAA Servers window, you can create, edit, or delete AAA servers using the following buttons:

- **Create** Click to define new AAA servers. Enabled only if no AAA server is selected.
- **Edit** Click to edit selected AAA servers (select by clicking the corresponding box). Enabled only if one AAA server is selected.
- **Delete** Click to delete selected AAA servers (select by clicking the corresponding box). Enabled only if one or more AAA servers are selected.

Defining an AAA Server

From the Create AAA Server window, you can define AAA servers.

To define such a device, do the following:

Step 1 Navigate **Service Inventory > Inventory and Connection Manager > AAA Servers**.

Step 2 Click the **Create** button.

The Create AAA Servers window appears, as shown in [Figure 3-100](#).

Figure 3-100 Create AAA Servers Window

The Create AAA Servers window contains the following fields:

- **Name** (required) Name given to the AAA Server that this record represents.
- **Owner** (required) This record can belong to a customer or it can be global to the system.
- **IP Address** (required) IP address of the AAA Server.
- **Server Type** (required) Choices: **RADIUS**, **NT DOMAIN**, **SDI**, or **TACACS+**. Default: **RADIUS**.
- **Server Role** (required) Specifies the role of the server, that is what it does. Choices: **Authentication**, **Accounting**, or **Both**. Default: **Authentication**.
- **Port** (optional) The Authentication Server port.
- **Accounting Server Port** (optional) Enabled when **Accounting** or **Both** is selected for the Server Type.
- **Timeout** (required) The timeout in seconds. Range: 1 to 30. Default: 4.
- **Retries** (required) The number of retries. Range: 0 to 10. Default: 2.
- **Secret** (required) Only enabled when **Radius** or **TACACS+** is selected for Server Type.

- **Verify Secret** (required) A verification field so that you confirm what you typed into the Secret field. Only enabled when **Radius** or **TACACS+** is selected for Server Type.
- **NT Domain Controller Name** (required) Only enabled when NT Domain is selected as the Server Type.

Step 3 Enter the desired information for the AAA server you are defining.

Step 4 Click **Save**.

The AAA Servers window reappears with the new AAA server listed.

Deleting AAA Servers

From the AAA Servers window, you can delete specific AAA servers.

To delete a AAA server, do the following:

Step 1 Navigate **Service Inventory > Inventory and Connection Manager > AAA Servers**.

Step 2 Select one or more AAA servers to delete by selecting the check box to the left of the AAA server name.

Step 3 Click the **Delete** button.

The Delete AAA Server(s) window appears.

Step 4 Click the **Delete** button to confirm that you want to delete the AAA servers listed.

The AAA Servers window reappears with the specified AAA servers deleted.

Named Physical Circuits

Named physical circuits (NPCs) are named circuits that describe a physical connection between a CPE or PE-CLE and a PE-POP. The intermediate nodes of the NPCs can either be CPE or PE. They can be connected in a circular fashion forming a ring of devices, which is represented by an entity known as NPC Rings. NPC Rings represent the circular topology between devices (CPE or PE) to the Named Physical Circuits. To create an NPC, you must specify how the source CPE/PE-CLE and the destination PE-POP are connected and specify the intermediate nodes.

The connectivity of the NPCs is defined by specifying a set of devices serving as physical links; each device has two interfaces that are part of the NPC connections. The Incoming Interface defines the interface from the CE direction. The Outgoing Interface defines the interface toward the PE direction.

You can also add (meaning after the chosen device) or insert (meaning before the chosen device) an NPC Ring in the link.

Keep in mind the following when you are creating an NPC:

- In the ISC software, the device you select can be any node in the link. The ISC software only shows the appropriate devices. The first device *must* be a CPE or PE-CLE and the last device *must* be a PE-POP.
- NPCs should be created before the MPLS multi-device, VPLS, or L2VPN service request is created with cpe1 and pe1. So when you create the SR, you would select the policy, cpe1, pe1, and the NPC that defines the link between cpe1 and pe1.

This section describes how you can create and delete NPCs and create, edit, and delete NPC Rings. This section includes the following:

- [Accessing the Named Physical Circuits Window, page 3-124](#)
- [Creating a Named Physical Circuit, page 3-125](#)
- [Deleting Named Physical Circuits, page 3-128](#)
- [Creating NPC Rings, page 3-129](#)
- [Editing NPC Rings, page 3-133](#)
- [Deleting NPC Rings, page 3-133](#)

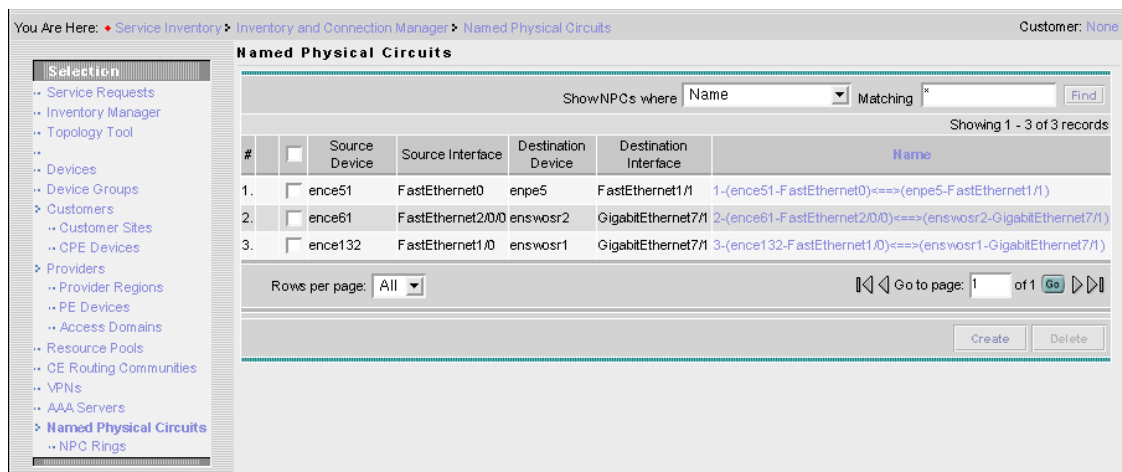
Accessing the Named Physical Circuits Window

The Named Physical Circuits feature is used to create and delete NPCs. You cannot edit or modify.

To access the Named Physical Circuits window, do the following:

- Step 1** Navigate **Service Inventory > Inventory and Connection Manager > Named Physical Circuits** to access the window shown in [Figure 3-101, “Named Physical Circuits Window.”](#)

Figure 3-101 Named Physical Circuits Window



From the Named Physical Circuits window, you can create or delete NPCs using the following buttons:

- **Create** Click to create new NPCs. Enabled only if no NPC is selected.
- **Delete** Click to delete selected NPCs (select by clicking the corresponding box(es)). Enabled only if one or more NPCs are selected.

Creating a Named Physical Circuit

To add an NPC physical link, do the following:

- Step 1** Navigate **Service Inventory > Inventory and Connection Manager > Named Physical Circuit**.
- Step 2** Click the **Create** button in [Figure 3-101](#), “**Named Physical Circuits Window**,” and a window, as shown in [Figure 3-102](#), “**Create a Named Physical Circuit**,” appears.

Figure 3-102 Create a Named Physical Circuit

Each line represents a physical link and each physical link contains the following attributes:

- **Device**
- **Incoming Interface**
- **Outgoing Interface**
- **Ring** (optional)



Note Before adding a ring in an NPC, create a ring and save it in the repository, as explained in the [“Creating NPC Rings”](#) section on page 3-129.



Note An NPC must have at least one link defined. The link must have two Devices, an Incoming Interface, and an Outgoing Interface.

- Step 3** Click **Add Device** or **Insert Device** and a window as shown in [Figure 3-103](#), “**Select Device**,” appears.

Figure 3-103 Select Device

Showing 1-9 of 9 records

#	Select	Device Name	Customer Name	Site Name	Management Type
1.	☐	barnes.cisco.com	Customer2	Boulder	UNMANAGED
2.	☐	carson.cisco.com	Customer2	SJ	UNMANAGED
3.	☐	ence11	Customer1	Site-ence11	MANAGED
4.	☐	ence132	Customer1	Site-ence132	MANAGED
5.	☐	ence21	Customer1	Site-ence21	MANAGED
6.	☐	ence51	Customer1	Site-ence51	MANAGED
7.	☐	ence61	Customer1	Site-ence61	MANAGED
8.	☐	ipsec-cpe-london	Customer1	Site-ipsec-cpe-london	MANAGED
9.	☐	ipsec-cpe-ny	Customer1	Site-ipsec-cpe-ny	MANAGED

Rows per page: 10 Go to page: 1 of 1

Select Cancel

- Step 4** Be sure that the drop-down in **Show** is **CPE** or **PE**. Click a radio button next to a device and then click **Select**.
- Step 5** Figure 3-102, “Create a Named Physical Circuit,” reappears with the chosen **Device**.

Figure 3-104 Select Device

Create a Named Physical Circuit

#	Device	Incoming Interface	Outgoing Interface	Ring
1.	☐ ence21		Select outgoing interface	
2.	☐ mlce203	Select incoming interface		

Insert Device Insert Ring Add Device Add Ring Delete Save Cancel

- Step 6** If you want to add a device to your NPC as the last item or after the item selected in the check box, click the **Add Device** button in Figure 3-102 on page 3-125 and then add device and interface information as explained in the previous steps. If you want to insert a device to your NPC as the first item or before the item selected in the check box, click the **Insert Device** button in Figure 3-102 on page 3-125 and then add device and interface information as explained in the previous steps.
- Step 7** In the **Outgoing Interface** column in this new version of Figure 3-102, “Create a Named Physical Circuit,” click **Select outgoing interface** and a window as shown in Figure 3-105, “Select Outgoing Interface,” appears with a list of interfaces.

Figure 3-105 Select Outgoing Interface

Interfaced for device **encl1**

ShowDevice Interfaces with matching

Showing 1-6 of 6 records

#	Select	Name	IP Address	Interface Logical Name
1.	☐	Ethernet0	192.168.129.189/30	
2.	☐	Ethernet1	192.168.132.9/29	
3.	☐	Loopback0	192.168.115.70/32	
4.	☐	Loopback1	14.1.1.1/32	
5.	☐	Serial0		
6.	☐	Serial1		

Rows per page: Go to page: of 1

- Step 8** Click a radio button next to the interface to be the source interface for this NPC and then click **Select**.
- Step 9** [Figure 3-102, “Create a Named Physical Circuit,”](#) reappears with the chosen **Interface**.
- Step 10** In the **Incoming Interface** column in this new version of [Figure 3-102, “Create a Named Physical Circuit,”](#) click **Select incoming interface** and a window as shown in [Figure 3-106, “Select Incoming Interface,”](#) appears with a list of interfaces.

Figure 3-106 Select Incoming Interface

Interfaced for device **encl1**

ShowDevice Interfaces with matching

Showing 1-10 of 18 records

#	Select	Name	IP Address	Interface Logical Name
1.	☐	ATM5/0		
2.	☐	Ethernet2/0		
3.	☐	Ethernet2/1		
4.	☐	Ethernet2/2		
5.	☐	Ethernet2/3		
6.	☐	FastEthernet0/0		
7.	☐	FastEthernet4/0		
8.	☐	Hssi1/0		
9.	☐	Hssi1/1		
10.	☐	Loopback0	192.168.115.64/32	

Rows per page: Go to page: of 2

- Step 11** Click a radio button next to the interface to be the incoming interface for this NPC and then click **Select**.
- Step 12** [Figure 3-102, “Create a Named Physical Circuit,”](#) reappears with the chosen **Incoming Interface**.

- Step 13** If you created an NPC ring that you want to insert or add into this NPC, as explained in the [“Creating NPC Rings”](#) section on page 3-129, you can click **Insert Ring** or **Add Ring** and the ring appears at the beginning or before the item selected in the check box for **Insert Ring** or the ring appears at then end or after the item selected in the check box for **Add Ring**, as shown in [Figure 3-107](#), “Select NPC Ring.”

**Note**

When inserting a ring, select the source device of the ring that connects to a source device or an NPC and the destination device of the ring that connects to the destination device of the NPC.

If you have not created an NPC ring that you want to insert into this NPC, proceed to [Step 17](#).

Figure 3-107 Select NPC Ring

Showing 1-1 of 1 records

#	Select	Ring Name
1.	☐	1-enpe1-Ethernet2/0

Rows per page: 10 Go to page: 1 of 1 Go

Select Cancel

- Step 14** Click a radio button next to the ring you choose and then click **Select**.
- Step 15** [Figure 3-102](#), “Create a Named Physical Circuit,” reappears with the chosen **Ring**.
- Step 16** Select the missing devices and interfaces as explained in the [“Creating NPC Rings”](#) section on page 3-129.
- Step 17** Click **Save**.
- Step 18** [Figure 3-102](#), “Create a Named Physical Circuit,” reappears with the new NPC listed.

Deleting Named Physical Circuits

To delete NPC(s), do the following:

- Step 1** Navigate **Service Inventory > Inventory and Connection Manager > Named Physical Circuits** to access the window shown in [Figure 3-101](#), “Named Physical Circuits Window.”
- Step 2** Select one or more NPCs to delete by selecting the check box(es) on the left.
- Step 3** Click the **Delete** button.
- The Delete NPC window appears.

**Note**

If the specified NPC is being used by any of the Service Requests, you will not be allowed to delete it. An error message appears explaining this.

- Step 4** Click the **Delete** button to confirm that you want to delete the NPCs listed.
- Figure 3-101, “Named Physical Circuits Window,” reappears with the specified NPCs deleted.

Creating NPC Rings

Create NPC rings as follows:

- Step 1** Navigate **Service Inventory > Inventory and Connection Manager > NPC Rings** and a window as shown in Figure 3-108, “NPC Rings,” appears.

Figure 3-108 NPC Rings

- Step 2** Click the **Create** button and a window as shown in Figure 3-109, “Create Ring,” appears. A ring has a minimum of three physical links that form of a ring.

Figure 3-109 Create Ring



Note

At any time, if you click **Cancel**, everything you have chosen disappears.

- Step 3** Start with the first line, which represents the first physical link.
- Step 4** In the **Source Device** column, click **Select source device** and a window as shown in Figure 3-110, “Select Source Device —CPE/PE,” appears.



Note

The CPE you choose *must* be a Multi-VRF CE.

Figure 3-110 Select Source Device —CPE/PE

Showing 1-9 of 9 records

#	Select	Device Name	Customer Name	Site Name	Management Type
1.	☐	barnes.cisco.com	Customer2	Boulder	UNMANAGED
2.	☐	carson.cisco.com	Customer2	SJ	UNMANAGED
3.	☐	ence11	Customer1	Site-ence11	MANAGED
4.	☐	ence132	Customer1	Site-ence132	MANAGED
5.	☐	ence21	Customer1	Site-ence21	MANAGED
6.	☐	ence51	Customer1	Site-ence51	MANAGED
7.	☐	ence61	Customer1	Site-ence61	MANAGED
8.	☐	ipsec-cpe-london	Customer1	Site-ipsec-cpe-london	MANAGED
9.	☐	ipsec-cpe-ny	Customer1	Site-ipsec-cpe-ny	MANAGED

Rows per page: 10 Go to page: 1 of 1

Select Cancel

Step 5 Click a radio button next to the device to be the source device for this physical link and then click **Select**.

Step 6 Figure 3-109, “Create Ring,” reappears with the chosen **Source Device**.

**Note**

When choosing the **Source Device** for a physical link, this same choice is made for the **Destination Device** for the previous physical link (or the last physical link if you are choosing for the first physical link). For a selected device, do not select the same interface for the source and destination interface.

Step 7 In the **Source Interface** column in this new version of Figure 3-109, “Create Ring,” click **Select source interface** and a window as shown in Figure 3-111, “Select Source Interface,” appears with a list of interfaces.

Figure 3-111 Select Source Interface

Interfaces for device **ence11**

Showing 1-6 of 6 records

#	Select	Name	IP Address	Interface Logical Name
1.	☐	Ethernet0	192.168.129.189/30	
2.	☐	Ethernet1	192.168.132.9/29	
3.	☐	Loopback0	192.168.115.70/32	
4.	☐	Loopback1	14.1.1.1/32	
5.	☐	Serial0		
6.	☐	Serial1		

Rows per page: 10 Go to page: 1 of 1

Select Cancel

Step 8 Click a radio button next to the interface to be the source interface for this physical link and then click **Select**.

Step 9 Figure 3-109, “Create Ring,” reappears with the chosen **Source Interface**.

- Step 10** In the **Destination Device** column in this new version of Figure 3-109, “Create Ring,” click **Select destination device** and a window as shown in Figure 3-112, “Select Destination Device —CPE/PE,” appears.

Figure 3-112 Select Destination Device —CPE/PE

PE for NPC

Show PEs with matching

Showing 1-10 of 14 records

#	Select	Device Name	Provider Name	Region Name	Role Type
1.	☐	enpe1	Provider1	US	PE_POP
2.	☐	enpe12	Provider1	US	PE_POP
3.	☐	enpe2	Provider1	US	PE_POP
4.	☐	enpe4	Provider1	US	PE_POP
5.	☐	enpe5	Provider1	US	PE_POP
6.	☐	enpe6	Provider1	US	PE_POP
7.	☐	enswostr1	Provider1	US	PE_POP
8.	☐	enswostr2	Provider1	US	PE_POP
9.	☐	ipsec-cpe-paris	Provider1	US	PE_POP
10.	☐	vmd-2950a	Provider1	US	PE_CLE

Rows per page: Go to page: of 2

- Step 11** Click a radio button next to the device to be the destination device for this physical link and then click **Select**.
- Step 12** Figure 3-109, “Create Ring,” reappears with the chosen **Destination Device**.



Note

When choosing the **Destination Device** for the a physical link, this same choice is made for the next **Source Device**. Do not choose the same Interface for these devices.

- Step 13** In the **Destination Interface** column in this new version of Figure 3-109, “Create Ring,” click **Select destination interface** and a window as shown in Figure 3-113, “Select Destination Interface,” appears with a list of interfaces.

Figure 3-113 Select Destination Interface

Interfaces for device **enpe1**

ShowDevice Interfaces with matching

Showing 1-10 of 18 records

#	Select	Name	IP Address	Interface Logical Name
1.	☐	ATM5/0		
2.	☐	Ethernet2/0		
3.	☐	Ethernet2/1		
4.	☐	Ethernet2/2		
5.	☐	Ethernet2/3		
6.	☐	FastEthernet0/0		
7.	☐	FastEthernet4/0		
8.	☐	Hssi1/0		
9.	☐	Hssi1/1		
10.	☒	Loopback0	192.168.115.64/32	

Rows per page:

- Step 14** Click a radio button next to the interface to be the destination interface for this NPC and then click **Select**.
- Step 15** [Figure 3-109](#), “**Create Ring**,” reappears with the chosen **Destination Interface**.
- Step 16** Repeat [Step 4](#) to [Step 15](#) for the middle physical links and [Step 4](#) to [Step 9](#) for the last physical link.
- Step 17** If you want to insert an extra physical link in the ring, select the check box for the line that represents the physical link you want the new physical link to follow and click **Insert**. Implement [Step 4](#) to [Step 15](#) to fill in the remaining entries in this new physical link.
- Step 18** If you want to delete a physical link in the ring but a minimum of three physical links will remain, select the check box for the line that represents the physical link you want to delete and click **Delete**.
- Step 19** If you want to establish additional cross links between non-adjacent devices in this ring, you can click **Edit Cross Links** in [Figure 3-109](#), “**Create Ring**,” and you then view a new window like [Figure 3-109](#) with no entry. Click the **Add** button and you can choose from the devices already in your ring. The result is a new entry in [Figure 3-109](#) with this device as the **Source Device**. Establish the Destination Device and Source and Destination Interfaces as you did when creating the ring. The choices of devices and interfaces is limited to those already established in your ring.
- Step 20** When you are completed setting up your ring, click **Save**.
- Step 21** The new ring is added in [Figure 3-108](#), “**NPC Rings**,” and a green check for Succeeded appears. The new ring is identified by the source device-source interface.
- Step 22** To create a ring with more than three physical links, select the check box for the link in [Figure 3-109 on page 3-129](#) to which you want to insert and the **Insert** button is then enabled. Proceed in adding links as explained in this section.

Editing NPC Rings

To edit NPC rings, do the following:



Note

If the specified NPC Ring is participating in any of the Named Physical Circuits, then you can not edit the ring. An error message appears containing IDs of the NPCs that contain the NPC Ring.

- Step 1** Navigate **Service Inventory > Inventory and Connection Manager > NPC Rings** and a window as shown in [Figure 3-114](#), “NPC Rings,” appears.

Figure 3-114 NPC Rings

- Step 2** Select the check box next to the line that represents an NPC ring and then click **Edit**. A window as shown in [Figure 3-109](#), “Create Ring,” appears with all the data for this ring. Proceed as in the “[Creating NPC Rings](#)” section on page 3-129 to make any changes you want.
- Step 3** When you have the ring as you want it, click **Save**.
- Step 4** [Figure 3-108](#), “NPC Rings,” appears with the appropriate name (source device-source interface) and a green check for Succeeded appears.

Deleting NPC Rings

To delete NPC rings, do the following.



Note

If the specified NPC Ring is participating in any of the Named Physical Circuits, then you can not delete the ring. An error message appears containing IDs of the NPCs that contain the NPC Ring.

- Step 1** Navigate **Service Inventory > Inventory and Connection Manager > NPC Rings** and a window as shown in [Figure 3-115](#), “NPC Rings,” appears.

Figure 3-115 NPC Rings

NPC Rings

Show NPC rings with name matching

Showing 1-1 of 1 records

#	Name
1. ☐	1-enpe1-Ethernet2/0

Rows per page: 10

- Step 2** Select the check box(es) next to the line(s) that represent(s) NPC ring(s) that you want to delete and then click **Delete**. A window as shown in [Figure 3-116](#), “Delete Rings,” appears with the chosen ring(s) for deletion.

Figure 3-116 Delete Rings

Delete Ring(s)

Confirm Delete

Showing 1-1 of 1 records

#	Name
1. ☐	2-ence11-Ethernet0

Rows per page: 10

- Step 3** Click **Cancel** if you change your mind about deleting the chosen ring(s) or click **Delete** to actually delete the ring.
- Step 4** [Figure 3-115](#), “NPC Rings,” appears with the remaining ring names and a green check for Succeeded appears.



Service Inventory > Inventory and Connection Manager > Inventory Manager

This chapter describes how to use Inventory Manager to prepare service inventory for the IP Solution Center (ISC) provisioning process. It contains the following subsections:

- [Overview of Inventory Manager, page 4-1](#)
- [Prerequisites and Limitations, page 4-2](#)
- [Inventory Manager from End to End, page 4-2](#)
- [Introducing the Inventory Manager GUI, page 4-12](#)
- [Inventory Manager GUI Reference, page 4-34](#)
- [Auto Discovery, page 4-105](#)
- [Service Discovery, page 4-108](#)
- [Ring Topology Discovery \(Connection Discovery\), page 4-113](#)

Overview of Inventory Manager

Inventory Manager provides a method of managing mass changes to inventory and service model data in the ISC provisioning process. In this process, Inventory Manager enables an operator to import network specific data into the ISC Repository (Repository) in bulk mode.

Inventory Manager performs three primary functions:

- Imports devices and configures CPE and PE by associating devices with a Customer or Provider.
- Collects live configuration files from a variety of devices (for example, routers, firewalls, and switches) in a network.



Note IPsec, firewall, NAT: **These features are not supported in this release.**

- Discovers logical, physical, and service level connectivity in a network.

Auto Discovery is an important tool in this process and is invoked from Inventory Manager. It can also be invoked from a Unix command line interface although this method is not recommended (see [UNIX Command Line Interface \(UNIX CLI\), page 4-107](#)). For a detailed description of Auto Discovery, see [Auto Discovery, page 4-105](#).

Prerequisites and Limitations

This document is intended for network engineers who have sufficient experience with MPLS VPN, L2VPN, and IPsec to provision these technologies using ISC.



Note IPsec: **This feature is not supported in this release.**

All of the network elements that you plan to provision should support the required hardware features and Cisco IOS versions.

Client Requirements

Java Runtime Environment (JRE) and Java Web Start must be installed to run Inventory Manager. If you are having trouble getting them to function properly, or need to update your local JRE, you can download and install the version appropriate for your operating system:

- Windows (all languages, including English): 1.4.2_04
- Solaris SPARC 32-bit self-extracting file: 1.4.2_04
- Linux self-extracting file: 1.4.2_04 (Not Supported)

Name Resolution

Inventory Manager requires name resolution. The ISC HTTP server host must be in the Domain Name System (DNS) that the web client is using or the name and address of the ISC server must be in the client host file.

SNMP

Prior to device discovery, SNMP must be enabled. All devices in the ISC provisioning environment must support SNMP. ISC supports SNMP versions 1, 2c, and 3.

CDP

CDP must be enabled to discover devices. Inventory Manager uses CDP to perform the service discovery task. CDP should be enabled globally and at the interface level for each device in the ISC provisioning environment.

NAT

This feature is not supported in this release.

Prior to device discovery, no Network Address Translation (NAT) mapping for router IP addresses is allowed.

Role Requirements

To run the Inventory Manager you need to use the predefined roles, CollectionRole and DeviceImportRole. This is the minimum requirement to successfully create physical or logical devices and to upload configuration files from the client to the ISC server.

Inventory Manager from End to End

This section describes how you use Inventory Manager to import and configure devices, collect configuration files, and perform service discovery.

These tasks should be carried out in the following order:

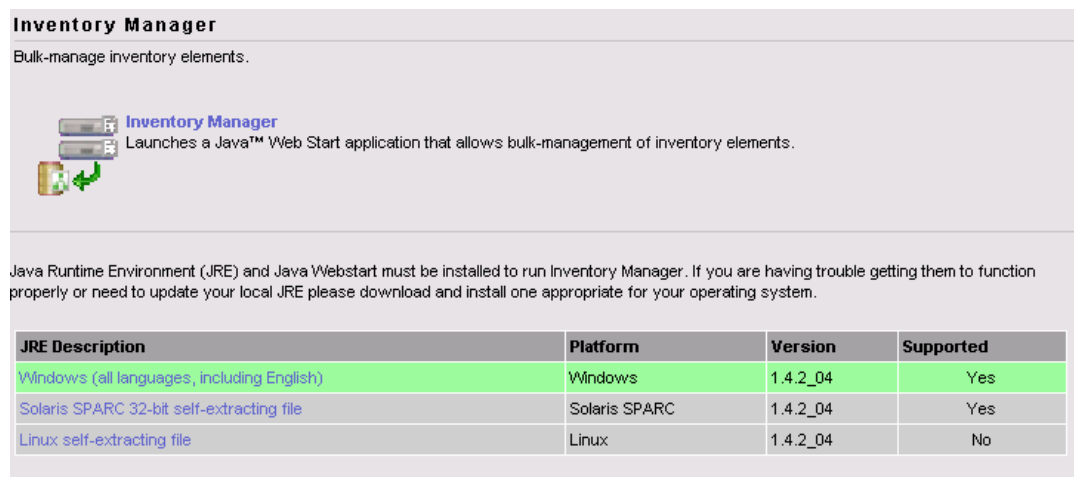
1. [Launching Inventory Manager, page 4-3](#)
2. [Importing Devices, page 4-5](#)
 - [Importing Devices from Configuration Files, page 4-5](#)
 - [Importing Devices with Auto Discovery, page 4-6](#)
3. [Configuring Device Credentials and SNMP Parameters, page 4-7](#)
4. [Collecting Configuration Files, page 4-9](#)
5. [Marking Interfaces for IPsec, Firewall, NAT, or QoS, page 4-9](#)
6. [Creating a New Customer with Devices, page 4-10](#)
7. [Creating a New Provider with Devices, page 4-10](#)
8. [Importing Connections with NPC Auto Discovery, page 4-11](#)
9. [Importing Services with Service Discovery, page 4-11](#)

Launching Inventory Manager

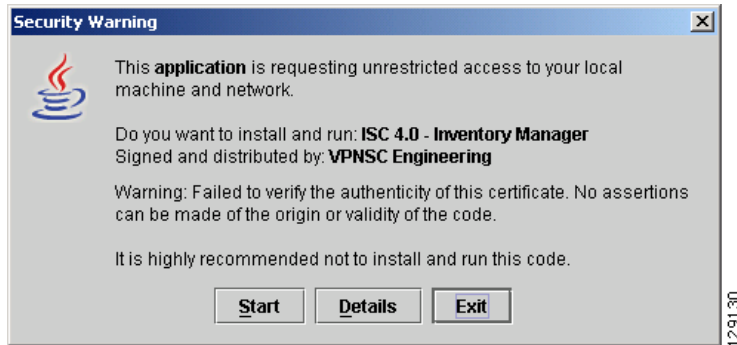
To launch Inventory Manager, follow these steps:

- Step 1** Log in to ISC.
- Step 2** Navigate **Service Inventory > Inventory and Connection Manager > Inventory Manager** and you receive a window, as shown in [Figure 4-1, “Inventory Manager.”](#) If you choose or need to click on an installation of Java Runtime Environment (JRE) for an operating system, follow that path, then quit the browser, log in again, and navigate the path in this step again.

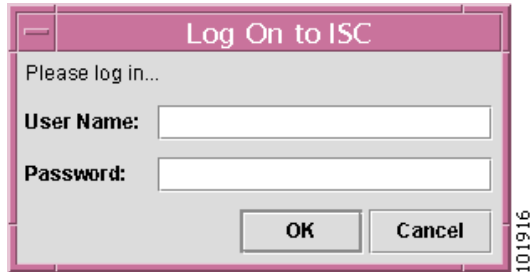
Figure 4-1 *Inventory Manager*



- Step 3** Click **Inventory Manager** in [Figure 4-1, “Inventory Manager.”](#) to launch Inventory Manager on the web client. The Java Web Start window appears.
- Step 4** From the Security Warning window, click **Start** to automatically complete the configuration, as shown in [Figure 4-2.](#)

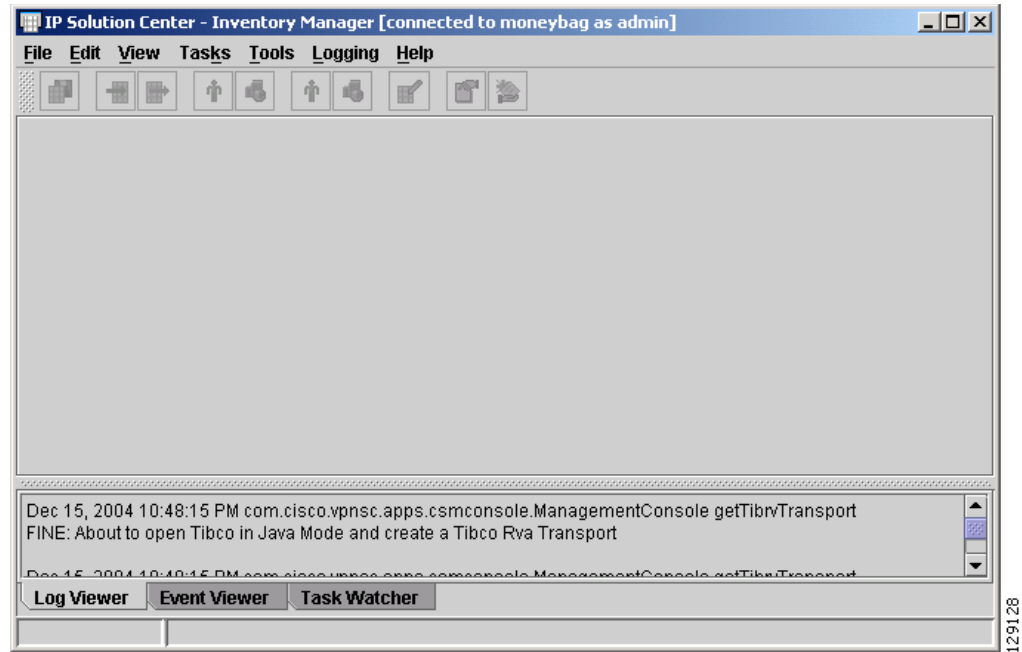
Figure 4-2 Start Java Web Start

Step 5 You receive a login window, as shown in [Figure 4-3](#), “Log On to ISC.”

Figure 4-3 Log On to ISC

Step 6 Enter your **User Name** and **Password** and click **OK**. Inventory Manager launches and connects to the Master ISC server.

The Inventory Manager Opening Screen in [Figure 4-4](#) appears.

Figure 4-4 Inventory Manager Opening Screen

Importing Devices

As described in the introduction to this chapter, devices can either be imported or created. The fastest way to bring device information into the Repository is to import devices using Inventory Manager.

Importing Devices from Configuration Files

If the configuration files are for a particular customer or provider, you can create a new customer or provider and associate the configuration files with CPEs or PEs. If the customer or provider currently exists in the Repository, you can open them and insert more CPEs or PEs to be associated with new or existing sites or regions.

To import devices with configuration files, follow these steps:

- Step 1** From Inventory Manager, choose **File > New > New Device Group**.
This step creates a container for target devices that can be moved to a provider or customer during the initialization process.
- Step 2** Enter a device group name and click **OK**.
You receive a prompt to import configuration files. You probably have a repository of configuration files on an existing network management device or TFTP server. Copy these files to the web client machine for import or make them available with a shared directory.
- Step 3** At the **No Config Files Specified for Import** prompt, click **Yes**.

The configuration files on the web client can be located by normal file browsing with both Shift and Ctrl+Click selected for multiple selections. When creating a new device group, only one filtering option is available: All Files.

**Note**

When creating new Providers, there are filters for files containing a specific BGP autonomous system number, or files that do not contain BGP configuration. The BGP filters can also be used to select PE devices that must have BGP configured or CE devices that do not require BGP.

Step 4 At the Open dialog box, browse to the location of the configuration files you want to import.

You may select multiple configuration files to import using SHIFT or CTRL + click. Please make sure that no more than X (250 or a number to be determined) configuration files are selected for import. There may be performance issues with Inventory Manager if more than X config files are selected for import at once.

Inventory Manager now imports a row in a spreadsheet workbook for each selected configuration file. By default, Inventory Manager inspects the configuration files and determines the device type, which includes Cisco IOS, CatOS, PIX, and VPN 3000 (IPsec, firewall, NAT, VPN 3000: **These features are not supported in this release**). It also parses passwords, SNMP information, interfaces, and virtual circuits.

If cells in the resulting spreadsheet are empty, Inventory Manager was not able to determine the value and, if it is required, the operator must provide the data or choose the information from a defined set of choices before saving.

These operations are described in more detail in the following sections as they are common to all methods of importing device information and administration.

Step 5 Once the appropriate files are selected, click **Open**, then click **OK**.

Importing Devices with Auto Discovery

**Note**

The Auto Discovery process can either be activated from Inventory Manager or from the command line on the ISC server using the Cisco Cornerstone Bridge Auto Discovery scripts.

To import devices with Auto Discovery, follow these steps:

Step 1 From Inventory Manager, select **File > New > New Dynamic Device List**.

This creates a spreadsheet where each row represents a potential seed device for discovery. For each seed device, the management interface must be provided. The management interface is the address on the device that the ISC host uses to reach the device.

After creating a new device list, a discovery starting point needs to be configured. This starting point is a device that can be reached from the ISC host. For each seed device, an accessible interface on the starting point is configured, because the management interface must be provided. The management interface is the address on the device that the ISC host uses to reach the device.

New dynamic device discovery requires the following manual tasks:

- Entering a seed IP address
- Entering a maximum hop count on the initialization of the task

A **policy.xml** file is created and a hop count is set automatically.

To choose the seed devices and hub, pick a seed device that can reach a large section of the network. Pick one or more of them until you think these devices will enable you to reach your entire managed network.

Point-of-presence (POP) routers are usually good choices. If you choose all the POPs in your network as the collection of seed devices and put in the appropriate number of hubs, you discover the entire managed network.

To pick the hub number, go to the CE that is the furthest from its associated POP, and count the number of devices between them. If this number is N, the hub number is N+1, assuming you are picking the POP as the seed.

Step 2 Click on the **Management Address** cell and enter the seed IP address for the new dynamic device list

Step 3 Choose **Tasks > Start Auto Discovery**.

A maximum hop count is specified for the Auto Discovery process. The Auto Discovery process queries the starting point device for its CDP table. From this table, all of those devices are queried for their CDP information. This CDP query process continues until the maximum hop count from the starting point is reached. Please note that only devices running the CDP process are discovered.

Step 4 Specify the maximum hop count when you receive the prompt.



Note

Only devices running the CDP process are discovered.

You are prompted to save two files. One file contains the list of the discovered devices and the other contains information related to connectivity between the devices. The discovered device information can be saved in XML to use as a starting point for future discovery efforts.

Step 5 Save the devices discovery.

Step 6 To view the Auto Discovery logs, go to **Administration > Control Center > Hosts > machine-name > cornerstone bridge**.

Configuring Device Credentials and SNMP Parameters

After the discovered devices are rendered in the spreadsheet, they must have several parameters set before the devices can be saved to the Repository and perform a successful live configuration collection. These parameters include:

- SNMP read and write community strings
- Telnet login password
- Device enable password



Note

The reachable management address is usually Loopback 0.

First remove any devices that are not required in the provisioning process. These items include core network devices or non-PE, CPE, and CLE devices that are used within the operator's network.

To remove unwanted devices, follow these steps:

-
- Step 1** Select the rows for the devices to be deleted.
Shift-select and Control-select are useful for multiple devices.
- Step 2** Choose **Edit > Remove Selected Devices**.
-

It is common in networks for devices to share many parameters. The Defaults option allows these common parameters to be entered for many devices at the same time; for example, login password, enable password, and SNMP strings.

To edit multiple devices, follow these steps:

-
- Step 1** Choose **Edit > Edit Default Attributes**.
A row for default values can be edited for each tab of the device list. The next step of the configuration process collects live configurations that require login and enable passwords.
- Step 2** Enter login and enable passwords into the defaults row.
After entering the default values, select all of the devices that share those common parameters. For devices that have values other than the default values, you can perform multiple editing techniques.
- Step 3** Select multiple rows or columns using standard selection techniques and choose **Edit > Edit Selected Devices**.
A dialog box, similar to the defaults window appears, allowing you to enter values to be applied to the selection.



-
- Note** You can right click on the column name and a menu appears showing you choices for sorting and selecting or de-selecting of columns.
-

- Step 4** To configure these devices, choose **Load Default Attributes to Selected Cells**.
The management IP address is the address that ISC uses to communicate with the element. This address must be reachable from the ISC host. When the devices were imported or discovered, ISC attempts to select the proper address as a management address starting with a loopback address. Verify the selected address for accessibility from the ISC host. ISC *must* be able to reach the network element for the configuration process to progress.
- Step 5** Click on the Management Address cell and enter the IP address in the dialog box.
-

Collecting Configuration Files

Collecting configuration files serves two purposes. It loads the current configuration information for the device, which populates many of the cells. It also verifies reachability and passwords for the reachable devices.

This task is created in the Repository and starts immediately. Logs can be viewed as normal for a collection spawned using only the Web GUI.

The task name is `Inventory_Manager_Collection_XXXXXX_username`, where `XXXXXX` is a unique number and the `username` is `admin`, or whatever the logged in username is in ISC.

To collect configurations, follow these steps:

-
Step 1	Select all the devices that have valid passwords and could be reached.
Step 2	Choose Tasks > Collect Latest Configuration Files .
-

Marking Interfaces for IPsec, Firewall, NAT, or QoS

IPsec, firewall, NAT: **These features are not supported in this release**

The interface marking process is only required for provisioning IPsec, Firewall, NAT, or QoS services. Marking interfaces on a one-by-one basis can be a very time consuming and tedious task. Inventory Manager provides a helpful tool to create rules for marking interfaces based on predefined criteria. You can apply one or more rules to selected devices to mark the interfaces in a bulk fashion.

For IPsec, the public interfaces are the interfaces where the IPsec or GRE tunnels terminate and the private interfaces are the interfaces behind which the subnets to be protected reside.

For firewalls, the outside interfaces connect to the outside, typically unsecured, networks and the inside interfaces are for the subnets residing behind the firewall.

To mark interfaces with Inventory Manager, follow these steps:

-
Step 1	Choose Tools > Interface Rule Marking Editor . A window appears allowing you to create, modify, or delete existing rules or folders. One simple rule can mark all Loopback0 interfaces as public for IPsec.
Step 2	To apply a rule to one or more devices, select the device(s) in the spreadsheet.
Step 3	Choose Edit > Apply Interface Marking Rule(s) to the selection. A rule chooser appears allowing you to select one or more rules to be applied.
-

**Note**

After completing the device configuration process, all the red X marks on the Device List tabs should be converted to either yellow or green Check Marks. These marks indicate that you have completed the required configuration and can save the device list, provider, and/or customer. Save all the completed lists by selecting **Save** under the file menu. Now all the device preparation should be complete and provisioning setup can begin.

Creating a New Customer with Devices

The devices should now be assigned roles, either PE or CE. For customers, you can assign roles by highlighting each device group and adding it to a new or existing Customer. Routers can be moved in bulk to customers with Inventory Manager.

To move CE routers to a new customer, follow these steps:

-
- Step 1** Select the desired routers and choose **Edit > Move to New Customer**.
 - Step 2** You are prompted to enter a customer name.
 - Step 3** Enter a customer name and click **OK**.
A new tab is created at the bottom of the device list and the routers are associated with the customer.
Each customer router must be put into a site. A site can have more than one router in it. All routers in a site should share routing information with the external provider network.
 - Step 4** Shift-select the **Site Name** cells for each customer router in the **CPE Attributes** tab.
 - Step 5** Choose **Edit Selected Devices**.
 - Step 6** Choose **CUSTOMER_ID+”SITE”+HOST_NAME**.
Repeat this process for all the CPEs.
All customer routers must have a **Management Type** selected. As with customer site, a range of router Management Type cells can be selected for bulk editing.
 - Step 7** Click the **Management Type** cell for all CEs.
 - Step 8** Choose **Edit Selected Devices**.
 - Step 9** Select the **Management Type**.
-

Creating a New Provider with Devices

A provider or provider administrative domain (PAD) is a group of Provider Edge (PE) devices that share a common BGP AS.

To move PE routers to a new provider and create a region, follow these steps:

-
- Step 1** Highlight the devices with a common BGP AS to be added to a new provider.
 - Step 2** Choose **Edit > Move to New Provider**.
When the devices are assigned a PAD, they become Provider Edge (PE) routers. PEs must be placed into regions. Each PAD must have one or more regions. A region is a collection of PEs that may share an address pool.
 - Step 3** To place a PE into a region, click on the **Region** cell for the PE.
If the desired region has already been created, it can be selected.
 - Step 4** Choose **Create Region** to add a region.
You can also add multiple PEs to a single region in one step using standard multiple selection techniques and choosing the **Edit > Edit Selected Devices** menu. As with single PE editing, you are prompted to choose an existing region or create a new region.

This completes the assignment of roles to devices.

**Note**

The tabs at the top of the device list pane of the Inventory Manager window corresponds to a grouping of information about the devices. The symbol to the left of the tab name indicates whether all the information required on that tab has been configured. A red X means that additional information is required. A yellow check mark indicates that all required information has been entered but not all possible information. A green check mark shows that all information for that tab has been entered. To save the devices to the Repository, each tab must show a check mark of green or yellow.

Importing Connections with NPC Auto Discovery

To discover connections, referred to as Named Physical Circuits (NPC), run NPC Auto Discovery. This task defines the PE and CE link information, which is used by Common Discovery in the final stage of the Auto Discovery process. NPC Auto Discovery has one prerequisite, the **connection.xml** file. Ensure that this file has been uploaded from the ISC server to the client workstation before running this task.

To import connections with NPC Auto Discovery, follow these steps:

-
- Step 1** Choose **Tasks > Start NPC Auto Discovery**.
- You are prompted to provide the path to the correct **connection.xml** file.
- Step 2** Select the correct **connection.xml** file and click **OK**.
- A dialog box appears, indicating that the NPC discovery process has started.
- Step 3** You are prompted if the task completes successfully. Select **OK** to finish this portion of the NPC Auto Discovery process.
- To find the discovered NPCs, go to **Service Inventory > Inventory and Connection Manager > Named Physical Circuits**.
-

Importing Services with Service Discovery

At this point, you can choose to run the Common Discovery process. ISC manages Ethernet over MPLS (L2VPN) and MPLS networks with IPsec (IPsec: **This feature is not supported in this release**). To detect free interfaces on each device for provisioning purposes, existing services either need to be discovered automatically or entered into the system manually.

For very large networks with many provisioned services, manual entry is time consuming and prone to human error. These issues are alleviated by the Common Discovery process. The Common Discovery process discovers:

- Layer 3 MPLS VPN services
- Layer 2 VPN (Metro) services
- Layer 2 VPN (L2TPv3) services.

To specifically import services with Auto Discovery, follow these steps:

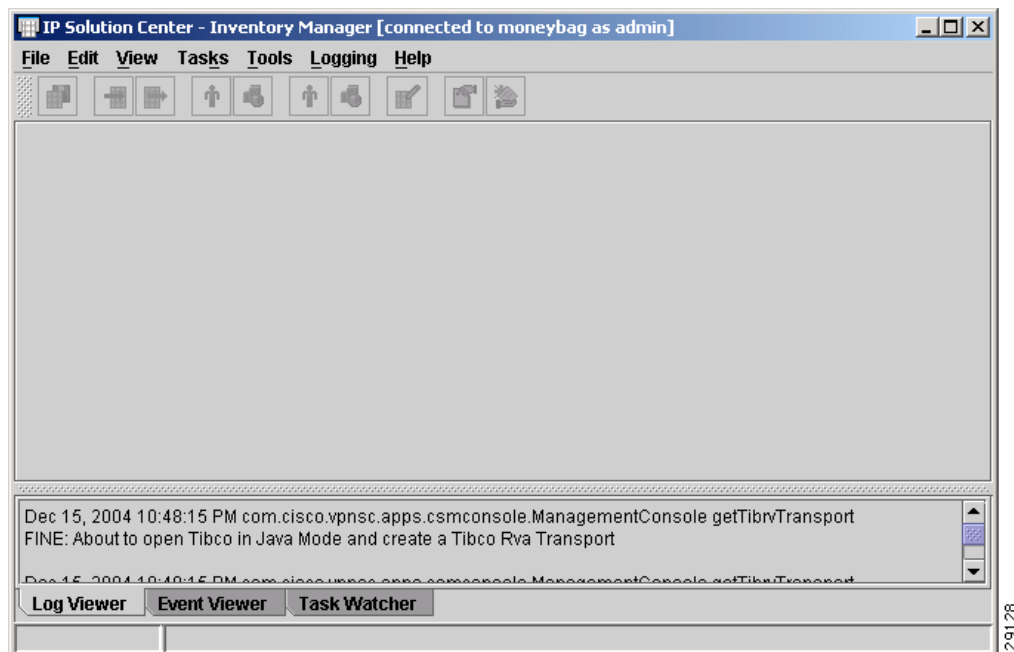
-
- Step 1** Choose **Tasks > Start Service Discovery**.
- The Service Discovery window in [Figure 4-112](#) appears (see [Start Service Discovery, page 4-96](#), for the GUI description). You are prompted to select which type of Common Discovery to perform.
- Step 2** Select one or more types of service discovery by checking the corresponding **Service Discovery** box.
- If you select **L2VPN (L2TPv3)**, the bottom **L2TPv3 Options** section become available:
- Step 3** Make the desired selections
- You are notified when Service Discovery is finished.
- Step 4** To find the discovered service requests, go to **Service Inventory > Inventory and Connection Manager > Service Requests**.
-

Introducing the Inventory Manager GUI

Although Inventory Manager has the physical look and feel of many windows applications, with File, Edit, View, Tasks, Tools, Logging, and Help menus, the application is designed to have the logical view of a spreadsheet. When you learn how to use one spreadsheet in Inventory Manager, you learn how to use them all.

After starting up Inventory Manager by following the steps outlined in [Launching Inventory Manager, page 4-3](#), the main Inventory Manager window in [Figure 4-4](#) appears.

Figure 4-5 Inventory Manager GUI



The various GUI elements are explained in the following sections and in [Inventory Manager GUI Reference, page 4-34](#).

This section contains the following sections:

- [Spreadsheet Features, page 4-13](#)
- [Provider Spreadsheet, page 4-15](#)
- [Customer Spreadsheet, page 4-22](#)
- [Device Group Spreadsheet, page 4-29](#)

Spreadsheet Features

This section contains the following sections:

- [Understanding the Spreadsheet, page 4-13](#)
- [Editing the Spreadsheet, page 4-14](#)

Understanding the Spreadsheet

Before using Inventory Manager, you need to know about these spreadsheet features:

- Spreadsheets
 - Contain Device Group and physical device information.
 - Contain PE and CPE logical device information.
 - Group information or attributes by tabs.
- Tabs
 - Contain a unique table of rows and columns within a spreadsheet.
 - Show the status of the entire spreadsheet with icons.
 - Signify with a Red X that the tab is missing required information.
 - Signify with a Yellow Arrow that the tab contains all required information, but not all optional information.
 - Signify with a Green Arrow that all required and optional information in the tab is provided.
- Rows
 - Contain information or attributes about a single device, module, or interface.
- Columns
 - Contain one type of information or attribute.
 - Have a unique description.
 - Have a Column Heading
 - Have referenced tabs. (For example, Domain Name is in every general tab for each spreadsheet.)
 - Sort up or down by clicking on the column header or clicking the column header and choosing a sort menu.
 - Sort a column in one tab of a spreadsheet to affect all other tables in the spreadsheet.

- Column Heading
 - Has a popup menu to click for selection, de-selection, and sorting.
 - Can have a color, depending on the column status (all cells combined for one column ordered together).
 - Indicates the status of the individual column with color. (As opposed to the Tab icon referenced above, which displays the status of the entire spreadsheet.)
- Host Name Column
 - Does not scroll and is always the first column on the left.
 - Selects or de-selects an entire row.
 - Available in every tab for a given logical or physical device.
 - Acts as a reference point when switching among tabs and scrolling to the right when columns exceed the window width (see menu **View > Fit Columns in Window**).

**Note**

When debugging why a tab has a Red X, this can help to identify the column in error, or missing data, very quickly.

Editing the Spreadsheet

When you learn how to set defaults or edit columns in one spreadsheet, you can set defaults or edit columns for each type of spreadsheet in Inventory Manager.

Cell Editing

Cell editing has the following features:

- Provides dialog box when you click a cell.
- Provides choices for each attribute. (Device Role is either Cisco IOS, CATOS, PIX, or VPN 3000. (IPsec, firewall, NAT, VPN 3000: **These features are not supported in this release**))
- Provides a simple input text dialog for some columns.
- Provides a password editor for some columns.
- Provides a choice dialog with a list of available options for some columns.

Cells

Cells have the following editing features:

- Can be edited by clicking. (Most individual cells can be edited, but not all columns.)
- Select or de-select multiple cells spanning multiple columns using standard selection techniques (Click, Shift-Click, or Ctrl-Click).
- Edit multiple cells in a single column at once using **Edit > Edit Selected Devices**.
- Edit multiple cells spanning multiple columns all at once using **Edit > Edit Selected Devices**.

**Note**

Close a spreadsheet by choosing **File > Close filename**. Do not forget to save your edits.

Provider Spreadsheet

The Provider spreadsheets contain the following tabs:

- [General, page 4-15](#)
- [Passwords, page 4-16](#)
- [SNMPv3 Attributes, page 4-17](#)
- [PE Attributes, page 4-18](#)
- [PE Interfaces, page 4-19](#)
- [CNS Attributes, page 4-21](#)
- [Platform Information, page 4-21](#)

General

Figure 4-6 shows an example of the General tab:

Figure 4-6 Provider Spreadsheet - General Tab

Host Name	Device Type	Device Description	Management Address	Domain Name	Access Protocol	Config Upload/Download	SNMP Version	Device Groups
enswosr3	Cisco Router			cisco.com	Default	Default	Default	
enswosr1	Cisco Router			cisco.com	Default	Default	Default	
enswosr4	Cisco Router			cisco.com	Default	Default	Default	
enswosr2	Cisco Router			cisco.com	Default	Default	Default	

The General tab contains the following columns:

- **Host Name**—Must begin with a letter, digit, or underscore followed by letters, digits, underscores, spaces, hyphens, or dots ending with a letter, digit, or underscore. This field is required and must match the name configured on the target router device. Limited to 256 characters.
- **Device Type**—The device type includes the following devices:
 - Cisco Router
 - Catalyst OS device
 - Terminal server

- VPN 3000 (**This feature is not supported in this release**)
- PIX firewall (**This feature is not supported in this release**)
- IE2100 (Cisco CNS appliance)
- **Device Description**—Can contain any pertinent information about the device, such as the type of device, its location, or other information that might be helpful to service provider operators. Limited to 80 characters.
- **Management Address**—Valid IP address of the device that ISC uses to configure the target router device. This IP address must be reachable from the ISC host.
- **Domain Name**—Must begin with a letter, digit, or underscore followed by letters, digits, underscores, spaces, hyphens, or dots ending with a letter, digit, or underscore. The name must match the domain name on the target router device.
- **Access Protocol**—Administers the access protocol for config upload and download. Choices include: Telnet, Secure Shell (SSH), and CNS. Default: Telnet
- **Config Upload/Download**—Protocol for downloading configurations. Choices include: Terminal, TFTP, and FTP. Default: Terminal.
- **SNMP Version**—Configures the version of SNMP to use when communicating with the device. Choices include: SNMP v1/v2c and SNMP v3. Default: SNMP v1/v2c.
- **Device Groups**—Lists the names of the Device Groups. You can add and modify Device Groups in this column.

Passwords

Figure 4-7 shows an example of the Passwords tab:

Figure 4-7 Provider Spreadsheet - Password Tab

General	Passwords	SNMPv3 Attributes	PE Attributes	PE Interfaces	CNS Attributes	Platform Information
Host Name	Login User	Login Password	Enable User	Enable Password	SNMP Read-Only	SNMP Read-Write
enswosr1		*****		*****	public	private
enswosr2		*****		*****	public	private
enswosr3		*****		*****	public	private
enswosr4		*****		*****	public	private

101023

The Passwords tab contains the following columns:

- **Host Name**—Must begin with a letter, digit, or underscore followed by letters, digits, underscores, spaces, hyphens, or dots ending with a letter, digit, or underscore. This field is required and must match the name configured on the target router device. Limited to 256 characters.
- **Login User**—Not required by ISC. However, collection and upload/download will not function without the Login User and Login Password, as ISC will not be able to access the device. Should match what is configured on the target router device. Limited to 80 characters.
- **Login Password**—Displayed as stars (*). Not required by ISC. However, collection and upload/download will not function without the Login User and Login Password, as ISC will not be able to access the device. Should match what is configured on the target router device. Limited to 80 characters.

- **Enable User**—Not required by ISC. However, collection and upload/download only function if the Login User has sufficient privileges to configure the router in EXEC mode. Should match what is configured on the target router device. Limited to 80 characters.
- **Enable Password**—Displayed as stars (*). Not required by ISC. However, collection and upload/download only function if the Login User has sufficient privileges to configure the router in EXEC mode. Should match what is configured on the target router device. Limited to 80 characters.
- **SNMP Read-Only**—SNMP Read-Only (Community String RO). Many tasks use SNMP to access the device. This field must match what is configured on the target router device. Limited to 80 characters.
- **SNMP Read-Write**—SNMP Read-Write (Community String RW). Many tasks use SNMP to access the device. This field must match what is configured on the target router device. Limited to 80 characters.

SNMPv3 Attributes

Figure 4-8 shows an example of the SNMPv3 Attributes tab:

Figure 4-8 Provider Spreadsheet - SNMPv3 Attributes Tab

General Passwords SNMPv3 Attributes PE Attributes PE Interfaces CNS Attributes Platform Information						
Host Name	Security Level	Authentication User	Authentication Password	Authentication Algorithm	Encryption Password	Encryption Algorithm
enswosr1	Default			NA		None
enswosr2	Default			NA		None
enswosr3	Default			NA		None
enswosr4	Default			NA		None

101024

The SNMPv3 Attributes contains the following columns:

- **Host Name**—Must begin with a letter, digit, or underscore followed by letters, digits, underscores, spaces, hyphens, or dots ending with a letter, digit, or underscore. This field is required and must match the name configured on the target router device. Limited to 256 characters.
- **Security Level**—Choices include: No Authentication/No Encryption, Authentication/No Encryption, and Authentication/Encryption. Default: No Authentication/No Encryption.
- **Authentication User**—User name configured on the specified device router. User must have permission to the object identification numbers (OIDs) specified in the security request (that is, write permission for a set request, and read permission for a get request). Should match what is configured on the target router device. Should be provisioned if the SNMP Security Level is Authentication/No Encryption or Authentication/Encryption. Limited to 80 characters.
- **Authentication Password**—Displayed as stars (*). Should be provisioned if the SNMP Security Level is Authentication/No Encryption or Authentication/Encryption. Should match what is configured on the target router device. Limited to 80 characters.
- **Authentication Algorithm**—Should be provisioned if the SNMP Security Level is Authentication/No Encryption or Authentication/Encryption. Choices include: None, Authentication. Message Digest 5 (MD5), and the Secure Hash Algorithm (SHA). Default: None.

- **Encryption Password**—Displayed as stars (*). In previous versions, this field was called Privacy Password. Should match what is configured on the target router device. Should be provisioned if the SNMP Security Level is Authentication/Encryption. Limited to 80 characters.
- **Encryption Algorithm**—In previous versions, this field was called Privacy Protocol. Should be provisioned if the SNMP Security Level is Authentication/Encryption. Choices include: None and IPsec Data Encryption Standard (DES 56). Default: None.



Note IPsec: This feature is not supported in this release.

PE Attributes

Figure 4-9 shows an example of the PE Attributes tab:

Figure 4-9 Provider Spreadsheet - PE Attributes Tab

General Passwords SNMPv3 Attributes PE Attributes PE Interfaces CNS Attributes Platform Information					
Host Name	Provider Name	Region Name	Role	Loopback Interface	Is Managed
enswosr1	PROVIDER-Y	WEST-Y	PE POP	Loopback0 : 192.168.115.100/32	☒
enswosr2	PROVIDER-Y	SOUTH-Y	PE POP	Loopback0 : 192.168.115.101/32	☒
enswosr3	PROVIDER-Y	EAST-Y	PE POP	Loopback0 : 192.168.115.12/32	☒
enswosr4	PROVIDER-Y	NORTH-Y	PE POP	Loopback0 : 192.168.114.53/32	☒

The PE Attributes tab contains the following columns:

- **Host Name**—Must begin with a letter, digit, or underscore followed by letters, digits, underscores, spaces, hyphens, or dots ending with a letter, digit, or underscore. This field is required and must match the name configured on the target router device. Limited to 256 characters.
- **Provider Name**—Lists the names of providers. Must begin with a letter. Can contain letters, numbers, and these punctuation characters: period, underscore, and dash. Limited to 80 characters. You can sort the list by provider name.
- **Region Name**—Lists the names of regions. Must begin with a letter. Can contain letters, numbers, and these punctuation characters: period, underscore, and dash. Limited to 80 characters. You can sort the list by region name.
- **Role**—Choices include: PE POP, PE CLE, PE CORE, and PE MVRP.
- **Loopback Interface**—Loopback address is the IP address of any loopback interface on the device. You can select one of the loopback interfaces for this field and use the IP address on that loopback interface.
- **IS Managed**—Provisioned by ISC. Click the check box for yes. Default is no.

PE Interfaces

Figure 4-10 shows an example of the PE Interfaces tab:

Figure 4-10 Provider Spreadsheet - PE Interfaces Tab

Host Name	IP Address	Type	Encapsulation	IPsec	Firewall	NAT	QoS Candidate	PIX Logical-Name	PIX Security-Level	Description
enswosr1										
FastEthernet8/2		fastethernet	dot1q	none	none	none	none			CONNECTIO...
GE-WAN9/2		gigabitethern...	ethernet	none	none	none	none			By VPNSC: J...
GE-WAN9/2.100		gigabitethern...		none	none	none	none			By VPNSC: J...

The PE Interfaces tab contains the following columns:

- **Host Name**—Must begin with a letter, digit, or underscore followed by letters, digits, underscores, spaces, hyphens, or dots ending with a letter, digit, or underscore. This field is required and must match the name configured on the target router device. Limited to 256 characters.
- **IP Address**—IP address associated with this interface.
- **Type**—Specifies the type of interface. It is a display-only field. Types include:
 - VLAN
 - UNKNOWN
 - STATIC
 - UNNUMBERED
 - DHCP
 - PPP
 - DOCSIS
- **Encapsulation**—The Layer 2 Encapsulation for this device. It is a display-only field. Choices include:
 - UNKNOWN
 - DEFAULT
 - DOT1Q
 - ETHERNET
 - ISL
 - FRAME_RELAY
 - FRAME_RELAY_IETF
 - HDLS
 - PPP
 - ATM
 - AAL5SNAP
 - AAL0
 - AAL5

- AAL5MUX
- AAL5NLPID
- AAL2
- ENCAP_QinQ
- GRE
- **IPsec—This feature is not supported in this release.**
View or edit (mark) interface settings for IPsec. Choices include:
 - None
 - Public
Interface to the public network (internet). All traffic is encrypted.
 - Private
Interface to the private network (internal LAN). All traffic is not encrypted.
- **Firewall—This feature is not supported in this release**
View or edit (mark) interface settings for Firewall. If Device Type is VPN 3000, Firewall is not available. Choices include:
 - Inside
Highest security interface.
 - Outside
Lowest security interface.
 - DMZ 1, ..., DMZ N
The Demilitarized Zone services to both inside and outside interfaces.
- **NAT—This feature is not supported in this release**
View or edit (mark) interface settings for NAT. If Device Type is PIX firewall or VPN 3000, NAT is not available. Choices include:
 - None
 - Inside
Highest security interface.
 - Outside
Lowest security interface.
- **QoS Candidate—View or edit (mark) interface settings for QoS. If Device Type is VPN 3000 (This feature is not supported in this release), QoS is not available. Choices include:**
 - None
 - Marking Rate Limit
This setting marks the Customer LAN facing interface with the **set** and **police** commands.
 - Endpoint
This setting marks the PE facing interface on the CE device and the CE facing interface on the PE device.
On the PE side, all QoS commands go on this interface.

On the CE side, all QoS commands, including the **set** and **police** commands, go on this interface if no interface on the CE device is identified as the Marking Rate Limit interface.

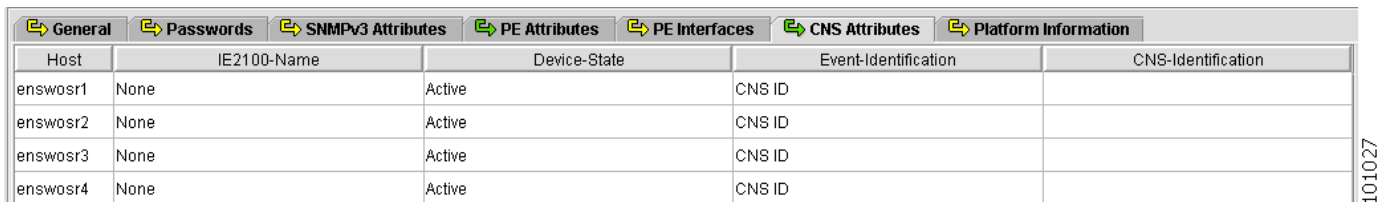
If one or more interfaces have been identified as Marking Rate Limit interfaces, then all QoS commands except the **set** and **police** commands go on this interface.

- **PIX Logical-Name**—Logical name of this interface. This field is displayed only. Field is populated by a collection/import of config file.
- **PIX Security-Level**—Security level of this interface. This field is display-only. Field is populated by importing a configuration file.
- **Description**—Description of the interface. This field is display-only. Field is populated by importing a configuration file.

CNS Attributes

Figure 4-11 shows an example of the CNS Attributes tab:

Figure 4-11 Provider Spreadsheet - CNS Attributes Tab



Host	IE2100-Name	Device-State	Event-Identification	CNS-Identification
enswosr1	None	Active	CNS ID	
enswosr2	None	Active	CNS ID	
enswosr3	None	Active	CNS ID	
enswosr4	None	Active	CNS ID	

The CNS Attributes tab contains the following columns:

- **Host Name**—Must begin with a letter, digit, or underscore followed by letters, digits, underscores, spaces, hyphens, or dots ending with a letter, digit, or underscore. This field is required and must match the name configured on the target router device. Limited to 256 characters.
- **IE2100-Name**—Disabled unless the Device-State field is Inactive or the Terminal Session Protocol field is CNS. A valid Cisco CNS appliance (CNS) must be selected if the Terminal Session Protocol is CNS. Choices include: None and the list of existing CNS names. Default: None.
- **Device-State**—Choices include: Active and Inactive. Active indicates that the router has been plugged on the network and can be part of ISC tasks such as collect config and provisioning. Inactive indicates the router has not been plugged-in. Default: Active.
- **Event-Identification**—Indicates whether the CNS Identification field contains a HOST NAME or CNS ID. Default: HOST NAME.
- **CNS-Identification**—Required if the Event Identification field is set to CNS ID. Can contain letters, numbers, and these punctuation characters: period, underscore, and dash.

Platform Information

Figure 4-12 shows an example of the Platform Information tab. These fields are typically filled in from the physical device during the collection process.

Figure 4-12 Provider Spreadsheet - Platform Information Tab

General Passwords SNMPv3 Attributes PE Attributes PE Interfaces CNS Attributes Platform Information				
Host	Platform	Software	Image	Serial
enswosr1	OSR-7609	12.2(vpls_eff_1.0.030630.)	c6sup2_rp-JSV-M:c6k222-jsv-mz.999-99...	
enswosr2	OSR-7609	12.2(vpls_eff_1.0.030630.)	c6sup2_rp-JSV-M:c6k222-jsv-mz.999-99...	
enswosr3	CISCO7606	12.2(vpls_eff_1.0.030630.)	c6sup2_rp-JSV-M:c6k222-jsv-mz.999-99...	
enswosr4	CISCO7606	12.2(vpls_eff_1.0.030630.)	c6sup2_rp-JSV-M:c6k222-jsv-mz.999-99...	

101028

The Platform Information tab contains the following columns:

- **Host Name**—Must begin with a letter, digit, or underscore followed by letters, digits, underscores, spaces, hyphens, or dots ending with a letter, digit, or underscore. This field is required and must match the name configured on the target router device. Limited to 256 characters.
- **Platform**—Should match what is configured on the target router device. Limited to 80 characters.
- **Software**—Should match what is configured on the target router device. Limited to 80 characters.
- **Image**—Should match what is configured on the target router device. Limited to 80 characters.
- **Serial**—Should match what is configured on the target router device. Limited to 80 characters

Customer Spreadsheet

The Customer spreadsheets contain the following tabs:

- [General, page 4-23](#)
- [Passwords, page 4-24](#)
- [SNMPv3 Attributes, page 4-25](#)
- [CPE Attributes, page 4-26](#)
- [CPE Interfaces, page 4-26](#)
- [CNS Attributes, page 4-28](#)
- [Platform Information, page 4-29](#)

General

Figure 4-13 shows an example of the General tab:

Figure 4-13 Customer Spreadsheet - General Tab

Host Name	Device Type	Device Description	Management Address	Domain Name	Access Protocol	Config Upload/Download	SNMP Version	Device Groups
mlce10	Cisco Router			cisco.com	Default	Default	Default	
mlce11	Cisco Router			cisco.com	Default	Default	Default	
mlce3	Cisco Router			cisco.com	Default	Default	Default	
mlce4	Cisco Router			cisco.com	Default	Default	Default	
mlce5	Cisco Router			cisco.com	Default	Default	Default	
mlce6	Cisco Router			cisco.com	Default	Default	Default	
mlce7	Cisco Router			cisco.com	Default	Default	Default	

The General tab contains the following columns:

- **Host Name**—Must begin with a letter, digit, or underscore followed by letters, digits, underscores, spaces, hyphens, or dots ending with a letter, digit, or underscore. This field is required and must match the name configured on the target router device. Limited to 256 characters.
- **Device Type**—The device type includes the following devices:
 - Cisco Router
 - Catalyst OS device
 - Terminal server
 - VPN 3000 (**This feature is not supported in this release**)
 - PIX firewall (**This feature is not supported in this release**)
 - IE2100 (Cisco CNS appliance)
- **Device Description**—Can contain any pertinent information about the device, such as the type of device, its location, or other information that might be helpful to service provider operators. Limited to 80 characters.
- **Management Address**—Valid IP address of the device that ISC uses to configure the target router device. This IP address must be reachable from the ISC host.
- **Domain Name**—Must begin with a letter, digit, or underscore followed by letters, digits, underscores, spaces, hyphens, or dots ending with a letter, digit, or underscore. The name must match the domain name on the target router device.

- **Access Protocol**—Administers the access protocol for config upload and download. Choices include: Telnet, Secure Shell (SSH), and CNS. Default: Telnet
- **Config Upload/Download**—Choices include: Terminal, TFTP, and FTP. Default: Terminal.
- **SNMP Version**—Configures the version of SNMP to use when communicating with the device. Choices include: SNMP v1/v2c and SNMP v3. Default: SNMP v1/v2c.
- **Device Groups**—Lists the names of the Device Groups. You can add and modify Device Groups in this column.

Passwords

Figure 4-14 shows an example of the Passwords tab:

Figure 4-14 Customer Spreadsheet - Passwords Tab

General	Passwords	SNMPv3 Attributes	CPE Attributes	CPE Interfaces	CNS Attributes	Platform Information
Host Name	Login User	Login Password	Enable User	Enable Password	SNMP Read-Only	SNMP Read-Write
mlce10		*****		*****	public	private
mlce11		*****		*****	public	private
mlce3		*****		*****	public	private
mlce4		*****		*****	public	private

The Passwords tab contains the following columns:

- **Host Name**—Must begin with a letter, digit, or underscore followed by letters, digits, underscores, spaces, hyphens, or dots ending with a letter, digit, or underscore. This field is required and must match the name configured on the target router device. Limited to 256 characters.
- **Login User**—Not required by ISC. However, collection and upload/download will not function without the Login User and Login Password, as ISC will not be able to access the device. Should match what is configured on the target router device. Limited to 80 characters.
- **Login Password**—Displayed as stars (*). Not required by ISC. However, collection and upload/download will not function without the Login User and Login Password, as ISC will not be able to access the device. Should match what is configured on the target router device. Limited to 80 characters.
- **Enable User**—Not required by ISC. However, collection and upload/download only function if the Login User has sufficient privileges to configure the router in EXEC mode. Should match what is configured on the target router device. Limited to 80 characters.
- **Enable Password**—Displayed as stars (*). Not required by ISC. However, collection and upload/download only function if the Login User has sufficient privileges to configure the router in EXEC mode. Should match what is configured on the target router device. Limited to 80 characters.
- **SNMP Read-Only**—SNMP Read-Only (Community String RO). Many tasks use SNMP to access the device. This field must match what is configured on the target router device. Limited to 80 characters.
- **SNMP Read-Write**—SNMP Read-Write (Community String RW). Many tasks use SNMP to access the device. This field must match what is configured on the target router device. Limited to 80 characters.

SNMPv3 Attributes

Figure 4-15 shows an example of the SNMPv3 Attributes tab:

Figure 4-15 Customer Spreadsheet - SNMPv3 Attributes Tab

General Passwords SNMPv3 Attributes CPE Attributes CPE Interfaces CNS Attributes Platform Information						
Host Name	Security Level	Authentication User	Authentication Password	Authentication Algorithm	Encryption Password	Encryption Algorithm
mlce10	Default			NA		None
mlce11	Default			NA		None
mlce3	Default			NA		None
mlce4	Default			NA		None

The SNMPv3 Attributes contains the following columns:

- **Host Name**—Must begin with a letter, digit, or underscore followed by letters, digits, underscores, spaces, hyphens, or dots ending with a letter, digit, or underscore. This field is required and must match the name configured on the target router device. Limited to 256 characters.
- **Security Level**—Choices include: No Authentication/No Encryption, Authentication/No Encryption, and Authentication/Encryption. Default: No Authentication/No Encryption.
- **Authentication User**—User name configured on the specified device router. User must have permission to the object identification numbers (OIDs) specified in the security request (that is, write permission for a set request, and read permission for a get request). Should match what is configured on the target router device. Should be provisioned if the SNMP Security Level is Authentication/No Encryption or Authentication/Encryption. Limited to 80 characters.
- **Authentication Password**—Displayed as stars (*). Should be provisioned if the SNMP Security Level is Authentication/No Encryption or Authentication/Encryption. Should match what is configured on the target router device. Limited to 80 characters.
- **Authentication Algorithm**—Should be provisioned if the SNMP Security Level is Authentication/No Encryption or Authentication/Encryption. Choices include: None, MD5, and SHA. Default: None.
- **Encryption Password**—Displayed as stars (*). In previous versions, this field was called Privacy Password. Should match what is configured on the target router device. Should be provisioned if the SNMP Security Level is Authentication/Encryption. Limited to 80 characters.
- **Encryption Algorithm**—In previous versions, this field was called Privacy Protocol. Should be provisioned if the SNMP Security Level is Authentication/Encryption. Choices include: None and DES 56. Default: None.

CPE Attributes

Figure 4-16 shows an example of the CPE Attributes tab:

Figure 4-16 Customer Spreadsheet - CPE Attributes Tab

General	Passwords	SNMPv3 Attributes	CPE Attributes	CPE Interfaces	CNS Attributes	Platform Information
Host Name	Customer Name	Site Name		Management Type		
mlce10	CUSTOMER-A	CUSTOMER-A-Site-mlce10		Managed		
mlce11	CUSTOMER-A	CUSTOMER-A-Site-mlce11		Managed		
mlce3	CUSTOMER-A	CUSTOMER-A-Site-mlce3		Multi-VRF		
mlce4	CUSTOMER-A	CUSTOMER-A-Site-mlce4		Managed		

The CPE Attributes tab contains the following columns:

- **Host Name**—Must begin with a letter, digit, or underscore followed by letters, digits, underscores, spaces, hyphens, or dots ending with a letter, digit, or underscore. This field is required and must match the name configured on the target router device. Limited to 256 characters.
- **Customer Name**—Lists the names of the customer. The first character must be a letter. Can contain letters, numbers, and these punctuation characters: period, underscore, and dash. Limit: 80 characters. You can sort the list by customer name.
- **Site Name**—Lists the names of sites. The first character must be a letter. Can contain letters, numbers, and these punctuation characters: period, underscore, and dash. Limit: 80 characters. You can sort the list by site name.
- **Management Type**—Choices include: Managed, Unmanaged, Managed - Management LAN, Unmanaged - Management LAN, Directly Connected, Directly Connected Management Host, and Multi-VRF.

CPE Interfaces

Figure 4-17 shows an example of the CPE Interfaces tab:

Figure 4-17 Customer Spreadsheet - CPE Interfaces Tab

General											Passwords	SNMPv3 Attributes	CPE Attributes	CPE Interfaces	CNS Attributes	Platform Information			
Host Name	IP Address	Type	Encapsulation	IPsec	Firewall	NAT	QoS Candidate	PIX Logical-Name	PIX Security-Level	Description									
mlce10																			
ATM1/0		atm		none	none	none	none												
FastEthernet0/0		172.29.146.3...	fastethernet	ethernet	none	none	none	none		CONNECTIO...									
mlce11																			

The CPE Interfaces tab contains the following columns:

- **Host Name**—Must begin with a letter, digit, or underscore followed by letters, digits, underscores, spaces, hyphens, or dots ending with a letter, digit, or underscore. This field is required and must match the name configured on the target router device. Limited to 256 characters.
- **IP Address**—IP address associated with this interface.
- **Type**—Specifies the type of interface. It is a display-only field.

- **Encapsulation**—The Layer 2 Encapsulation for this device. It is a display-only field. Choices include:
 - UNKNOWN
 - DEFAULT
 - DOT1Q
 - ETHERNET
 - ISL
 - FRAME_RELAY
 - FRAME_RELAY_IETF
 - HDLS
 - PPP
 - ATM
 - AAL5SNAP
 - AAL0
 - AAL5
 - AAL5MUX
 - AAL5NLPID
 - AAL2
 - ENCAP_QinQ
 - GRE
- **IPsec**—**This feature is not supported in this release**
View or edit (mark) interface settings for IPsec. Choices include:
 - None
 - Public
Interface to the public network (internet). All traffic is encrypted.
 - Private
Interface to the private network (internal LAN). All traffic is not encrypted.
- **Firewall**—**This feature is not supported in this release**
View or edit (mark) interface settings for Firewall. If Device Type is VPN 3000, Firewall is not available. Choices include:
 - Inside
Highest security interface.
 - Outside
Lowest security interface.
 - DMZ 1, ..., DMZ N
The Demilitarized Zone services to both inside and outside interfaces.

- **NAT—This feature is not supported in this release**
View or edit (mark) interface settings for NAT. If Device Type is PIX firewall or VPN 3000, NAT is not available. Choices include:
 - None
 - Inside
Highest security interface.
 - Outside
Lowest security interface.
- **QoS Candidate**—View or edit (mark) interface settings for QoS. If Device Type is VPN 3000 (**This feature is not supported in this release**), QoS is not available. Choices include:
 - None
 - Marking Rate Limit
This setting marks the Customer LAN facing interface with the **set** and **police** commands.
 - Endpoint
This setting marks the PE facing interface on the CE device and the CE facing interface on the PE device.
On the PE side, all QoS commands go on this interface.
On the CE side, all QoS commands, including the **set** and **police** commands, go on this interface if no interface on the CE device is identified as the Marking Rate Limit interface.
If one or more interfaces have been identified as Marking Rate Limit interfaces, then all QoS commands except the **set** and **police** commands go on this interface.
- **PIX Logical-Name**—Logical name of this interface. This field is displayed only. Field is populated by a collection/import of config file.
- **PIX Security-Level**—Security level of this interface. This field is display-only. Field is populated by importing a configuration file.
- **Description**—Description of the interface. This field is display-only. Field is populated by importing a configuration file.

CNS Attributes

Figure 4-18 shows an example of the CNS Attributes tab:

Figure 4-18 Customer Spreadsheet - CNS Attributes Tab

General Passwords SNMPv3 Attributes CPE Attributes CPE Interfaces CNS Attributes Platform Information				
Host	IE2100-Name	Device-State	Event-Identification	CNS-Identification
mlce10	None	Active	Host Name	
mlce11	None	Active	Host Name	
mlce3	None	Active	Host Name	
mlce4	None	Active	Host Name	

101016

The CNS Attributes tab contains the following columns:

- **Host Name**—Must begin with a letter, digit, or underscore followed by letters, digits, underscores, spaces, hyphens, or dots ending with a letter, digit, or underscore. This field is required and must match the name configured on the target router device. Limited to 256 characters.
- **IE2100-Name**—Disabled unless the Device-State field is Inactive or the Terminal Session Protocol field is CNS. A valid Cisco CNS IE2100 appliance must be selected if the Terminal Session Protocol is CNS. Choices include: None and the list of existing Cisco CNS IE2100 appliance names. Default: None.
- **Device-State**—Choices include: Active and Inactive. Active indicates that the router has been plugged on the network and can be part of ISC tasks such as collect config and provisioning. Inactive indicates the router has not been plugged-in. Default: Active.
- **Event-Identification**—Indicates whether the CNS Identification field contains a HOST NAME or CNS ID. Default: HOST NAME.
- **CNS-Identification**—Required if the Event Identification field is set to CNS ID. Can contain letters, numbers, and these punctuation characters: period, underscore, and dash.

Platform Information

Figure 4-19 shows an example of the Platform Information tab. These fields are typically filled in from the physical device during the collection process.

Figure 4-19 Customer Spreadsheet - Platform Information Tab

General	Passwords	SNMPv3 Attributes	CPE Attributes	CPE Interfaces	CNS Attributes	Platform Information
Host	Platform	Software	Image	Serial		
mlce10	3620	12.2(16.6)	C3620-JS-M:c3620-js-mz.122-16.6			
mlce11	3620	12.3(2.3)	C3620-J1S3-M:c3620-j1s3-mz.123-2.3			
mlce3	3620	12.3(2.3)	C3620-J1S3-M:c3620-j1s3-mz.123-2.3			
mlce4	2621	12.2(16.6)	C2600-JS-M:c2600-js-mz.122-16.6			

The Platform Information tab contains the following columns:

- **Host Name**—Must begin with a letter, digit, or underscore followed by letters, digits, underscores, spaces, hyphens, or dots ending with a letter, digit, or underscore. This field is required and must match the name configured on the target router device. Limited to 256 characters.
- **Platform**—Should match what is configured on the target router device. Limited to 80 characters.
- **Software**—Should match what is configured on the target router device. Limited to 80 characters.
- **Image**—Should match what is configured on the target router device. Limited to 80 characters.
- **Serial**—Should match what is configured on the target router device. Limited to 80 characters.

Device Group Spreadsheet

The Device Group spreadsheets contain the following tabs:

- [General](#), page 4-30
- [Passwords](#), page 4-31
- [SNMPv3 Attributes](#), page 4-32

- [CNS Attributes, page 4-33](#)
- [Platform Information, page 4-33](#)

General

Figure 4-20 shows an example of the General tab:

Figure 4-20 Device Group Spreadsheet - General Tab

Host Name	Device Type	Device Description	Management Address	Domain Name	Access Protocol	Config Upload/Download	SNMP Version	Device Groups
enpe1	Cisco Router				Default	Default	Default	DeviceGroup
enpe2	Cisco Router				Default	Default	Default	DeviceGroup
enpe3	Cisco Router				Default	Default	Default	DeviceGroup
enpe4	Cisco Router				Default	Default	Default	DeviceGroup
enpe5	Cisco Router				Default	Default	Default	DeviceGroup
enpix1	PIX Firewall				Secure Shell (ssh)	Default	Default	DeviceGroup
enpix2	PIX Firewall				Secure Shell (ssh)	Default	Default	DeviceGroup
envpn3k1	VPN3000				Secure Shell (ssh)	Default	Default	DeviceGroup
intce11	Cisco Router				Default	Default	Default	DeviceGroup
intce12	Cisco Router				Default	Default	Default	DeviceGroup
intce13	Cisco Router				Default	Default	Default	DeviceGroup
intce14	Cisco Router				Default	Default	Default	DeviceGroup
intce15	Cisco Router				Default	Default	Default	DeviceGroup

Group: DeviceGroup

The General tab contains the following columns:

- **Host Name**—Must begin with a letter, digit, or underscore followed by letters, digits, underscores, spaces, hyphens, or dots ending with a letter, digit, or underscore. This field is required and must match the name configured on the target router device. Limited to 256 characters.
- **Device Type**—The device type includes the following devices:
 - Cisco IOS router
 - Catalyst OS device
 - Terminal server
 - VPN 3000 (**This feature is not supported in this release**)
 - PIX firewall (**This feature is not supported in this release**)
 - IE2100 (Cisco CNS appliance)
- **Device Description**—Can contain any pertinent information about the device, such as the type of device, its location, or other information that might be helpful to service provider operators. Limited to 80 characters.
- **Management Address**—Valid IP address of the device that ISC uses to configure the target router device. This IP address must be reachable from the ISC host.

- **Domain Name**—Must begin with a letter, digit, or underscore followed by letters, digits, underscores, spaces, hyphens, or dots ending with a letter, digit, or underscore. The name must match the domain name on the target router device.
- **Access Protocol**—Administers the access protocol for config upload and download. Choices include: Telnet, Secure Shell (SSH), and CNS. Default: Telnet
- **Config Upload/Download**—Choices include: Terminal, TFTP, and FTP. Default: Terminal.
- **SNMP Version**—Configures the version of SNMP to use when communicating with the device. Choices include: SNMP v1/v2c and SNMP v3. Default: SNMP v1/v2c.
- **Device Groups**—Lists the names of the Device Groups. You can add and modify Device Groups in this column.

Passwords

Figure 4-21 shows an example of the Passwords tab:

Figure 4-21 Device Group Spreadsheet - Passwords Tab

General Passwords SNMPv3 Attributes CNS Attributes Platform Information						
Host Name	Login User	Login Password	Enable User	Enable Password	SNMP Read-Only	SNMP Read-Write
enpe1		*****		*****	public	private
enpe2		*****		*****	public	private
enpe3		*****		*****	public	private
enpe4		*****		*****	public	private

The Passwords tab contains the following columns:

- **Host Name**—Must begin with a letter, digit, or underscore followed by letters, digits, underscores, spaces, hyphens, or dots ending with a letter, digit, or underscore. This field is required and must match the name configured on the target router device. Limited to 256 characters.
- **Login User**—Not required by ISC. However, collection and upload/download will not function without the Login User and Login Password, as ISC will not be able to access the device. Should match what is configured on the target router device. Limited to 80 characters.
- **Login Password**—Displayed as stars (*). Not required by ISC. However, collection and upload/download will not function without the Login User and Login Password, as ISC will not be able to access the device. Should match what is configured on the target router device. Limited to 80 characters.
- **Enable User**—Not required by ISC. However, collection and upload/download only function if the Login User has sufficient privileges to configure the router in EXEC mode. Should match what is configured on the target router device. Limited to 80 characters.
- **Enable Password**—Displayed as stars (*). Not required by ISC. However, collection and upload/download only function if the Login User has sufficient privileges to configure the router in EXEC mode. Should match what is configured on the target router device. Limited to 80 characters.

- **SNMP Read-Only**—SNMP Read-Only (Community String RO). Many tasks use SNMP to access the device. This field must match what is configured on the target router device. Limited to 80 characters.
- **SNMP Read-Write**—SNMP Read-Write (Community String RW). Many tasks use SNMP to access the device. This field must match what is configured on the target router device. Limited to 80 characters.

SNMPv3 Attributes

Figure 4-22 shows an example of the SNMPv3 Attributes tab:

Figure 4-22 Device Group Spreadsheet - SNMPv3 Attributes Tab

General Passwords SNMPv3 Attributes CNS Attributes Platform Information						
Host Name	Security Level	Authentication User	Authentication Password	Authentication Algorithm	Encryption Password	Encryption Algorithm
enpe1	Default			NA		None
enpe2	Default			NA		None
enpe3	Default			NA		None
enpe4	Default			NA		None

The SNMPv3 Attributes contains the following columns:

- **Host Name**—Must begin with a letter, digit, or underscore followed by letters, digits, underscores, spaces, hyphens, or dots ending with a letter, digit, or underscore. This field is required and must match the name configured on the target router device. Limited to 256 characters.
- **Security Level**—Choices include: No Authentication/No Encryption, Authentication/No Encryption, and Authentication/Encryption. Default: No Authentication/No Encryption.
- **Authentication User**—User name configured on the specified device router. User must have permission to the object identification numbers (OIDs) specified in the security request (that is, write permission for a set request, and read permission for a get request). Should match what is configured on the target router device. Should be provisioned if the SNMP Security Level is Authentication/No Encryption or Authentication/Encryption. Limited to 80 characters.
- **Authentication Password**—Displayed as stars (*). Should be provisioned if the SNMP Security Level is Authentication/No Encryption or Authentication/Encryption. Should match what is configured on the target router device. Limited to 80 characters.
- **Authentication Algorithm**—Should be provisioned if the SNMP Security Level is Authentication/No Encryption or Authentication/Encryption. Choices include: None, MD5, and SHA. Default: None.
- **Encryption Password**—Displayed as stars (*). In previous versions, this field was called Privacy Password. Should match what is configured on the target router device. Should be provisioned if the SNMP Security Level is Authentication/Encryption. Limited to 80 characters.
- **Encryption Algorithm**—In previous versions, this field was called Privacy Protocol. Should be provisioned if the SNMP Security Level is Authentication/Encryption. Choices include: None and DES 56. Default: None.

CNS Attributes

Figure 4-23 shows an example of the CNS Attributes tab:

Figure 4-23 Device Group Spreadsheet - CNS Attributes Tab

General	Passwords	SNMPv3 Attributes	CNS Attributes	Platform Information
Host	IE2100-Name	Device-State	Event-Identification	CNS-Identification
enpe1	None	Active	Host Name	
enpe2	None	Active	Host Name	
enpe3	None	Active	Host Name	
enpe4	None	Active	Host Name	

The CNS Attributes tab contains the following columns:

- **Host Name**—Must begin with a letter, digit, or underscore followed by letters, digits, underscores, spaces, hyphens, or dots ending with a letter, digit, or underscore. This field is required and must match the name configured on the target router device. Limited to 256 characters.
- **IE2100-Name**—Disabled unless the Device-State field is Inactive or the Terminal Session Protocol field is CNS. A valid Cisco CNS IE2100 appliance must be selected if the Terminal Session Protocol is CNS. Choices include: None and the list of existing Cisco CNS IE2100 appliance names. Default: None.
- **Device-State**—Choices include: Active and Inactive. Active indicates that the router has been plugged on the network and can be part of ISC tasks such as collect config and provisioning. Inactive indicates the router has not been plugged-in. Default: Active.
- **Event-Identification**—Indicates whether the CNS Identification field contains a HOST NAME or CNS ID. Default: HOST NAME.
- **CNS-Identification**—Required if the Event Identification field is set to CNS ID. Can contain letters, numbers, and these punctuation characters: period, underscore, and dash.

Platform Information

Figure 4-24 shows an example of the Platform Information tab. These fields are typically filled in from the physical device during the collection process.

Figure 4-24 Device Group Spreadsheet - Platform Information Tab

General	Passwords	SNMPv3 Attributes	CNS Attributes	Platform Information
Host	Platform	Software	Image	Serial
enpe1				
enpe2				
enpe3				
enpe4				

The Platform Information tab contains the following columns:

- **Host Name**—Must begin with a letter, digit, or underscore followed by letters, digits, underscores, spaces, hyphens, or dots ending with a letter, digit, or underscore. This field is required and must match the name configured on the target router device. Limited to 256 characters.

- **Platform**—Should match what is configured on the target router device. Limited to 80 characters.
- **Software**—Should match what is configured on the target router device. Limited to 80 characters.
- **Image**—Should match what is configured on the target router device. Limited to 80 characters.
- **Serial**—Should match what is configured on the target router device. Limited to 80 characters.

Inventory Manager GUI Reference

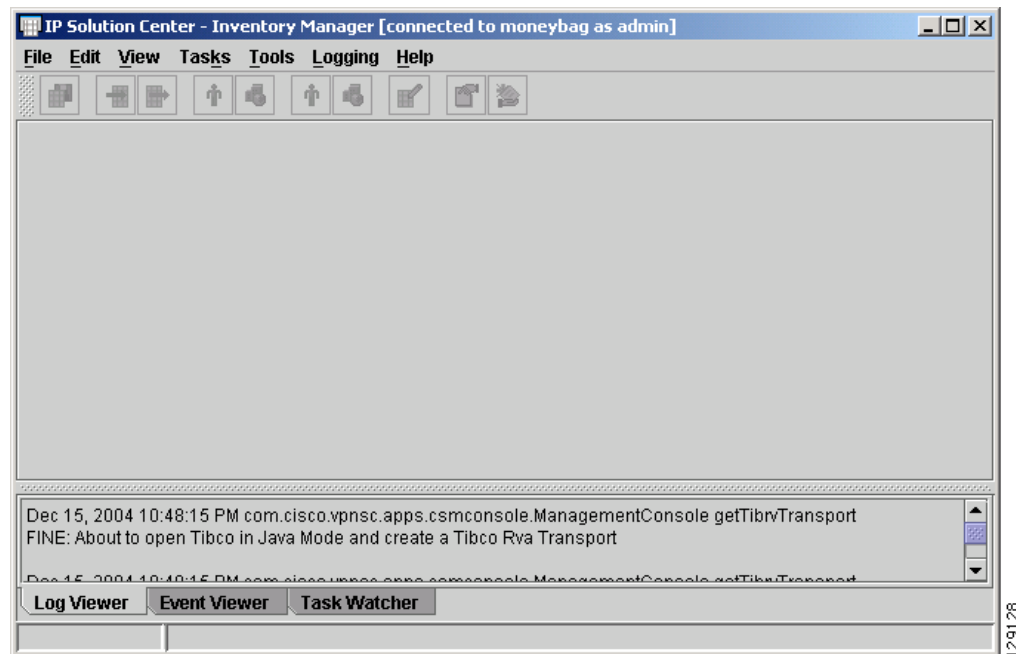
This section describes the Inventory Manager GUI. It is organized by the external design of the GUI: what you see when you look at the windows, menus, and options. It is intended for new users who want to get started with Inventory Manager, and for experienced users who need a reference for the GUI workflow.

To access the Inventory Manager GUI, follow these steps:

-
- Step 1** Log in to ISC.
 - Step 2** Choose **Service Inventory > Inventory and Connection Manager > Inventory Manager**.
 - Step 3** Click the Inventory Manager icon.

After initializing Java Web Start, Inventory Manager appears, as shown in [Figure 4-25](#).

Figure 4-25 *Inventory Manager*



You now have access to the Inventory Manager Task Bar.

This section contains a section for each Inventory Manager menu:

- [Viewer and Task Watcher Tabs, page 4-35](#)

- [File Menu, page 4-35](#)
- [Edit Menu, page 4-84](#)
- [View Menu, page 4-90](#)
- [Tasks Menu, page 4-90](#)
- [Tools Menu, page 4-97](#)
- [Logging Menu, page 4-104](#)
- [Help, page 4-105](#)

Viewer and Task Watcher Tabs

The tabs at the bottom of the main Inventory Manager GUI in [Figure 4-4](#) are used to monitor events and perform troubleshooting.

They serve the following purpose:

- Log Viewer—Displays Log messages.
- Event Viewer—Displays Inventory Manager and TIBCO events.
- Task Watcher—Can be used to monitor tasks used by Inventory Manager.

File Menu

The File menu has the following options:

- [New, page 4-35](#)
- [Open, page 4-52](#)
- [Required Attributes, page 4-62](#)
- [Save, page 4-83](#)
- [Close, page 4-83](#)
- [Exit, page 4-84](#)

New

From the Inventory Manager main menu, New is the first option under the File menu on the Task Bar. The New option has the following options:

- [New Device Group, page 4-36](#)
- [New Provider, page 4-43](#)
- [New Region, page 4-46](#)
- [New Customer, page 4-48](#)
- [New Site, page 4-49](#)
- [New Dynamic Device List \(without existing configs\), page 4-50](#)
- [New IE2100 Device List, page 4-51](#)
- [New IPsec VPN Service Module \(VPNSM\), page 4-51](#)

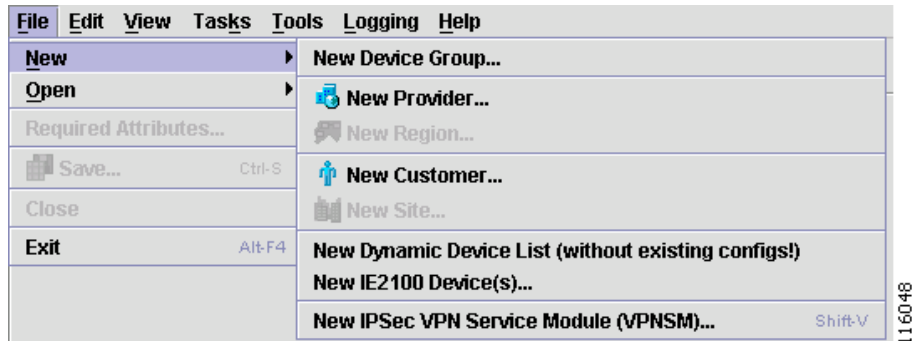
Additionally, [Open, page 4-52](#), is an option from alternate tabs.

New Device Group

To create a new Device Group, follow these steps:

- Step 1** From the Inventory Manager menu, choose **File > New > New Device Group**, as shown in [Figure 4-26](#).

Figure 4-26 Choose New Device Group



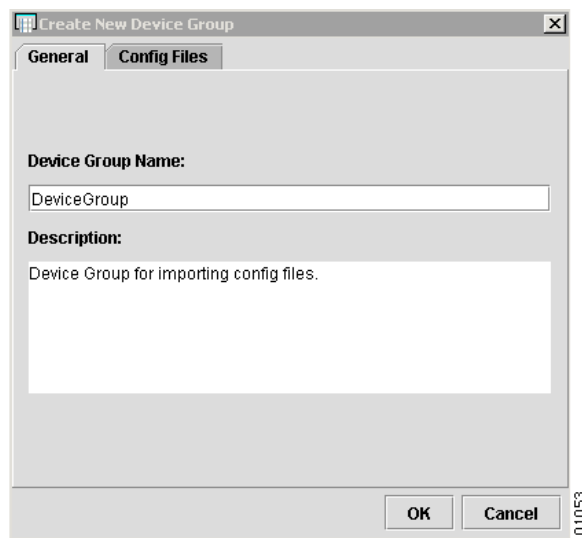
The New Device Group window appears, as shown in [Figure 4-27](#).



Note

You have the option to add configuration files to a Device Group using the New Device Group window, by choosing the Config Files tab.

Figure 4-27 Create New Device Group



- Step 2** **Device Group Name:** Enter the name of the device group.

- Step 3** **Description:** Enter a description.

- Step 4** Click the **Config Files** tab.
The **Config Files** tab appears, as shown in [Figure 4-28](#).

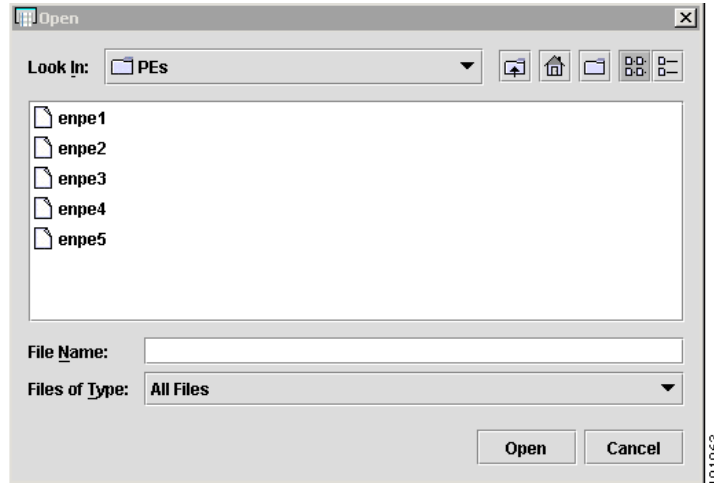
Figure 4-28 Config Files Tab



- Step 5** Click **Add** to search for your configuration files.

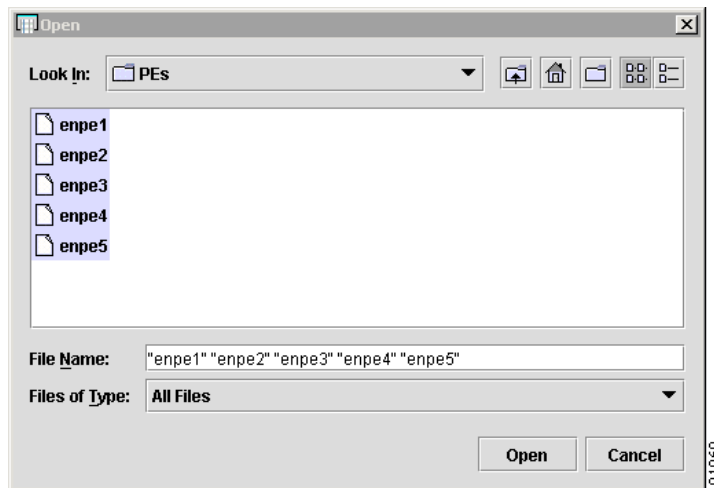
- Step 6** Navigate to your configuration file folder, select it, and click **OK**.
The Open Config Files window appears, as shown in [Figure 4-29](#).

Figure 4-29 Open Config Files

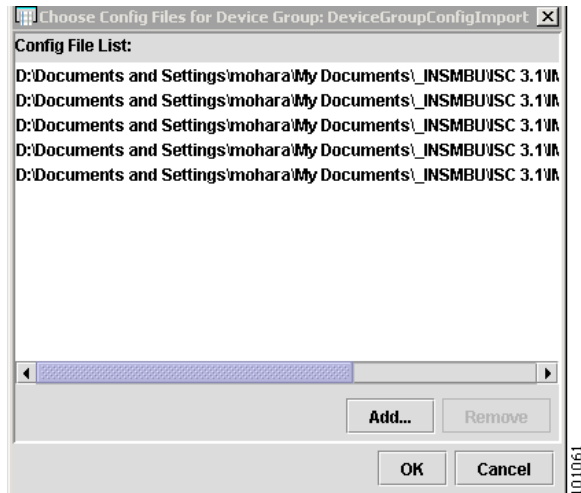


- Step 7** Use Ctrl+click to select the files.
The files appear highlighted, as shown in [Figure 4-30](#).

Figure 4-30 Highlighted Config Files



- Step 8** Click **Open**.
The Config File List appears, as shown in [Figure 4-31](#).

Figure 4-31 Config Files List

Step 9 Click **OK**.

The Device Group spreadsheet appears, as shown in [Figure 4-32](#).

Figure 4-32 Device Group Spreadsheet

File Edit View Tasks Tools Logging Help								
General Passwords SNMPv3 Attributes CNS Attributes Platform Information								
Host Name	Device Type	Device Description	Managem... Address	Domain Name	Access Protocol	Config Upload/Do...	SNMP Version	Device Groups
enpe5	Cisco Rout...				Default	Default	Default	DeviceGro...
enpe1	Cisco Rout...				Default	Default	Default	DeviceGro...
enpe2	Cisco Rout...				Default	Default	Default	DeviceGro...
enpe3	Cisco Rout...				Default	Default	Default	DeviceGro...
enpe4	Cisco Rout...				Default	Default	Default	DeviceGro...

When you create devices this way, no CPEs or PEs are created. To create CPEs or PEs, devices must be associated with a Customer, Site, Provider, or Region.

You have created a new Device Group and added the configuration files. The Spreadsheet Editor enables you to specify attributes for the devices. The following examples show how to edit or specify fields in the device workbook.

Cell Editing Examples

To enter the Domain Name, click the cell. The Domain Name dialog box appears, as shown in [Figure 4-33](#).

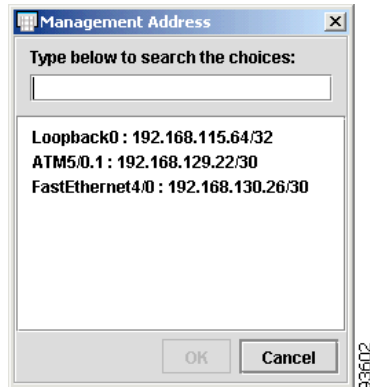
Figure 4-33 Domain Name



Enter the Domain Name and click **OK**.

To enter the Management Address, click the cell. The Management Address dialog box appears, as shown in [Figure 4-34](#).

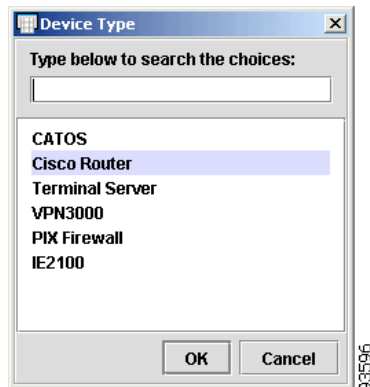
Figure 4-34 Management Address



Enter the Management Address, or select one from the list, and click **OK**.

To enter the Device Type, click the cell. The Device Type dialog box appears, as shown in [Figure 4-35](#).

Figure 4-35 Device Type



Enter the Device Type, or select one from the list, and click **OK**.

To enter the Device Description, click the cell. The Device Description dialog box appears, as shown in [Figure 4-36](#).

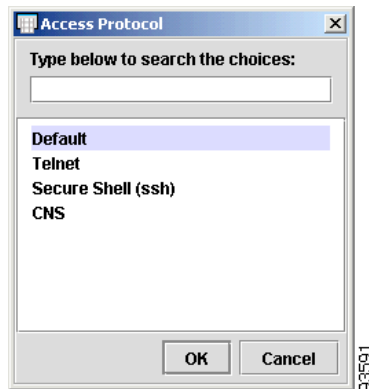
Figure 4-36 Device Description



Enter the Device Description and click **OK**.

To enter the Access Protocol, click the cell. The Access Protocol dialog box appears, as shown in [Figure 4-37](#).

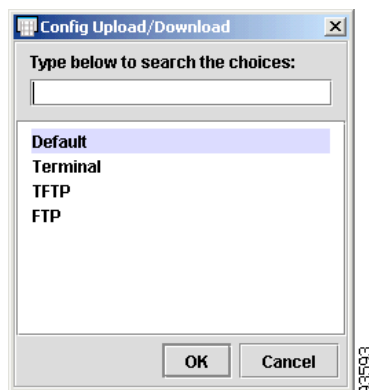
Figure 4-37 Access Protocol



Enter the Access Protocol, or select one from the list, and click **OK**.

To enter the Config Upload/Download, click the cell. The Config Upload/Download dialog box appears, as shown in [Figure 4-38](#).

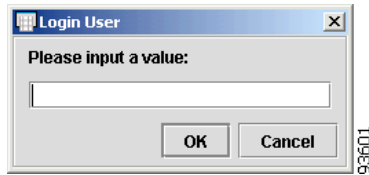
Figure 4-38 Config Upload/Download



Enter the Config Upload/Download, or select one from the list, and click **OK**.

To enter the Login User, click the cell. The Login User dialog box appears, as shown in [Figure 4-39](#).

Figure 4-39 Login User



Enter the Login User and click **OK**.

To enter the Login Password, click the cell. The Login Password dialog box appears, as shown in [Figure 4-40](#).

Figure 4-40 Login Password



Enter the Login Password in both dialog boxes and click **OK**.

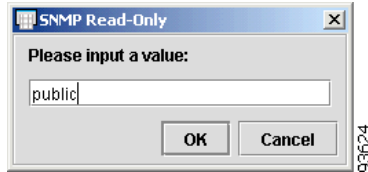
To enter the Enable Password, click the cell. The Enable Password dialog box appears, as shown in [Figure 4-41](#).

Figure 4-41 Enable Password



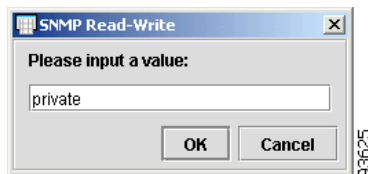
Enter the Enable Password in both dialog boxes and click **OK**.

To enter the SNMP Read-Only, click the cell. The SNMP Read-Only dialog box appears, as shown in [Figure 4-42](#).

Figure 4-42 SNMP Read-Only

Enter the SNMP Read-Only value, or select one from the list, and click **OK**.

To enter the SNMP Read-Write value, click the cell. The SNMP Read-Write dialog box appears, as shown in [Figure 4-43](#).

Figure 4-43 SNMP Read-Write

Enter the SNMP Read-Write value, or select one from the list, and click **OK**.

Step 10 To finish, choose **File > Save**.

New Provider

To create a new Provider, follow these steps:



Note

You have the option to add regions or configuration files to a Provider using the **New Provider** window, by choosing the appropriate tab. For an example of how to add regions, see the [“New Region” section on page 4-46](#).

Step 1 From the Inventory Manager menu, choose **File > New > New Provider**.

The New Provider window appears, as shown in [Figure 4-44](#).

Figure 4-44 New Provider

The screenshot shows the 'Create New Provider' dialog box with the 'General' tab selected. The dialog has three tabs: 'General', 'Regions', and 'Config Files'. The 'General' tab contains the following fields:

- Provider Name:** A text box containing 'ProviderOne'.
- BGP AS Number:** A text box containing '100'.
- Contact Information:** A text area containing 'Provider One', '888 555-1212', and 'http://www.providerone.com'.

At the bottom right of the dialog are 'OK' and 'Cancel' buttons. A small number '93607' is visible on the right side of the dialog box.

- Step 2** **Provider Name:** Enter the name of the Provider.
- Step 3** **BGP AS Number:** Enter the BGP Autonomous System Number.
- Step 4** **Contact Information:** Enter the contact information.
- Step 5** Click the **Config Files** tab.

The **Config Files** tab appears, as shown in [Figure 4-45](#).

Figure 4-45 Config Files Tab

The screenshot shows the 'Create New Provider' dialog box with the 'Config Files' tab selected. The dialog has three tabs: 'General', 'Regions', and 'Config Files'. The 'Config Files' tab contains the following elements:

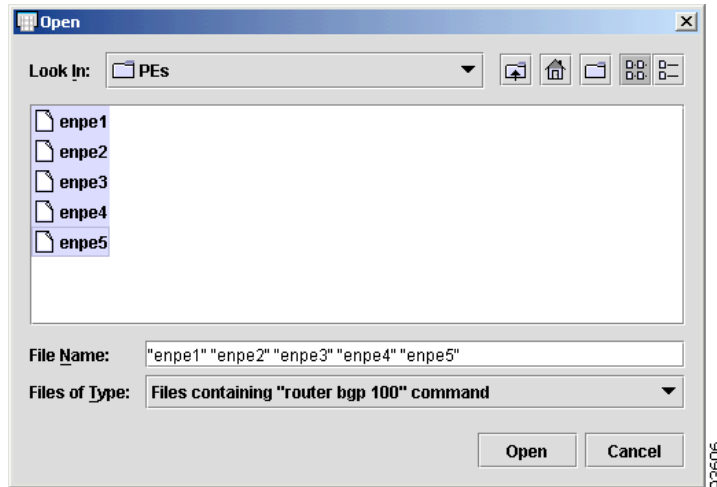
- Config File List:** A large empty text area for listing configuration files.
- Add...** and **Remove** buttons located below the list area.

At the bottom right of the dialog are 'OK' and 'Cancel' buttons. A small number '93604' is visible on the right side of the dialog box.

- Step 6** Click **Add** to search for configuration files.
- Step 7** Navigate to your configuration file folder, select it, and click **OK**.
The Open Config Files window appears.
- Step 8** Use Ctrl+click to select the files.

The files appear highlighted, as shown in [Figure 4-46](#).

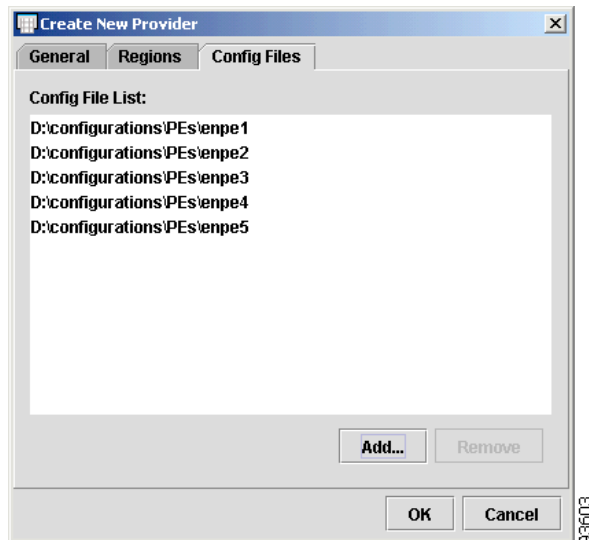
Figure 4-46 Highlighted Config Files



Step 9 Click **Open**.

The Config File List appears, as shown in [Figure 4-47](#).

Figure 4-47 Config Files List



Step 10 Click **OK**.

The New Provider spreadsheet appears, as shown in [Figure 4-48](#).

Figure 4-48 New Provider Spreadsheet

Host Name	Device Type	Device Description	Management Address	Domain Name	Access Protocol	Config Upload/Downl...	SNMP Version	Device Groups
enpe1	Cisco Router				Default	Default	Default	
enpe2	Cisco Router				Default	Default	Default	
enpe3	Cisco Router				Default	Default	Default	
enpe4	Cisco Router				Default	Default	Default	
enpe5	Cisco Router				Default	Default	Default	

You have created a new Provider and added the configuration files. The Spreadsheet Editor enables you to specify attributes for the devices. When you create devices this way, PEs are created.

To finish, choose **File > Save**.

New Region

To create a new Region, follow these steps:

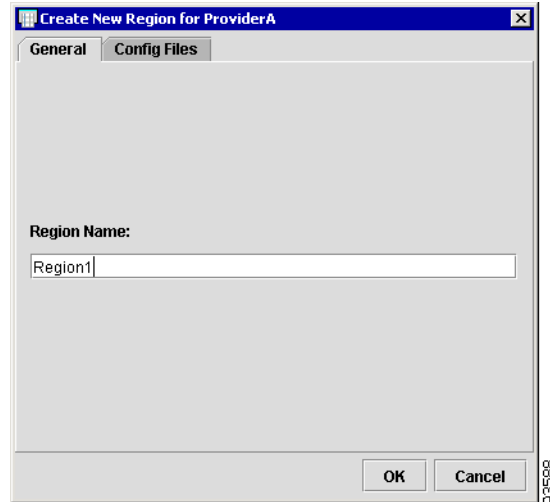


Note

You have the option to add configuration files to a New Region using the New Region for Provider window, by choosing the Config Files tab.

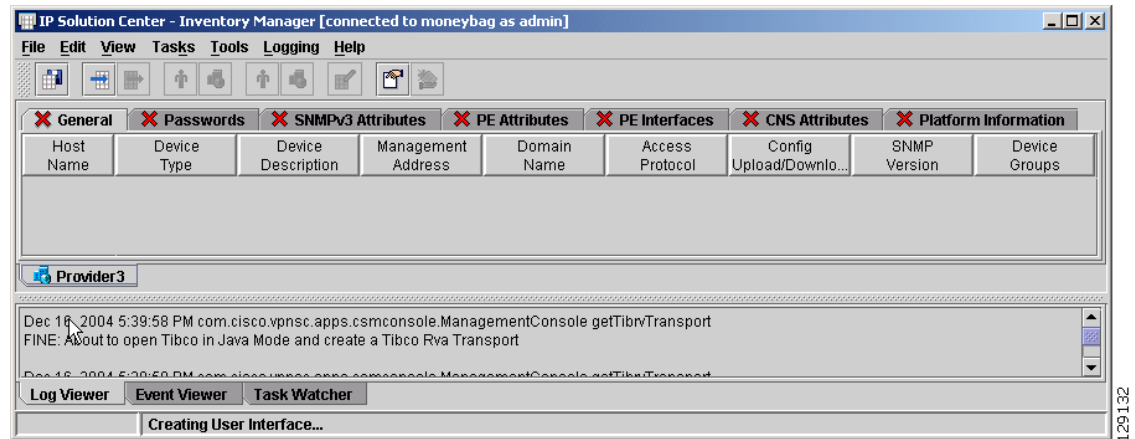
Step 1 From the Inventory Manager menu, choose **File > New > New Region**.

The New Region for Provider window appears, as shown in [Figure 4-49](#).

Figure 4-49 New Region for Provider

Step 2 Region Name: Enter the name of the Region and click **OK**.

The Inventory Manager menu appears with a spreadsheet for the Provider, as shown in [Figure 4-50](#).

Figure 4-50 New Provider Spreadsheet

For a description of the tabs and definition of the fields in the Provider, Region, and PE spreadsheets, see the [“Spreadsheet Features”](#) section on page 4-13.

New Customer

To create a new Customer, follow these steps:



Note

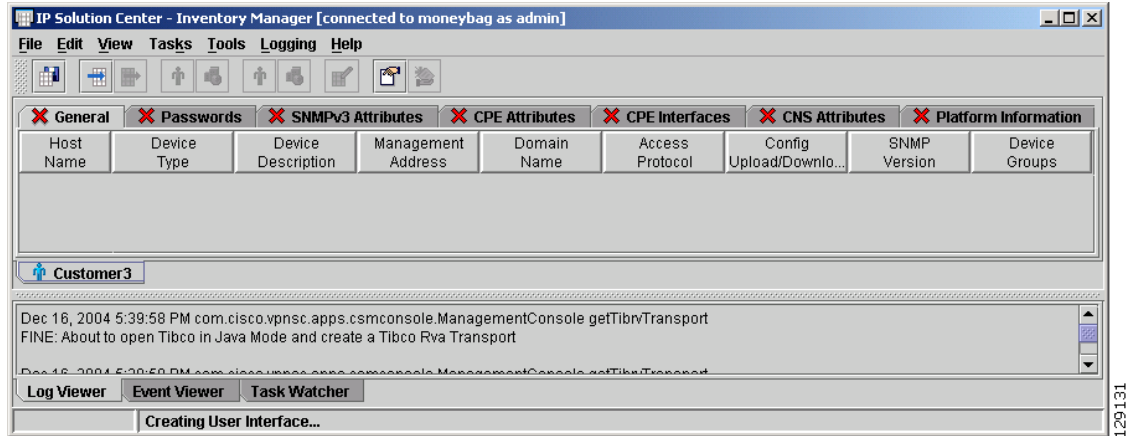
You have the option to add sites or configuration files to a Customer using the New Customer window, by choosing the appropriate tab. For an example of how to add sites, see the [“New Site” section on page 4-49](#).

- Step 1** From the Inventory Manager menu, choose **File > New > Customer**.
The New Customer window appears, as shown in [Figure 4-51](#).

Figure 4-51 New Customer

- Step 2** **Customer Name:** Enter the name of the Customer.
Step 3 **Contact Information:** Enter contact information and click **OK**.

The Inventory Manager menu appears with a spreadsheet for the Customer, as shown in [Figure 4-52](#).

Figure 4-52 New Customer Spreadsheet

You now have access to the Customer spreadsheet.

New Site

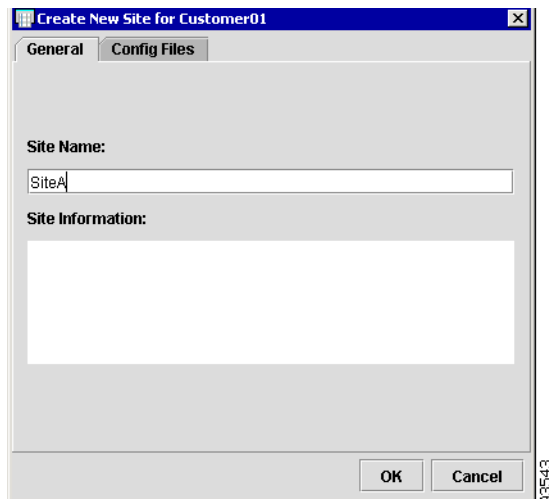
To create a new Site, follow these steps:



Note

You have the option to add configuration files to a New Site using the New Site window, by choosing the Config Files tab.

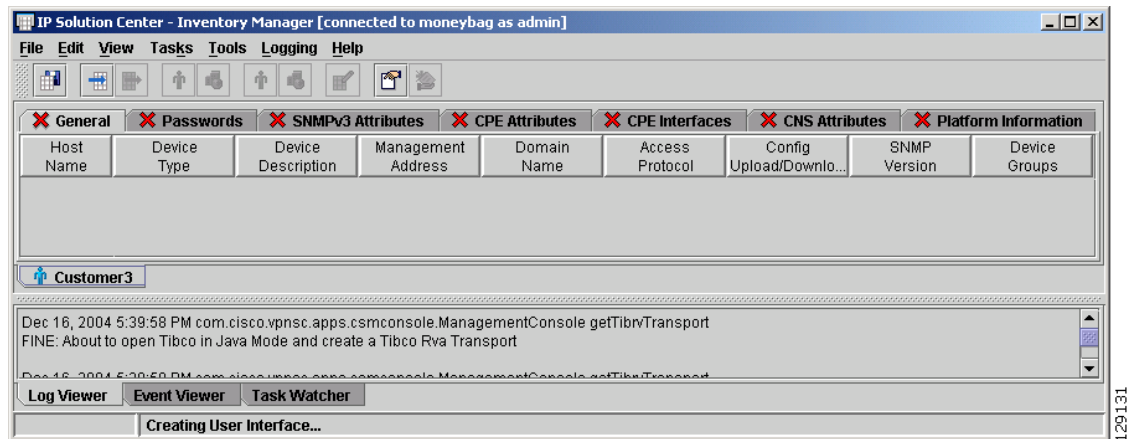
- Step 1** From the Inventory Manager menu, choose **File > New > Site**, as shown in [Figure 4-53](#).

Figure 4-53 New Site

- Step 2** **Site Name:** Enter the name of the Site.
- Step 3** **Site Information:** Enter contact information and click **OK**.

The Inventory Manager menu appears with a spreadsheet for the Customer, as shown in [Figure 4-54](#).

Figure 4-54 New Customer Spreadsheet



You now have access to the Customer spreadsheet.

New Dynamic Device List (without existing configs)

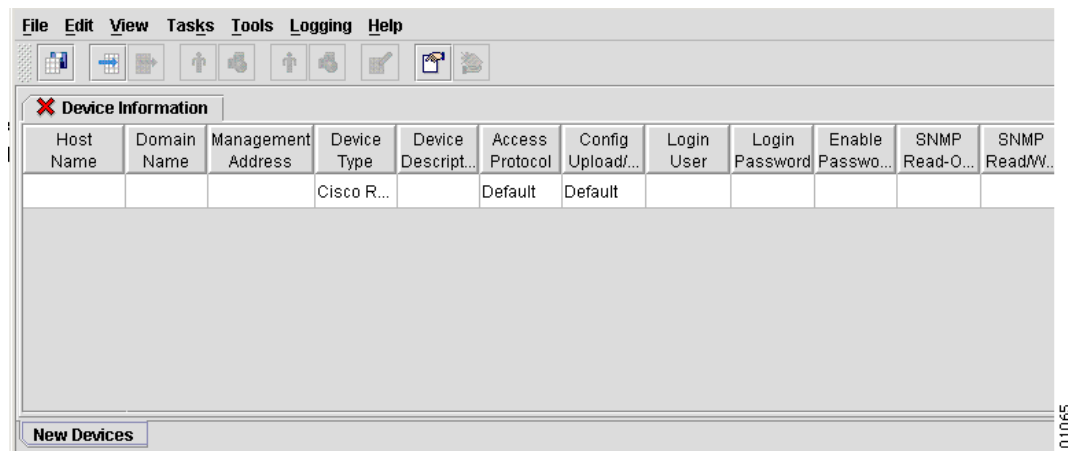
If you do not have existing configuration files, you can discover devices on your network, using the Dynamic Device List. The devices can be associated with logical CPE and PE devices at a later time.

To create a new Device List, follow these steps:

- Step 1** From the Inventory Manager menu, choose **File > New > New Dynamic Device List (without existing configs)**.

A new Device Spreadsheet appears, as shown in [Figure 4-55](#).

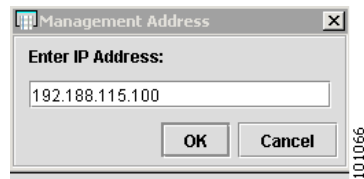
Figure 4-55 New Device Spreadsheet



- Step 2** To discover devices on your network, click the **Management Address** cell.

A Management Address window appears, as shown in [Figure 4-56](#).

Figure 4-56 Enter IP Address



Step 3 Enter the IP address and click **OK**.

A new Device Spreadsheet appears.

Step 4 Start the Device Discovery process.

For an example of how to start the device discovery process, see the [“Start Auto Discovery”](#) section on [page 4-91](#).

New IE2100 Device List

ISC supports the Cisco CNS IE2100 appliance Device Access Protocol for communication with any Cisco IOS device. Inventory Manager supports the same functionality for the Cisco CNS IE2100 appliance as the other devices described in the chapter.

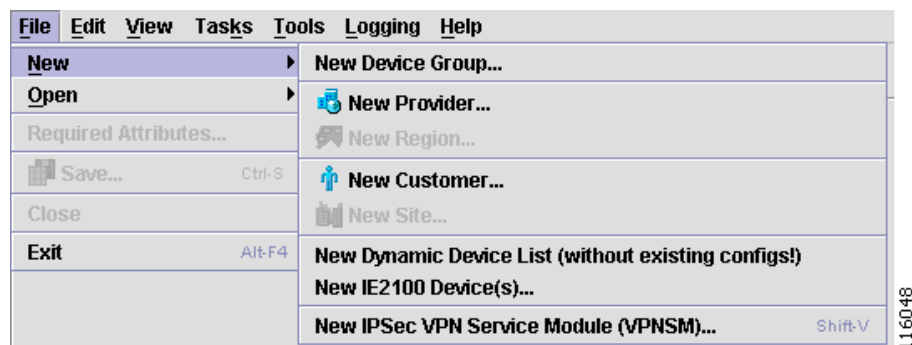
New IPsec VPN Service Module (VPNSM)

This feature is not supported in this release

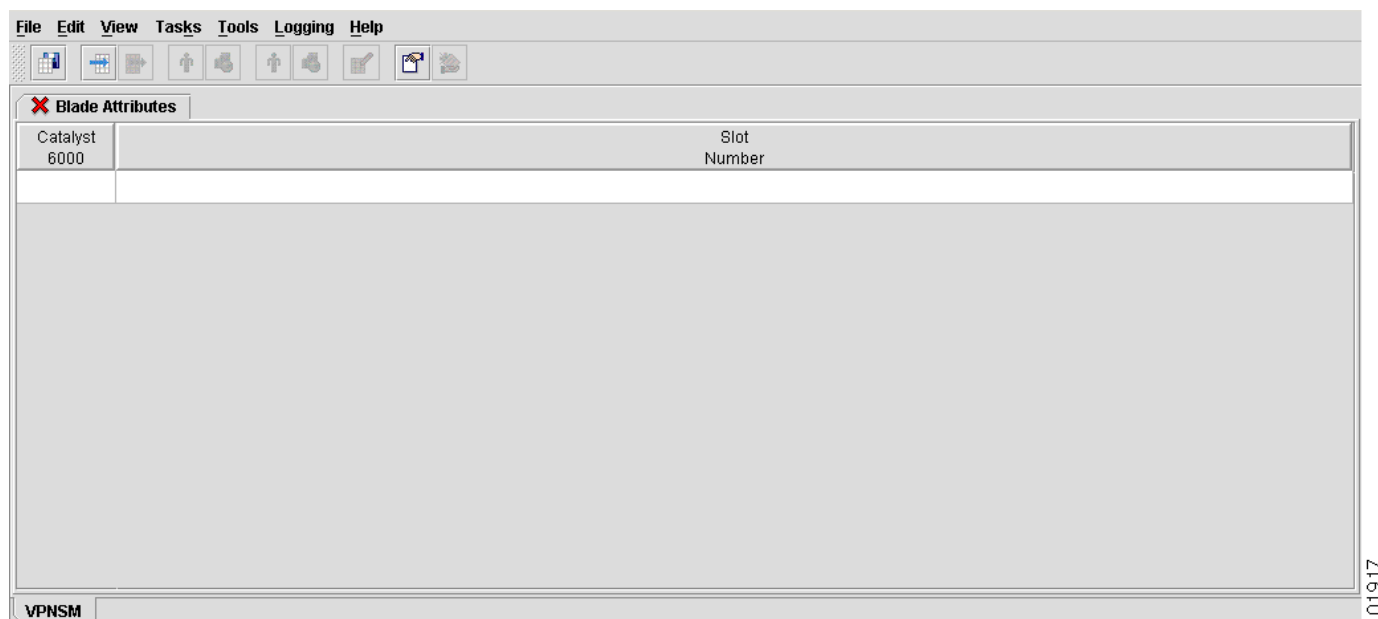
To create a new VPNSM Device, follow these steps:

Step 1 From the Inventory Manager menu, choose **File > New > New IPsec VPN Service Module (VPNSM)**, as shown in [Figure 4-57](#).

Figure 4-57 Choose New IPsec VPN Service Module



The New IPsec VPN Service Module spreadsheet appears, as shown in [Figure 4-58](#).

Figure 4-58 Create New IPsec VPN Service Module

101917

- Step 2** Click the **Catalyst 6500** cell.
The **Catalyst 6500** window appears (not shown).
- Step 3** Choose a Catalyst 6500 Device.
- Step 4** Click the **Slot Number** cell and then enter a *slot number*.
- Step 5** Choose **File > Save** to create a VPNSM in the Repository.

Open

From the Inventory Manager main menu, shown in [Figure 4-26 on page 4-36](#), Open is the second option under the File menu on the Task Bar. The Open option has the following options:

- [Open Devices, page 4-53](#)
- [Open Discovery Seed File, page 4-54](#)
- [Open Device Group, page 4-56](#)
- [Open Provider, page 4-57](#)
- [Open Region, page 4-58](#)
- [Open Customer, page 4-59](#)
- [Open Site, page 4-60](#)
- [Open IPsec VPN Service Modules, page 4-61](#)

Open Devices

This section describes how to open a Device with Inventory Manager. To open a Device, follow these steps:

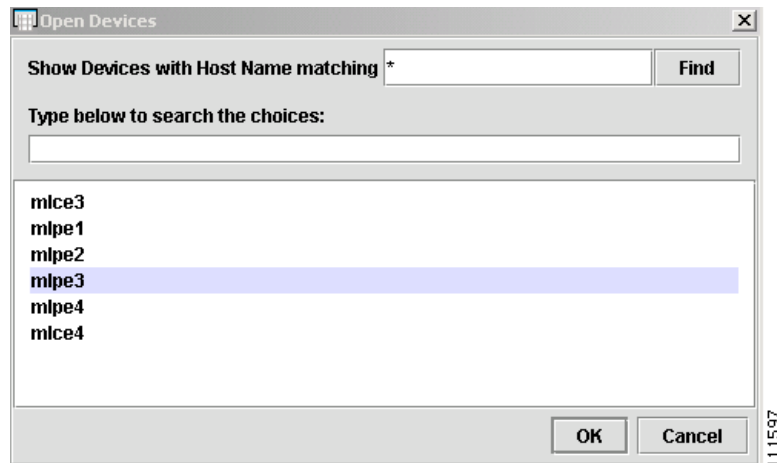
- Step 1** From the **Inventory Manager** task bar (not shown), choose **File > Open > Open Devices**. The **Open Devices** window appears, as shown in [Figure 4-59](#).

Figure 4-59 Open Devices

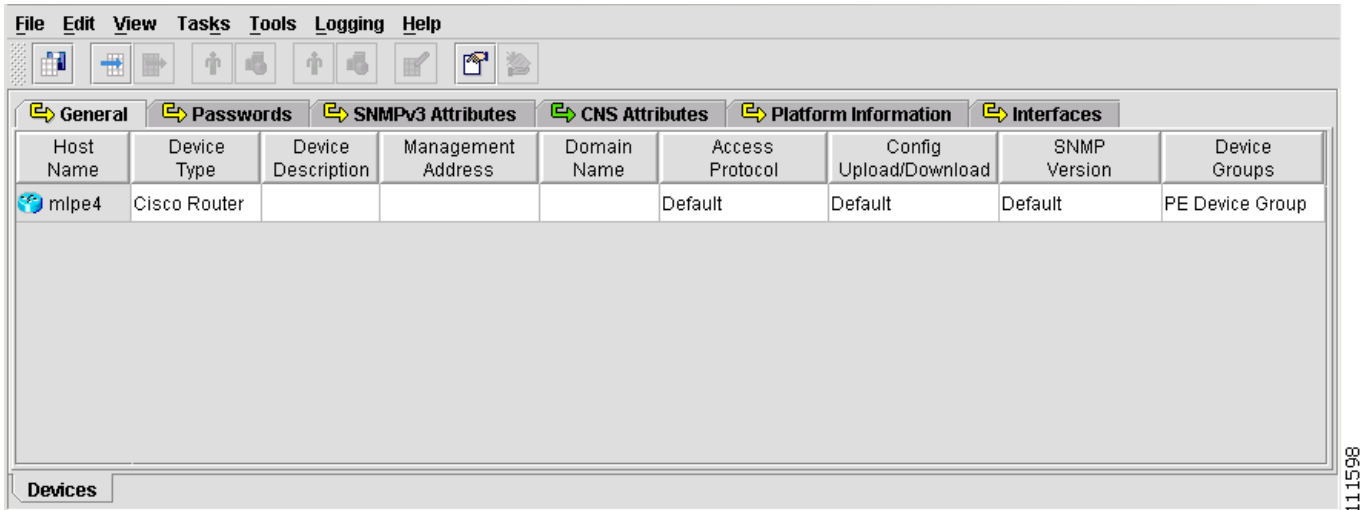


- Step 2** Click **Find**. The **Open Devices** window now displays available devices, as shown in [Figure 4-60](#).

Figure 4-60 Open Devices Found



- Step 3** Choose a Device and click **OK**. (**mlpe3**) The **Devices** spreadsheet appears, as shown in [Figure 4-61](#).

Figure 4-61 Devices Spreadsheet


Host Name	Device Type	Device Description	Management Address	Domain Name	Access Protocol	Config Upload/Download	SNMP Version	Device Groups
mlpe4	Cisco Router				Default	Default	Default	PE Device Group

111598

Open Discovery Seed File

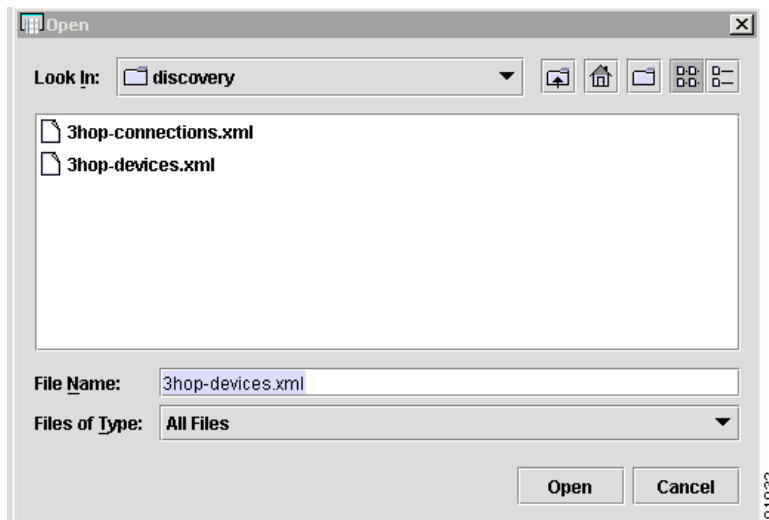


Note

A discovery seed file is an XML representation of the devices found during Auto Discovery.

To open a discovery seed file, follow these steps:

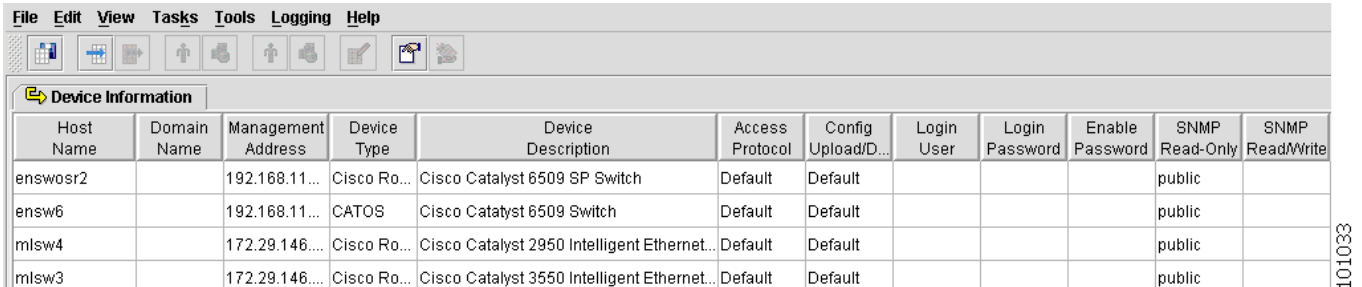
- Step 1** From the Inventory Manager menu, choose **File > Open > Open Discovery Seed File**. The Open window appears, as shown in [Figure 4-62](#).

Figure 4-62 Open Discovery Seed File

101032

- Step 2** Select the devices file, which you saved after discovering your devices, and choose **Open**.
The Device Information spreadsheet appears, as shown in [Figure 4-63](#).

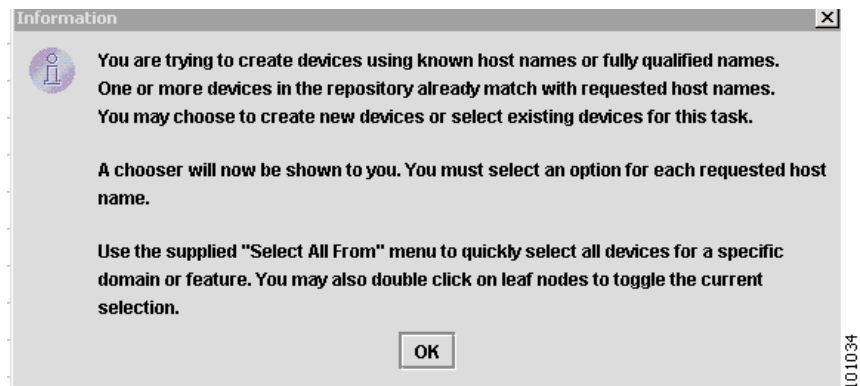
Figure 4-63 Device Information



Host Name	Domain Name	Management Address	Device Type	Device Description	Access Protocol	Config Upload/D...	Login User	Login Password	Enable Password	SNMP Read-Only	SNMP Read/Write
enswosr2		192.168.11...	Cisco Ro...	Cisco Catalyst 6509 SP Switch	Default	Default				public	
ensw6		192.168.11...	CATOS	Cisco Catalyst 6509 Switch	Default	Default				public	
mlsw4		172.29.146...	Cisco Ro...	Cisco Catalyst 2950 Intelligent Ethernet...	Default	Default				public	
mlsw3		172.29.146...	Cisco Ro...	Cisco Catalyst 3550 Intelligent Ethernet...	Default	Default				public	

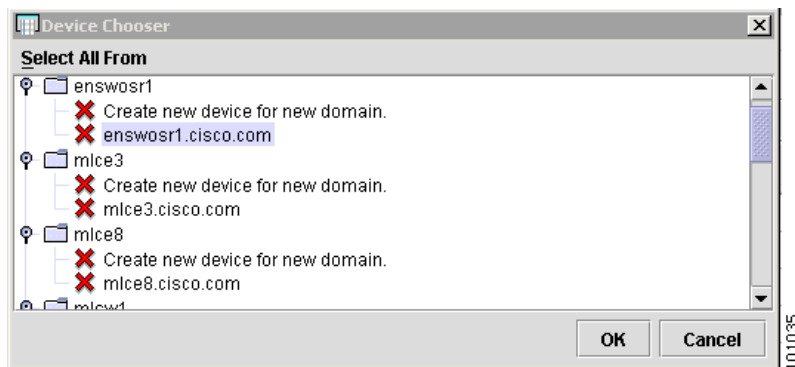
If a device has already been created in the Repository, a message window appears, as shown in [Figure 4-64](#).

Figure 4-64 Device in the Repository



- Step 3** Click **OK** and the Device Chooser window appears, as shown in [Figure 4-65](#).

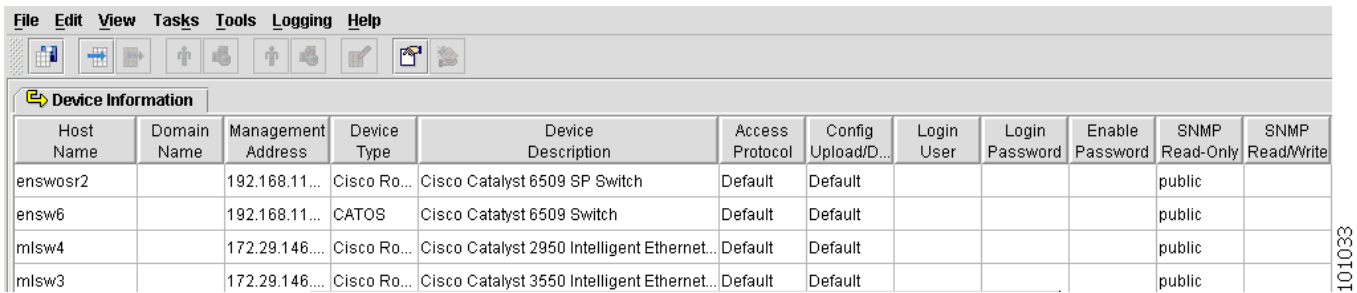
Figure 4-65 Device Chooser



- Step 4** Click the device name and domain to save the device as is. To create a new domain for the device and save it, click **Create new device for new domain**.

The Device Information spreadsheet appears, as shown in [Figure 4-66](#).

Figure 4-66 Device Information



Host Name	Domain Name	Management Address	Device Type	Device Description	Access Protocol	Config Upload/D...	Login User	Login Password	Enable Password	SNMP Read-Only	SNMP Read/Write
enswosr2		192.168.11...	Cisco Ro...	Cisco Catalyst 6509 SP Switch	Default	Default				public	
ensw6		192.168.11...	CATOS	Cisco Catatyst 6509 Switch	Default	Default				public	
mls4		172.29.146...	Cisco Ro...	Cisco Catalyst 2950 Intelligent Ethernet...	Default	Default				public	
mls3		172.29.146...	Cisco Ro...	Cisco Catalyst 3550 Intelligent Ethernet...	Default	Default				public	

Now you can edit your devices and collect the latest configuration files.

Open Device Group

To open an existing Device Group, follow these steps:

- Step 1** From the Inventory Manager menu, choose **File > Open > Open Device Group**.

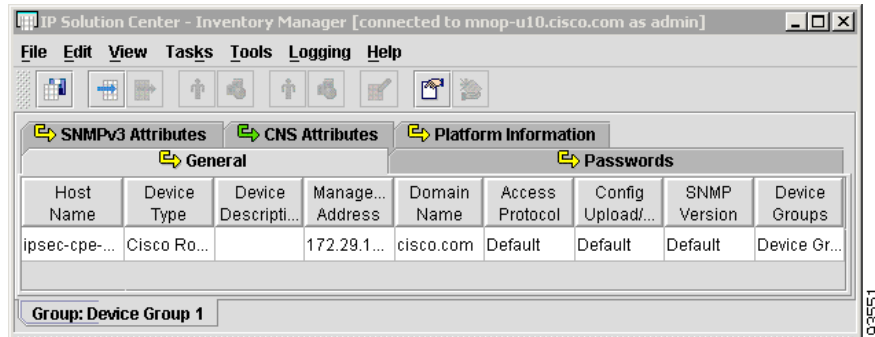
A search dialog appears, as shown in [Figure 4-67](#).

Figure 4-67 Open Device Group



- Step 2** Click the **Find** button to download all Device Groups, enter the name to search for the one you want, or enter a partial name with an asterisk to get a list of available device names.
- Step 3** Select the Device Group and click **OK**.

A Device Spreadsheet Editor appears, where you can edit device parameters such as passwords and SNMP information, as shown in [Figure 4-68](#).

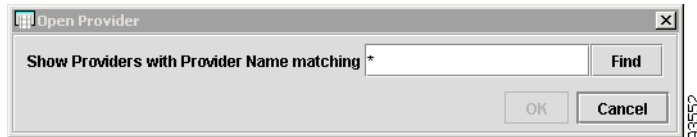
Figure 4-68 Device Spreadsheet Editor

You now have access to the Device spreadsheet.

Open Provider

To open an existing Provider, follow these steps:

- Step 1** From the Inventory Manager menu, choose **File > Open > Open Provider**.
A search dialog appears, as shown in [Figure 4-69](#).

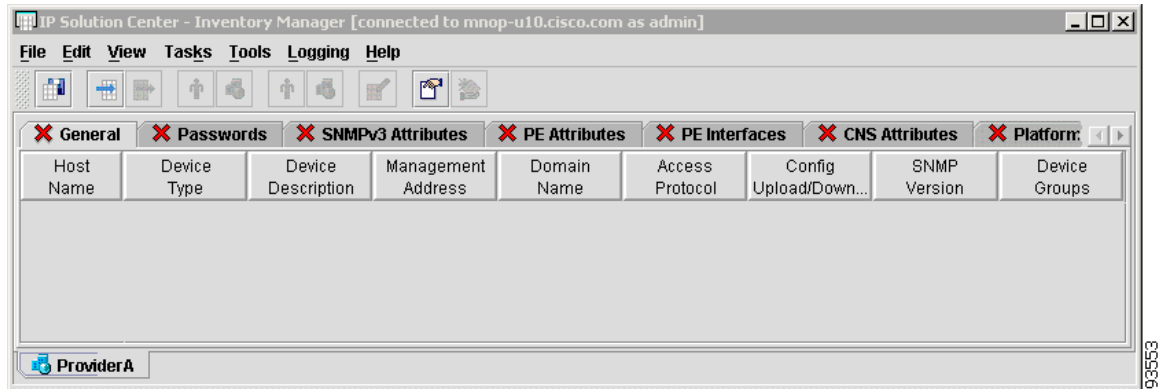
Figure 4-69 Open Provider

- Step 2** Click the **Find** button to download all Providers, enter the name to search for the one you want, or enter a partial name with an asterisk to get a list of available Providers.
- Step 3** Select the Provider and choose **OK**.
A PE Spreadsheet Editor appears with all Regions and PEs for that Provider listed in the Spreadsheet Editor, as shown in [Figure 4-70](#).



Note

In the following example, the Spreadsheet Editor is empty.

Figure 4-70 Provider Spreadsheet Editor

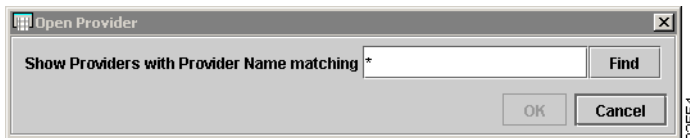
You now have access to the Provider spreadsheet.

Open Region

To open an existing Region, follow these steps:

- Step 1** From the Inventory Manager menu, choose **File > Open > Open Region**.

A search dialog appears, as shown in [Figure 4-71](#).

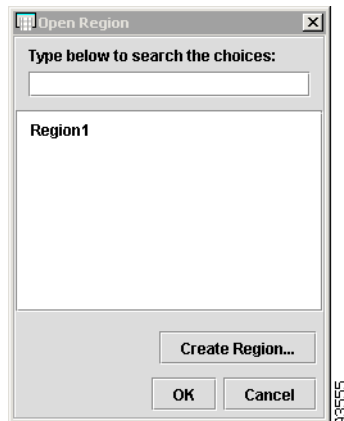
Figure 4-71 Open Provider

- Step 2** Click the **Find** button to download all Providers, enter the name of the provider to search for the one you want, or enter a partial name with an asterisk to get a list of available Providers.

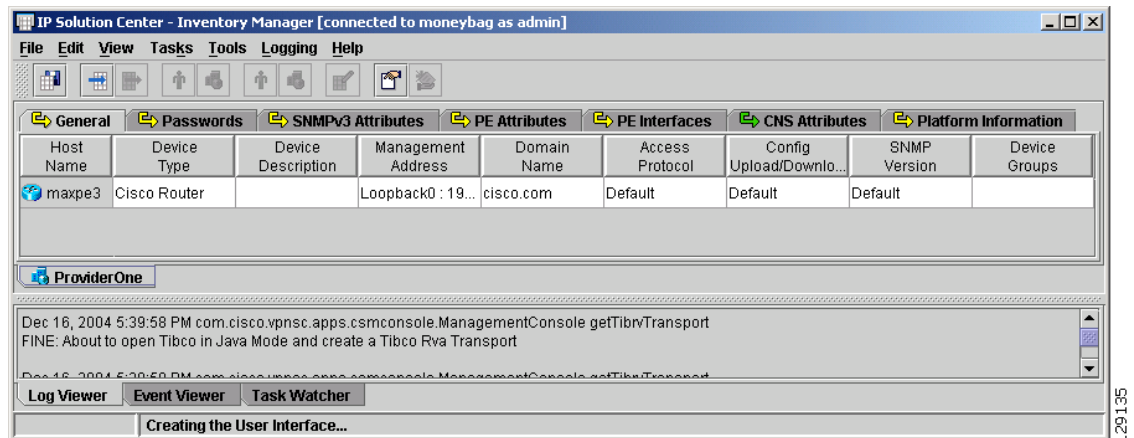
- Step 3** Select the Provider and choose **OK**.

- Step 4** Choose from the list of existing Regions, as shown in [Figure 4-72](#).

You can also create a Region for the Provider by choosing **Create Region**.

Figure 4-72 Open Region

A PE Spreadsheet Editor appears with all PEs for the Region listed in the Spreadsheet Editor, as shown in [Figure 4-73](#).

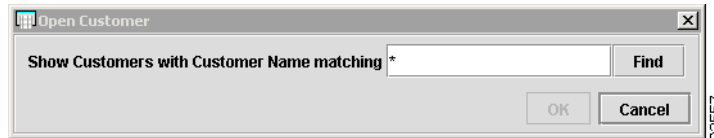
Figure 4-73 PE Spreadsheet Editor

You now have access to the Provider spreadsheet.

Open Customer

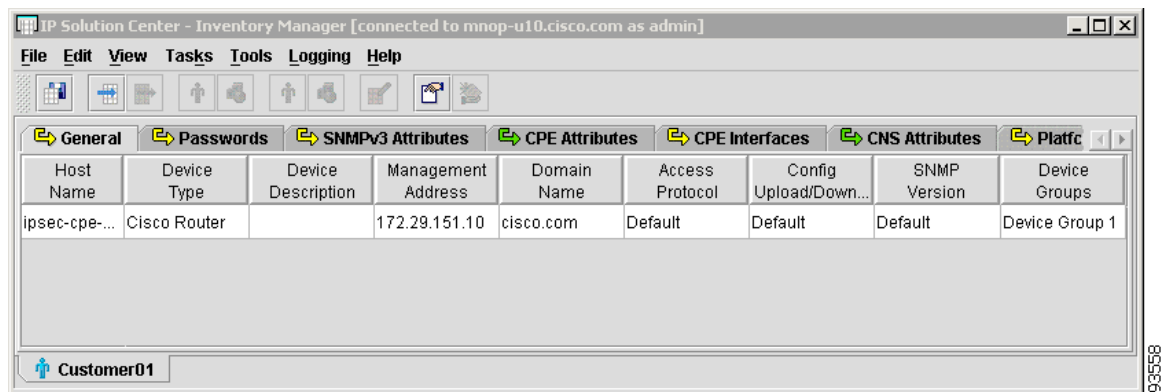
To open an existing Customer, follow these steps:

- Step 1** From the Inventory Manager menu, choose **File > Open > Open Customer**.
A search dialog appears, as shown in [Figure 4-74](#).

Figure 4-74 Open Customer

- Step 2** Click the **Find** button to download all Customers, enter the name of the Customer to search for the one you want, or enter a partial name with an asterisk to get a list of available Customers.
- Step 3** Select the Customer and choose **OK**.

A CPE Spreadsheet Editor appears with all Sites and CPE for the Customer listed in the Spreadsheet Editor, as shown in [Figure 4-75](#).

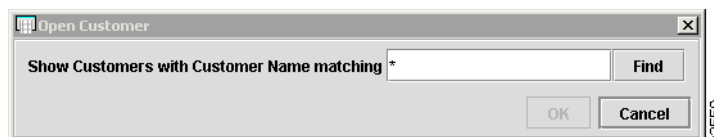
Figure 4-75 CPE Spreadsheet Editor

You now have access to the Customer spreadsheet.

Open Site

To open an existing Site, follow these steps:

- Step 1** From the Inventory Manager menu, choose **File > Open > Open Site**.
A search dialog appears, as shown in [Figure 4-76](#).

Figure 4-76 Open Customer

- Step 2** Click the **Find** button to download all Customers, enter the name to search for the one you want, or enter a partial name with an asterisk to get a list of available Customers. You must specify a Customer first.
- Step 3** Select the Customer and choose **OK**.

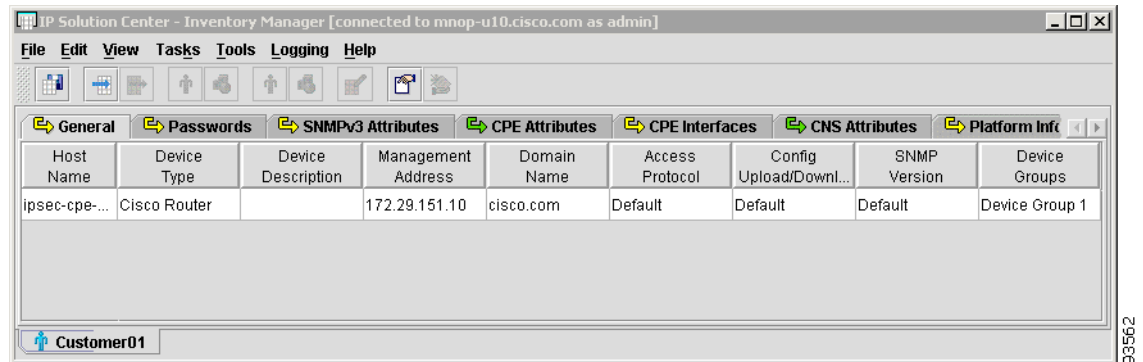
Choose from the list of existing Sites, as shown in [Figure 4-77](#). You can also create a Site for the Customer by choosing **Create Site**.

Figure 4-77 Open Site



A CPE Spreadsheet Editor appears with all the CPEs for that Site listed in the Spreadsheet Editor, as shown in [Figure 4-78](#).

Figure 4-78 CPE Spreadsheet Editor



You now have access to the Customer spreadsheet.

Open IPsec VPN Service Modules

This feature is not supported in this release

To open an existing VPNSM, follow these steps:

- Step 1** From the Inventory Manager menu, choose **File > Open > Open IPsec VPN Service Modules**. Open Device Blades window appears (not shown).

- Step 2** Choose a Device Blade.
- Step 3** Choose **File > Save** to save your changes to the VPNSM in the Repository.
-

Required Attributes

From the Inventory Manager main menu, shown in [Figure 4-26 on page 4-36](#), Required Attributes is the third option under the File menu on the Task Bar. To specify required attributes, you must open a Spreadsheet Editor for one of the following options:

- Discovery Seed File (No example is provided)
- Device Groups
- Providers
- Regions
- PEs
- Customers
- Sites
- CEs

The Spreadsheet Editors work the same for each inventory group. They default to the General tab and display a list of attributes. Some attributes in each Spreadsheet Editor are required and others are not. You can make some of the non-system required attributes required by clicking a checkbox for that attribute.

If an attribute is required, the spreadsheet tab will have a red X indicating that more information is required by the system for all later processing to proceed without errors. For example, errors can occur when processing service requests or creating a VPN. When all required information is filled out, the red X changes to either a yellow or green Continue Image. When you see a red X on a tab, it means you need to fill out more information for the tab.

From the Required Attributes option, you can specify required attributes for the following inventory groups:

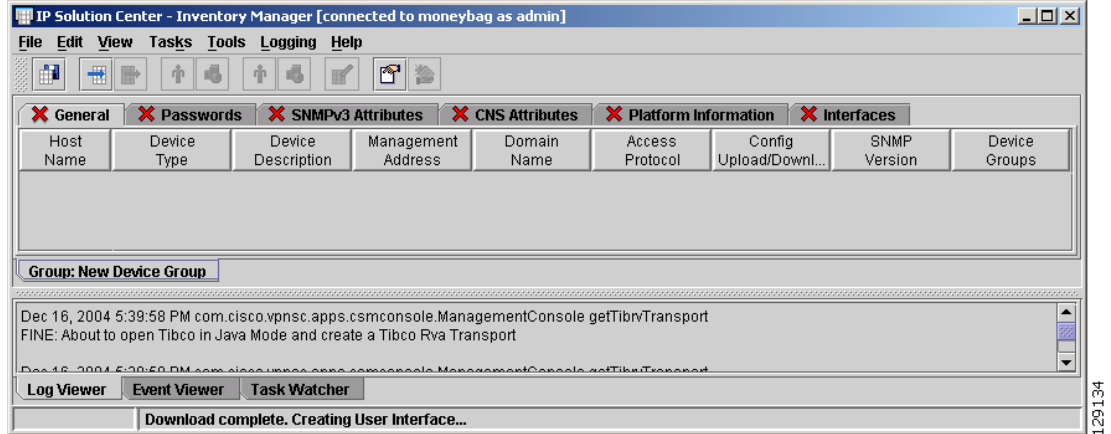
- [Device Groups, page 4-62](#)
- [Providers, Regions, and PE, page 4-68](#)
- [Customers, Sites, and CE, page 4-76](#)

Device Groups

To specify required attributes for a Device Group, follow these steps:

-
- Step 1** From the Inventory Manager menu, choose **File > Open > Open Device Group**.
A search dialog appears.
- Step 2** Select the Device Group and a Spreadsheet Editor appears, as shown in [Figure 4-79](#).

Figure 4-79 Open Device Group

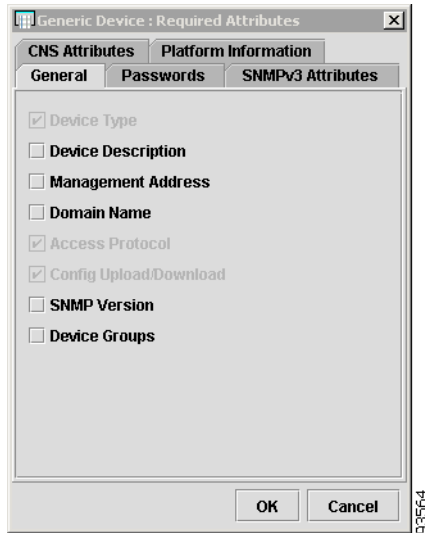


Step 3 Choose **File > Required Attributes**.

The **General** tab on the Required Attributes window for a Device Group appears, as shown in [Figure 4-80](#).

Step 4 To set an attribute to **Required**, click the appropriate checkbox. A blank box signifies **Optional**.

Figure 4-80 Generic Device - General Attributes



The General tab contains the following attributes:

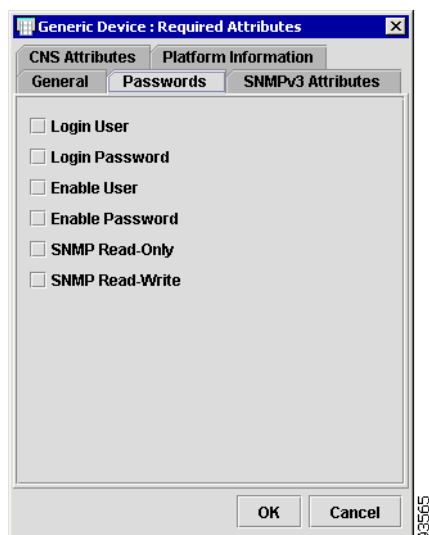
- **Device Name**
- **Device Description**
- **Management Address**
- **Domain Name**
- **Access Protocol**
- **Config Upload/Download**
- **SNMP Version**
- **Device Groups**

Step 5 To modify attributes for passwords, choose the **Passwords** tab.

The Passwords tab on the Required Attributes window appears, as shown in [Figure 4-81](#).

Step 6 To set an attribute to **Required**, click the appropriate checkbox. A blank box signifies **Optional**.

Figure 4-81 Generic Device - Password Attributes



The Passwords tab contains the following attributes:

- **Login User**
- **Login Password**
- **Enable User**
- **Enable Password**
- **SNMP Read-Only**
- **SNMP Read-Write**

Step 7 To modify attributes for SNMPv3, choose the **SNMPv3 Attributes** tab.

The SNMPv3 tab on the Required Attributes window appears, as shown in [Figure 4-82](#).

Step 8 To set an attribute to **Required**, click the appropriate checkbox. A blank box signifies **Optional**.

Figure 4-82 Generic Device - SNMPv3 Attributes



The SNMPv3 Attributes tab contains the following attributes:

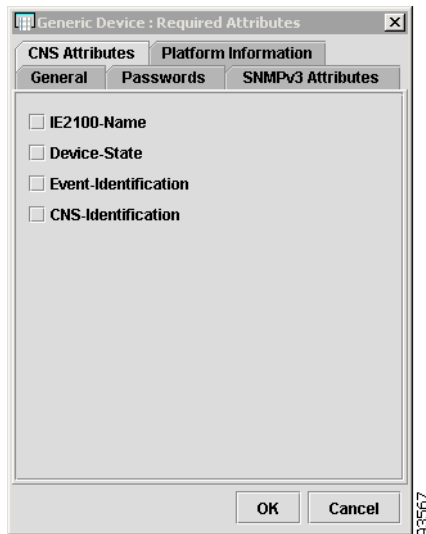
- **Security Level**
- **Authentication User**
- **Authentication Password**
- **Authentication Algorithm**
- **Encryption Password**
- **Encryption Algorithm**

Step 9 To modify attributes for CNS, choose the **CNS Attributes** tab.

The CNS tab on the Required Attributes window appears, as shown in [Figure 4-83](#).

Step 10 To set an attribute to **Required**, click the appropriate checkbox. A blank box signifies **Optional**.

Figure 4-83 Generic Device - CNS Attributes



The CNS Attributes tab contains the following attributes:

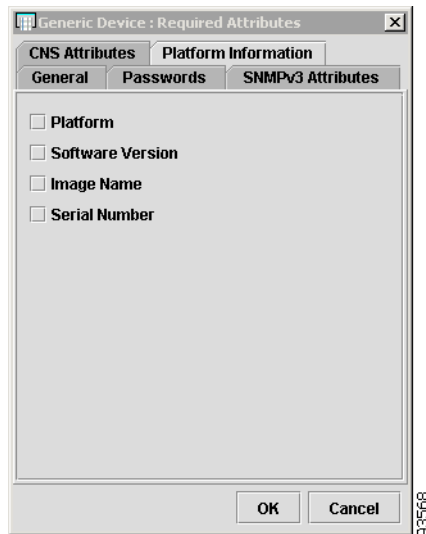
- **IE2100-Name**
- **Device-State**
- **Event-Identification**
- **CNS-Identification**

Step 11 To modify attributes for Platform Information, choose the **Platform Information** tab.

The Platform Information tab on the Required Attributes window appears, as shown in [Figure 4-84](#).

Step 12 To set an attribute to **Required**, click the appropriate checkbox. A blank box signifies **Optional**.

Figure 4-84 Generic Device - Platform Information Attributes



The Platform Information tab contains the following attributes:

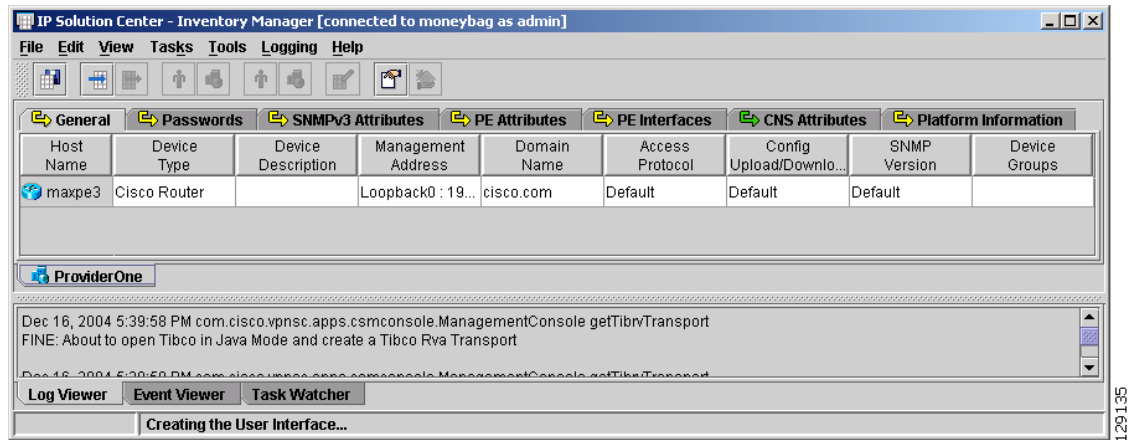
- **Platform**
- **Software Version**
- **Image Name**
- **Serial Number**

Providers, Regions, and PE

To specify required attributes for a Provider, follow these steps:

- Step 1** From the Inventory Manager menu, choose **File > Open > Open Provider**.
A search dialog appears.
- Step 2** Select the Provider and a Spreadsheet Editor appears, as shown in [Figure 4-85](#).

Figure 4-85 Open Provider

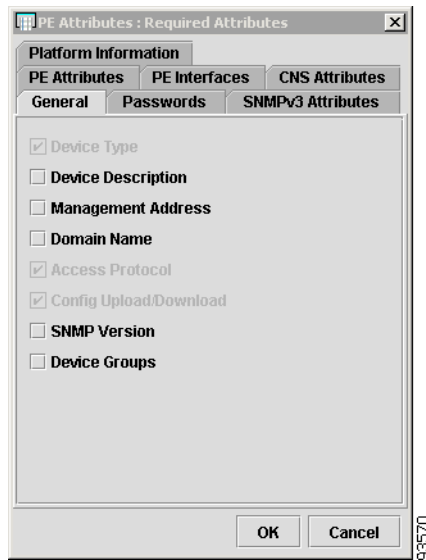


- Step 3** Choose **File > Required Attributes**.

The General tab on the Required Attributes window for the provider appears, as shown in [Figure 4-86](#).

Step 4 To set an attribute to **Required**, click the appropriate checkbox. A blank box signifies **Optional**.

Figure 4-86 PE Device - General Attributes



The General tab contains the following attributes:

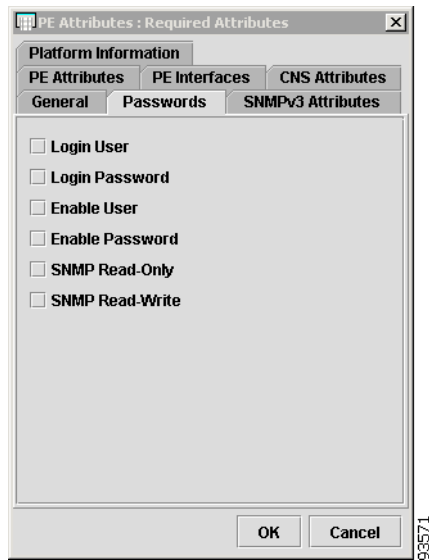
- **Device Name**
- **Device Description**
- **Management Address**
- **Domain Name**
- **Access Protocol**
- **Config Upload/Download**
- **SNMP Version**
- **Device Groups**

Step 5 To modify attributes for passwords, choose the **Passwords** tab.

The Passwords tab on the Required Attributes window appears, as shown in [Figure 4-87](#).

Step 6 To set an attribute to **Required**, click the appropriate checkbox. A blank box signifies **Optional**.

Figure 4-87 PE Device - Password Attributes



The Passwords tab contains the following attributes:

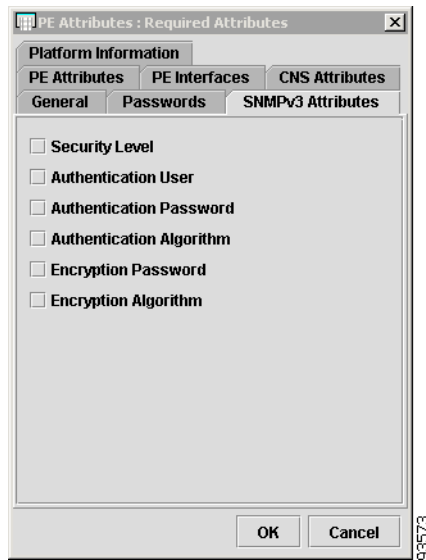
- **Login User**
- **Login Password**
- **Enable User**
- **Enable Password**
- **SNMP Read-Only**
- **SNMP Read-Write**

Step 7 To modify attributes for SNMP attributes, choose the **SNMPv3 Attributes** tab.

The SNMPv3 Attributes tab on the Required Attributes window appears, as shown in [Figure 4-88](#).

Step 8 To set an attribute to **Required**, click the appropriate checkbox. A blank box signifies **Optional**.

Figure 4-88 PE Device - SNMPv3 Attributes



The SNMPv3 Attributes contains the following attributes:

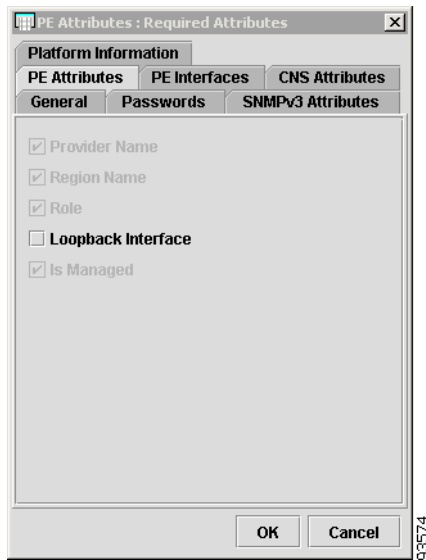
- **Security Level**
- **Authentication User**
- **Authentication Password**
- **Authentication Algorithm**
- **Encryption Password**
- **Encryption Algorithm**

Step 9 To modify attributes for PE attributes, choose the **PE Attributes** tab.

The PE Attributes tab on the Required Attributes window appears, as shown in [Figure 4-89](#).

Step 10 To set an attribute to **Required**, click the appropriate checkbox. A blank box signifies **Optional**.

Figure 4-89 PE Device - PE Attributes



The PE Attributes tab contains the following attributes:

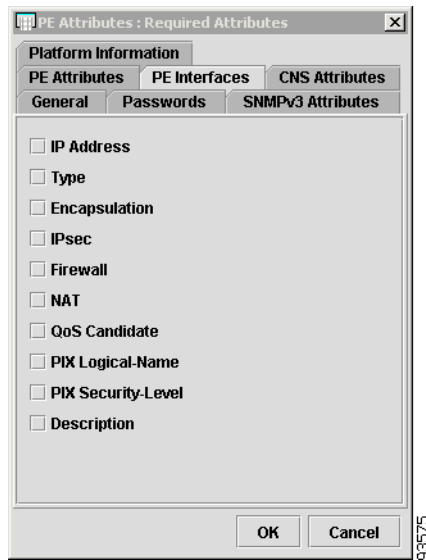
- **Provider Name**
- **Region Name**
- **Role**
- **Loopback Interface**
- **IS Managed**

Step 11 To modify attributes for PE interfaces, choose the **PE Interfaces** tab.

The PE Interfaces tab on the Required Attributes window appears, as shown in [Figure 4-90](#).

Step 12 To set an attribute to **Required**, click the appropriate checkbox. A blank box signifies **Optional**.

Figure 4-90 PE Device - PE Interfaces



The PE Interfaces tab contains the following attributes:

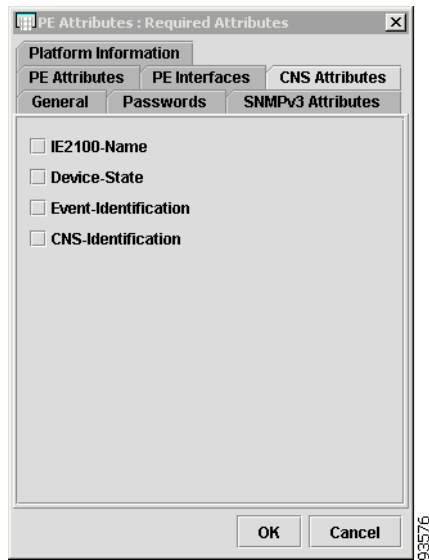
- IP Address
- Type
- Encapsulation
- IPsec (This feature is not supported in this release)
- Firewall (This feature is not supported in this release)
- NAT (This feature is not supported in this release)
- QoS Candidate
- PIX Logical Name
- PIX Security-Level
- Description

Step 13 To modify attributes for CNS attributes, choose the **CNS Attributes** tab.

The CNS Attributes tab on the Required Attributes window appears, as shown in [Figure 4-91](#).

Step 14 To set an attribute to **Required**, click the appropriate checkbox. A blank box signifies **Optional**.

Figure 4-91 PE Device - CNS Attributes



The CNS Attributes tab contains the following attributes:

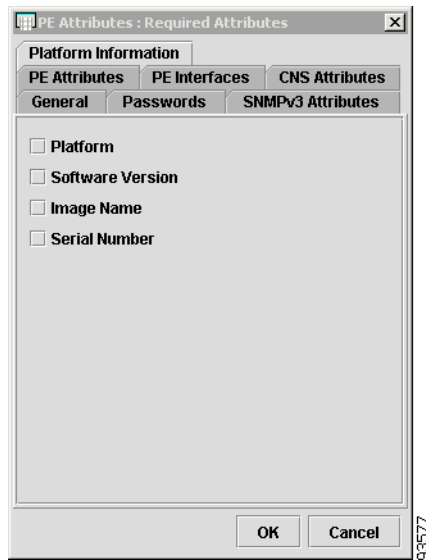
- **IE2100-Name**
- **Device-State**
- **Event-Identification**
- **CNS-Identification**

Step 15 To modify attributes for Platform Information, choose the **Platform Information** tab.

The Platform Information tab on the Required Attributes window appears, as shown in [Figure 4-92](#).

Step 16 To set an attribute to **Required**, click the appropriate checkbox. A blank box signifies **Optional**.

Figure 4-92 PE Device - Platform Information



The Platform Information tab contains the following attributes:

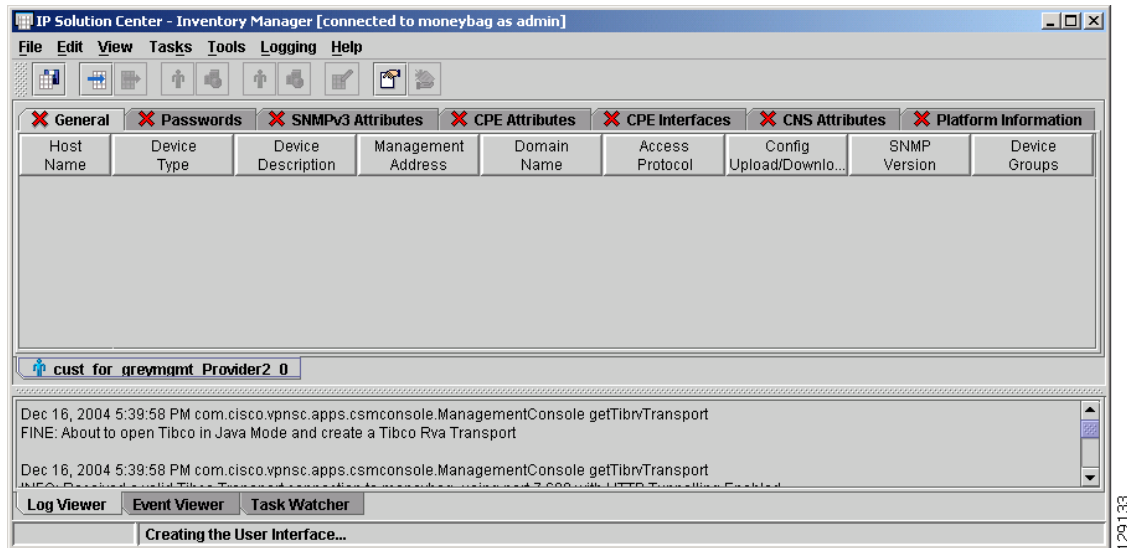
- **Platform**
- **Software Version**
- **Image Name**
- **Serial Number**

Customers, Sites, and CE

To specify required attributes for a Customer, follow these steps:

- Step 1** From the Inventory Manager menu, choose **File > Open > Open Customer**.
A search dialog appears.
- Step 2** Select the Customer and a Spreadsheet Editor appears, as shown in [Figure 4-93](#).

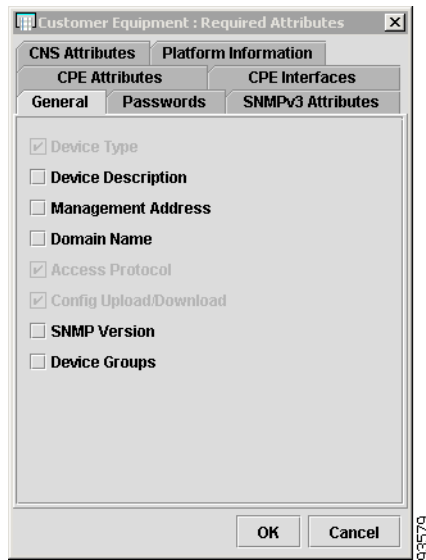
Figure 4-93 Open Customer



- Step 3** Choose **File > Required Attributes**.
The General tab on the Required Attributes window appears, as shown in [Figure 4-94](#).

Step 4 To set an attribute to **Required**, click the appropriate checkbox. A blank box signifies **Optional**.

Figure 4-94 CPE Device - General Attributes



The General tab contains the following attributes:

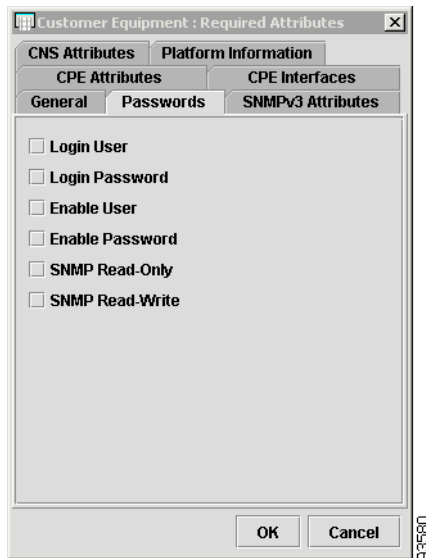
- **Device Name**
- **Device Description**
- **Management Address**
- **Domain Name**
- **Access Protocol**
- **Config Upload/Download**
- **SNMP Version**
- **Device Groups**

Step 5 To modify attributes for passwords, choose the **Passwords** tab.

The Passwords tab on the Required Attributes window appears, as shown in [Figure 4-95](#).

Step 6 To set an attribute to **Required**, click the appropriate checkbox. A blank box signifies **Optional**.

Figure 4-95 CPE Device - Password Attributes



The Passwords tab contains the following attributes:

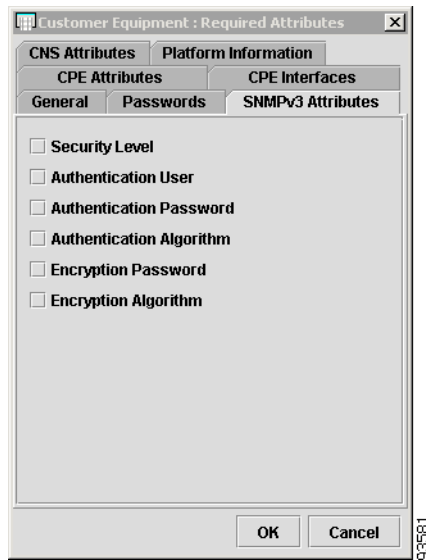
- **Login User**
- **Login Password**
- **Enable User**
- **Enable Password**
- **SNMP Read-Only**
- **SNMP Read-Write**

Step 7 To modify attributes for SNMPv3, choose the **SNMPv3 Attributes** tab.

The SNMPv3 Attributes tab on the Required Attributes window appears, as shown in [Figure 4-96](#).

Step 8 To set an attribute to **Required**, click the appropriate checkbox. A blank box signifies **Optional**.

Figure 4-96 CPE Device - SNMPv3 Attributes



The SNMPv3 Attributes contains the following attributes:

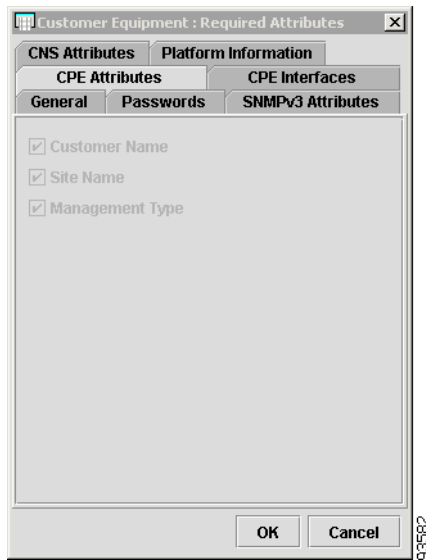
- **Security Level**
- **Authentication User**
- **Authentication Password**
- **Authentication Algorithm**
- **Encryption Password**
- **Encryption Algorithm**

Step 9 To modify attributes for CPE, choose the **CPE Attributes** tab.

The CPE Attributes tab on the Required Attributes window appears, as shown in [Figure 4-97](#).

Step 10 To set an attribute to **Required**, click the appropriate checkbox. A blank box signifies **Optional**.

Figure 4-97 CPE Device - CPE Attributes



The CPE Attributes tab contains the following attributes:

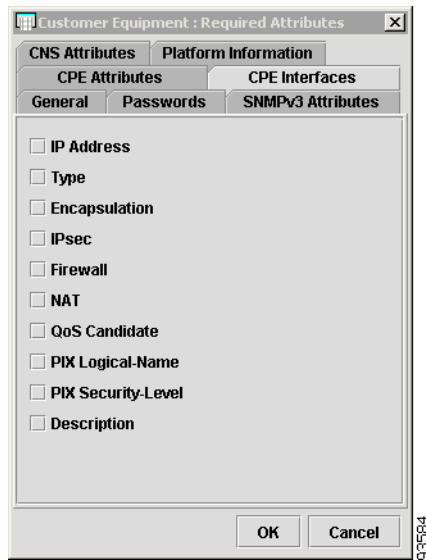
- **Customer Name**
- **Site Name**
- **Management Type**

Step 11 To modify attributes for CPE interfaces, choose the **CPE Interfaces** tab.

The CPE Interfaces tab on the Required Attributes window appears, as shown in [Figure 4-98](#).

Step 12 To set an attribute to **Required**, click the appropriate checkbox. A blank box signifies **Optional**.

Figure 4-98 CPE Device - CPE Interfaces



The CPE Interfaces tab contains the following attributes:

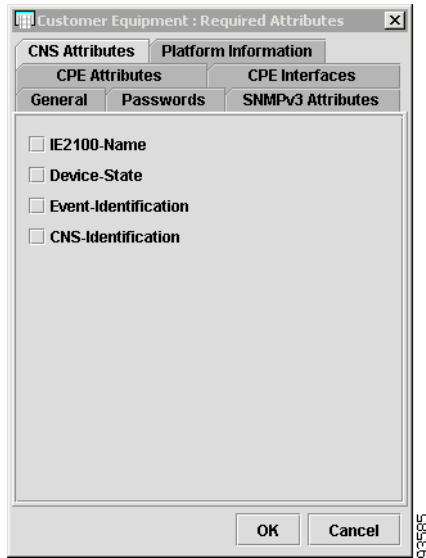
- **IP Address**
- **Type**
- **Encapsulation**
- **IPsec (This feature is not supported in this release)**
- **Firewall (This feature is not supported in this release)**
- **NAT (This feature is not supported in this release)**
- **QoS Candidate**
- **PIX Logical-Name**
- **PIX Security-Level**
- **Description**

Step 13 To modify attributes for CNS, choose the **CNS Attributes** tab.

The CNS Attributes tab on the Required Attributes window appears, as shown in [Figure 4-99](#).

Step 14 To set an attribute to **Required**, click the appropriate checkbox. A blank box signifies **Optional**.

Figure 4-99 CPE Device - CNS Attributes



The CNS Attributes tab contains the following attributes:

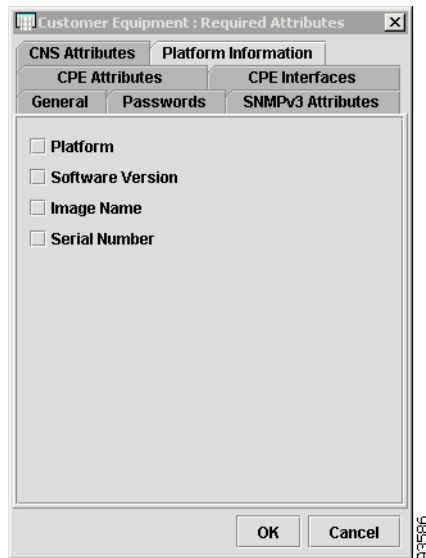
- **IE2100-Name**
- **Device-State**
- **Event-Identification**
- **CNS-Identification**

Step 15 To modify attributes for Platform Information, choose the **Platform Information** tab.

The Platform Information tab on the Required Attributes window appears, as shown in [Figure 4-100](#).

Step 16 To set an attribute to **Required**, click the appropriate checkbox. A blank box signifies **Optional**.

Figure 4-100 CPE Device - Platform Information Attributes



The Platform Information tab contains the following attributes:

- **Platform**
- **Software Version**
- **Image Name**
- **Serial Number**

Save

From the Inventory Manager main menu, shown in [Figure 4-26 on page 4-36](#), Save is the fourth option under the File menu on the Task Bar.

This option saves your work.

Close

From the Inventory Manager main menu, shown in [Figure 4-26 on page 4-36](#), Close is the fifth option under the File menu on the Task Bar.

This option name changes depending on which Spreadsheet Editor you choose. For example, if you are editing a Customer named CustomerA, the menu would show File Close CustomerA.

If there are changes to be saved, the system prompts you to save, and then the Spreadsheet Editor closes. You have an opportunity to cancel the operation if saving is required.

Exit

From the Inventory Manager main menu, shown in [Figure 4-26 on page 4-36](#), Exit is the sixth option under the File menu on the Task Bar.

This option shuts down the Inventory Manager. If there are changes to be made, the system prompts you to save changes before exiting.

Edit Menu

From the Inventory Manager main menu, shown in [Figure 4-25 on page 4-34](#), Edit is the second menu on the Task Bar. The Edit menu has the following options:

- [Insert More Devices, page 4-84](#)
- [Remove Selected Devices, page 4-85](#)
- [Move to New Customer, page 4-85](#)
- [Move to New Provider, page 4-85](#)
- [Move to Customer, page 4-86](#)
- [Move to Provider, page 4-86](#)
- [Edit Selected Devices, page 4-87](#)
- [Edit Default Attributes, page 4-88](#)
- [Load Default Values to Selected Cells, page 4-89](#)
- [Apply Interface Marking Rules to Selection, page 4-89](#)
- [Select All, page 4-89](#)

Insert More Devices

When editing a Device Group, Provider, or Customer, choosing this option causes a File Open Dialog to appear, where you can select more configuration files to be inserted. A new row is created for each new configuration file that is added:

- If you are editing a Provider or a Region, a physical device and a logical PE are created in the Repository.
- If you are editing a Customer or a Site, a physical device and a logical CPE are created in the Repository.
- If you are editing a Device Group, only a physical device is created and you *must* associate it with a PE or CPE using the **Edit > Move To** menu options.
- If you are editing in a Dynamic Device List spreadsheet, choosing this option adds one more empty row into the spreadsheet for editing.

To insert more devices in a Spreadsheet Editor, choose **Edit > Insert More Devices** from the Inventory Manager Task Bar.

Remove Selected Devices

When editing a Device Group, Provider, or Customer, choosing this option allows selected rows to be removed from the spreadsheet.

To delete rows in a Spreadsheet Editor, choose **Remove Selected Devices** from the Inventory Manager Task Bar.

Use the Host Name Column to select rows of device information. A confirmation dialog appears. If you choose **Yes**, the selected rows are removed from the Spreadsheet Editor.

**Note**

These objects are not removed from the Repository.

Move to New Customer

This option is enabled only when you create devices using the Open Discovery Seed File or New Dynamic Device List options. You must select rows using the Host Name Column or the Select All option. The selected rows in the spreadsheet are moved to a new tab for a Customer in a CPE Spreadsheet Editor.

To create a new Customer and move the selected rows to a new CPE Spreadsheet Editor, follow these steps:

- Step 1** Select the desired rows using the host name column of a device spreadsheet.
- Step 2** From the Inventory Manager Task Bar, choose **Edit > Move to New Customer** to create a new Customer and move the selected rows to a new CPE Spreadsheet Editor.
- Step 3** A dialog box prompts you to enter the new Customer information such as Name and Contact information.
- Step 4** Click OK and the selected rows are removed from the current spreadsheet and moved into a new Customer CPE spreadsheet. In the process, each moved physical device is associated with a new CPE logical device in the Repository.
- Step 5** Proceed to edit the CPE as you would for any Customer, by associating it with new Site objects. If the originating spreadsheet is empty after the operation, it automatically closes.

Move to New Provider

This option is enabled only when you create devices using the Open Discovery Seed File or New Dynamic Device List options. You must select rows using the Host Name Column or the Select All option. The selected rows in the spreadsheet are moved to a new tab for a Provider in a PE Spreadsheet Editor.

To create a new Provider and move the selected rows to a new PE Spreadsheet Editor, follow these steps:

-
- Step 1** Select the desired rows using the host name column of a device spreadsheet.
 - Step 2** From the Inventory Manager Task Bar, choose **Edit > Move to New Provider** to create a new Provider and move the selected rows to a new PE Spreadsheet Editor.
 - Step 3** A dialog box prompts you to enter the new Provider information such as Name, BGP AS number, and Contact information.
 - Step 4** Click OK and the selected rows are removed from the current spreadsheet and moved into a new Customer PE spreadsheet. In the process, each moved physical device is associated with a new PE logical device in the Repository.
 - Step 5** Proceed to edit the PE as you would for any Provider, by associating it with new Region objects. If the originating spreadsheet is empty after the operation, it automatically closes.
-

Move to Customer

This option is enabled only when you create devices using the Open Discovery Seed File or New Dynamic Device List. You must use the Host Name Column or the Select All options to select rows. The selected rows in the spreadsheet are moved to a new tab for the customer in a CPE Spreadsheet Editor.

To select rows in a table, open an existing customer, and move the rows to a new CPE Spreadsheet Editor, and follow these steps:

-
- Step 1** Select the desired rows using the host name column.
 - Step 2** From the Inventory Manager Task Bar, choose **Edit > Move to Customer**.
A dialog box appears asking you to enter the existing Customer name.
 - Step 3** Click the Find button and a list of customers appears.
 - Step 4** Choose a customer.
If you click OK, the selected rows are removed from the current spreadsheet into an existing customer CPE spreadsheet.



Note

In the process, each moved physical device is associated with a new CPE logical device in the Repository.

Edit the CPEs as you would for any customer by associating them with new or existing Region objects. If the originating spreadsheet is empty after the operation, it automatically closes.

Move to Provider

This option is enabled only when you create devices using the Open Discovery Seed File or New Dynamic Device List. You must use the Host Name Column or the Select All options to select rows. The selected rows in the spreadsheet are moved to a new tab for the Provider in a PE Spreadsheet Editor.

To select rows in a table, open an existing provider, and move the rows to a new PE Spreadsheet Editor, and follow these steps:

-
- Step 1** Select the desired rows using the host name column.
- Step 2** From the Inventory Manager Task Bar, choose **Edit > Move to Provider**.
A dialog box appears asking you to enter the existing Provider name.
- Step 3** Click the Find button and a list of providers appears.
- Step 4** Choose a provider.
If you click OK, the selected rows are removed from the current spreadsheet into an existing Provider PE spreadsheet.
-  **Note** In the process, each moved physical device is associated with a new PE logical device in the Repository.
-
- Step 5** Edit the PEs as you would for any provider by associating them with new or existing Region objects. If the originating spreadsheet is empty after the operation, it automatically closes.
-

Edit Selected Devices

To edit selected devices from rows in a spreadsheet, follow these steps:

-
- Step 1** Choose **Edit > Edit Selected Devices** from the Inventory Manager Task Bar.
A Multi-Attribute Cell Editor appears where you can set a value that is applied to all selected cells for each respective column in the selection.
- Step 2** Click the Multi-Attribute Editor cell to set the value.
- Step 3** To edit an individual cell in a column, click the cell.
A column-specific editor appears.
- Step 4** Use the column-specific editor to specify a value for the cell.
A new dialog appears showing a table with one row. Each column containing selected cells in the originating spreadsheet is represented in the dialog.
- Step 5** Click each cell in the new dialog and a column specific editor appears allowing you to enter a value or select from a list of existing values.
- Step 6** When you are finished filling in the one row spreadsheet, click OK and the values are applied to each selected cell in the original spreadsheet respectively.
- Step 7** To edit a single value in a cell, click the cell.
You are prompted with a search dialog to specify the value. The type of search dialog depends on the column you are editing. For example, if you edit a username you are prompted with a single input editor. If you are editing a password column, you get a password editor.
-

To edit multiple attributes at one time, select the cells using the following standard techniques for multiple selections:

- Select a single cell that represents the upper boundary. Press the Shift Key and select the lower boundary of the selection.
- Click and drag to and from a boundary.
- To toggle your selection, press the Ctrl Key and click on a cell.
- To select entire rows, use the Host Name Column as your main point of selection.

Edit Default Attributes

Each spreadsheet editor (Device Group, CPE, PE, and Dynamic Device List) has the ability to store separate default attributes. Defaults for passwords and other parameters for PEs can be different from those of CPEs.

For example, all PEs in a provider network can share the same passwords, SNMP attributes, and so on. Using Inventory Manager, you can store default attributes for most of the attributes in each spreadsheet. These default attributes can then be applied to selected cells using the **Edit > Load Default Attributes to Selected Cells** menu.

To edit default attributes, follow these steps:

-
Step 1	Choose Edit > Edit Default Attributes from the Inventory Manager Task Bar. A new dialog appears containing a table with one row.
Step 2	To specify the default attribute for a particular column, click it and specify the value in the column-specific editor.
Step 3	When you are finished editing the desired defaults, click the OK button and the default attributes are stored.
-

Each specific Spreadsheet Editor has its own unique set of columns. Each editor allows the specification for default values to be stored and retrieved at a later time. It is the standard spreadsheet format, and to specify the values you must click on each cell. These values are automatically saved between sessions and are stored per user on the client machine running the Inventory Manager.

When specifying default values for the Management Address or PE Loopback Interface columns, you may enter more than one interface name.

For example, **Loopback0;FastEthernet0;Ethernet0**, where the separator between names must be a semicolon. When attempting to set the Management Interface using the default supplied for any given device, the interfaces stored on the device must be checked against the value provided. If the value provided is Loopback0 and the interface does not exist on the device, it can not be set. The interface must actually exist on the device before Inventory Manager allows it as a valid value.

In the example of **Loopback0;FastEthernet0;Ethernet0**, Inventory Manager uses a left to right precedence rule. For each selected device it first checks to see whether Loopback0 exists. If it is found on the device, it is used as the correct value, otherwise it looks for FastEthernet0 and continues down the list until it finds an acceptable result. If no interfaces on the device match the request string, the value remains unchanged.

Load Default Values to Selected Cells

To load default values to selected cells, follow these steps:

-
- Step 1** From the Inventory Manager Task Bar, choose **Edit > Edit Default Attributes**.
 - Step 2** Select the desired cells in the spreadsheet.
 - Step 3** Choose **Edit > Load Default Attributes to Selected Cells** option.
 - Step 4** Specify the default attributes for desired columns.
 - Step 5** Modify the selected cell values with the default attribute, if possible.
 - Step 6** Select the cells you want to edit.
 - Step 7** Choose **Edit > Load Default Values to Selected Cells**.

The values that you stored using the Edit > Edit Default Attributes menu are applied to each selected cell.

For example, if all the devices you are editing belong to the same provider and share the same passwords, you can specify the default password and apply it to the entire spreadsheet without having to remember it.

Apply Interface Marking Rules to Selection

This option is only enabled when you are editing CPE and PE devices in a spreadsheet. To apply the rules, select the desired cells in the spreadsheet and, from the Inventory Manager Task Bar, choose **Tools > Apply Interface Marking Rules to Selection**.

A Rule chooser dialog appears. Select one or more rules to apply on interfaces.

If you select one or more devices, the rules are applied to each interface on the selected devices.

If you select one or more interfaces in the Interface tab, the rules are only applied to the selected interfaces.

For each interface encountered, marking will only occur if the interface and/or parent device properties meet those specified in the rule.

Before you apply interface marking rules to selected devices, you must first create a set of rules for your organization. For an example of how to create interface marking rules, see the [“New Rule” section on page 4-98](#).

Select All

From the Inventory Manager Task Bar, choose **Edit > Select All** to use this option.

This option selects all the cells in a spreadsheet, except the host name column. Typically, the host name column is not editable and does not participate in typical edit operations.

If you want to select all rows in the spreadsheet, first click on the Host Name column and press the Ctrl+A accelerator key. This operation selects all the cells in a Spreadsheet Editor that are currently open.

View Menu

From the Inventory Manager Task Bar, shown in [Figure 4-25 on page 4-34](#), View is the third menu on the Task Bar. The View menu has the following options:

- [Fit Columns in Window, page 4-90](#)
- [Show Color Coded Column Headers, page 4-90](#)

Fit Columns in Window

From the Inventory Manager Task Bar, choose **View > Fit Columns in Window** to expand or contract the cells in the Spreadsheet Editor to fit the window.

Show Color Coded Column Headers

From the Inventory Manager Task Bar, choose **View > Show Color Coded Column Headers** to show the colors of the column headers.

If you choose **View > Show Color Coded Column Headers**, you could see three colors:

- Red—some required data is missing in this column.
- Yellow—all required data is in this column, but not all optional data.
- Green—all data is provided.

Tasks Menu

From the Inventory Manager Task Bar, shown in [Figure 4-25 on page 4-34](#), Tasks is the fourth menu on the Task Bar. The Task menu has the following options:

- [Collect Latest Configuration Files, page 4-90](#)
- [Start Auto Discovery, page 4-91](#)
- [Start NPC Auto Discovery, page 4-95](#)
- [Start Service Discovery, page 4-96](#)

Collect Latest Configuration Files

This option is applied to selected rows in a spreadsheet, if rows are selected. If no rows are selected, all devices contained in the spreadsheet are visited and their configurations are downloaded to the ISC server. It is important for the login and enable passwords to be specified correctly, together with the management address, for each device to be reached and files to be successfully collected.

A persistent task is created on the Master server and Inventory Manager waits for the collection process to complete. When the task completes, you are notified of success or failure. You can use the Web GUI to view the task logs on the Master server to see why a task has failed. If successful, you are prompted to refresh from the Repository. This is recommended, because it is possible that the configuration has changed since the last time the configuration was retrieved.

From the Inventory Manager Task Bar, choose **Tasks > Collect Latest Configuration Files** to collect the latest configuration files.

Start Auto Discovery



Note

This option is designed to work in conjunction with the **New Dynamic Device List** option.

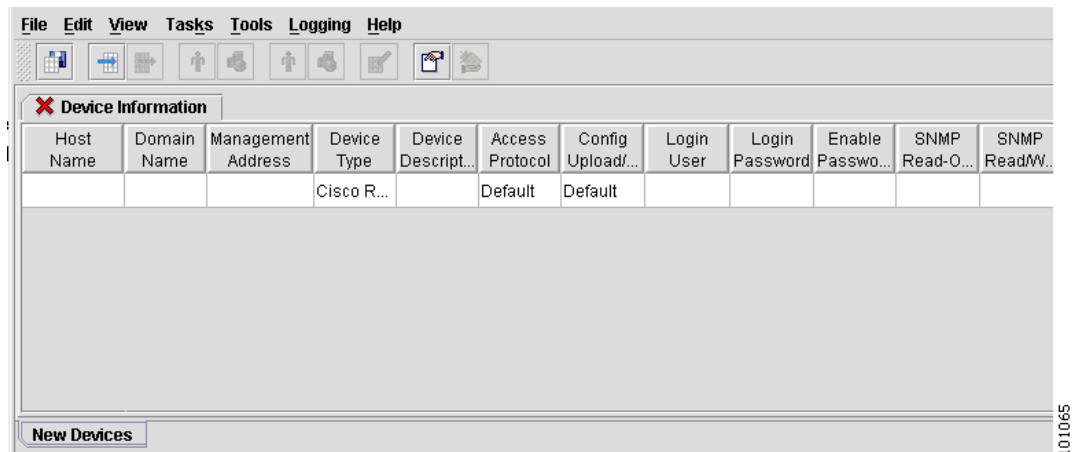
If you do not have existing configuration files, you can discover devices on your network, using the Dynamic Device List.

To create a new Device List and start Auto Discovery, follow these steps:

- Step 1** From the Inventory Manager menu, choose **File > New > New Dynamic Device List (without existing configs)**.

A new Device Spreadsheet appears, as shown in [Figure 4-101](#).

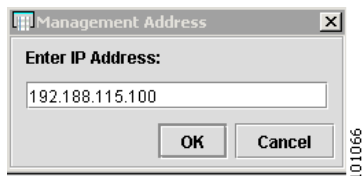
Figure 4-101 New Device Spreadsheet



- Step 2** Click the **Management Address** cell.

A Management Address window appears, as shown in [Figure 4-56](#).

Figure 4-102 Enter IP Address

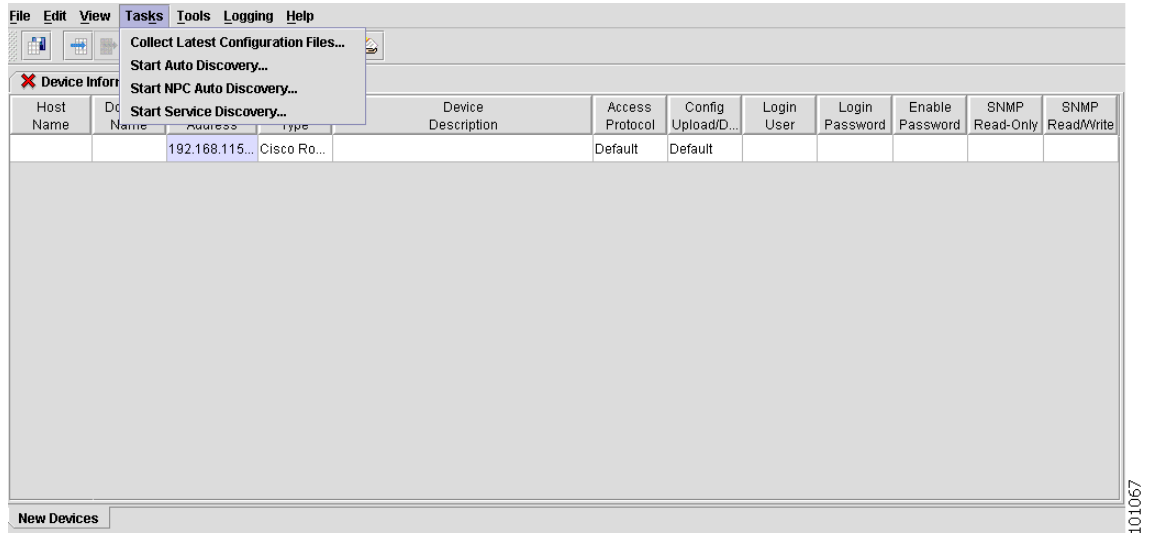


- Step 3** Enter the IP address of the device from which you want to start the device discovery process and click **OK**.

A Device Information spreadsheet appears, as shown in [Figure 4-103](#).

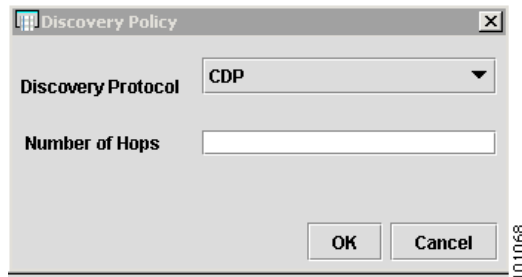
- Step 4** From the Inventory Manager Task Bar, choose **Tasks > Start Auto Discovery** to start the device discovery process.

Figure 4-103 Start Device Discovery



The Discovery Policy window appears, as shown in [Figure 4-104](#).

Figure 4-104 Discovery Policy

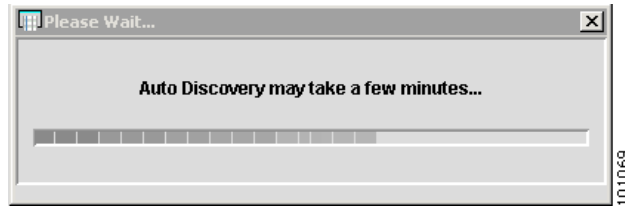


- Step 5** Enter the Number of Hops.

This number represents the number of hops from the device with the IP address. For example, the number **1**.

The Please Wait window appears, as shown in [Figure 4-105](#).

Figure 4-105 Please Wait



Note

This waiting period depends on the number of hops and number of devices in the network.

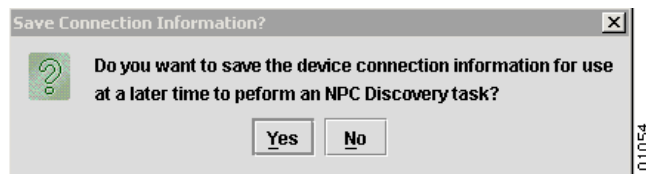
When the waiting period ends, the Device Information spreadsheet appears with the discovered devices, as shown in [Figure 4-106](#).

Figure 4-106 Discovered Devices

Device Information										
Host Name	Domain Name	Management Address	Device Type	Device Description	Access Protocol	Config Upload/Do...	Login User	Login Password	Enable Password	
enswosr1	cisco.com	192.168.115.100	Cisco Router	Cisco Catalyst 6509 SP Switch	Default	Default				pu
mlsw4		172.29.146.40	Cisco Router	Cisco Catalyst 2950 Intelligent Ethernet Switch	Default	Default				pu
ensw4000-1		192.168.115.181	CATOS	Cisco Catalyst 4003 Switch	Default	Default				pu
ensw3550-1		192.168.115.178	Cisco Router	Cisco Catalyst 3550 Intelligent Ethernet Switch	Default	Default				pu

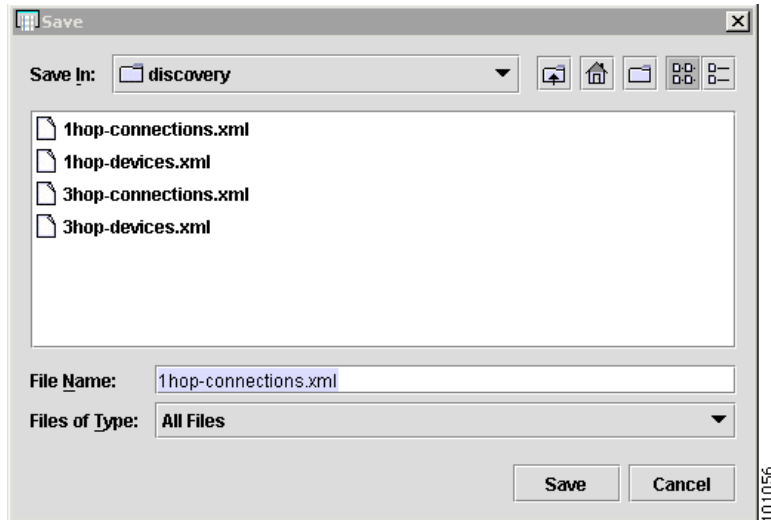
The Save Connection Information window also appears, as shown in [Figure 4-107](#).

Figure 4-107 Save Connection Information

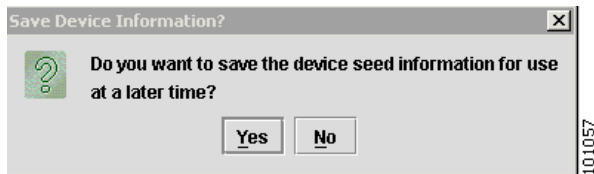


Step 6 To save the connection information, click **Yes**. This information will be used in the **Start NPC Auto Discovery** process.

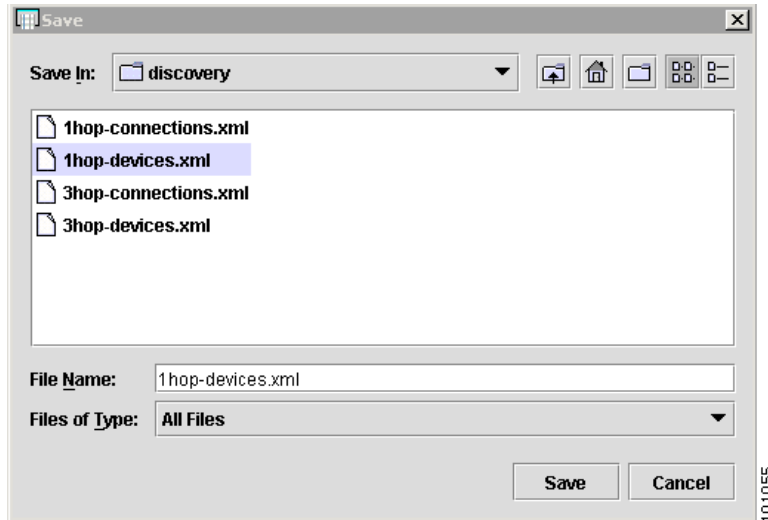
A Save Connection Information Confirmation window appears, as shown in [Figure 4-108](#).

Figure 4-108 Save Connection Information Confirmation

- Step 7** To save the connection information, give the file a name and click **Save**.
 Another Save Device Information window appears, as shown in [Figure 4-109](#).

Figure 4-109 Save Device Information

- Step 8** To save the device information, click **Save**.
 The Save Device Information Confirmation window appears, as shown in [Figure 4-110](#).

Figure 4-110 Save Device Information Confirmation

- Step 9** To save the device information, give the file a name and click **Save**.
The Device Information spreadsheet appears, as shown in [Figure 4-111](#).

Figure 4-111 Device Information

Device Information										
Host Name	Domain Name	Management Address	Device Type	Device Description	Access Protocol	Config Upload/Do...	Login User	Login Password	Enable Password	
enswosr1	cisco.com	192.168.115.100	Cisco Router	Cisco Catalyst 6509 SP Switch	Default	Default				pu
mlsw4		172.29.146.40	Cisco Router	Cisco Catalyst 2950 Intelligent Ethernet Switch	Default	Default				pu
ensw4000-1		192.168.115.181	CATOS	Cisco Catalyst 4003 Switch	Default	Default				pu
ensw3550-1		192.168.115.178	Cisco Router	Cisco Catalyst 3550 Intelligent Ethernet Switch	Default	Default				pu

Now you can edit your devices and collect the latest configuration files.

Start NPC Auto Discovery

From the Inventory Manager Task Bar, choose **Tasks > Start NPC Auto Discovery** to start the connection discovery process.

To import connections with NPC Auto Discovery, follow these steps:

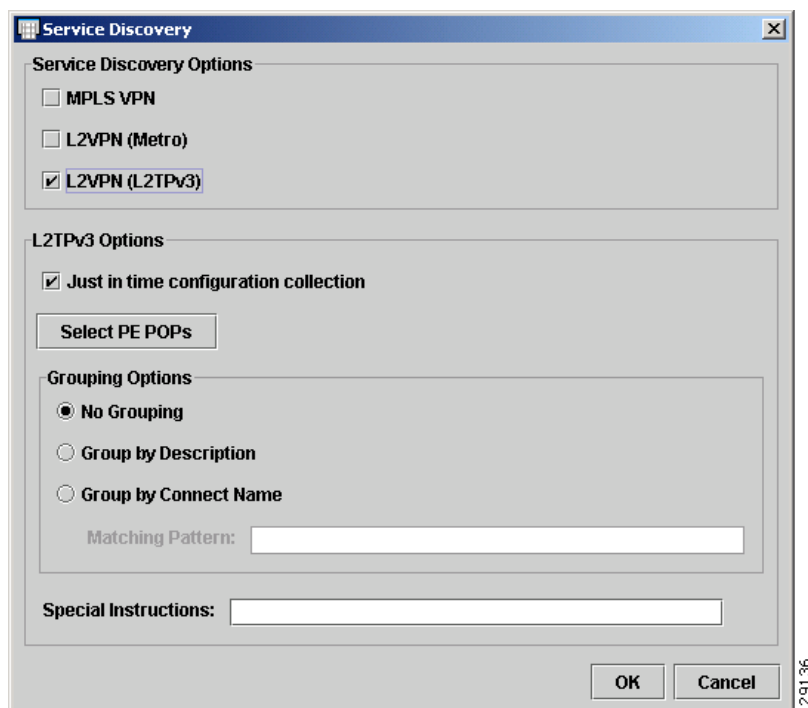
-
- Step 1** Choose **Tasks > Start NPC Auto Discovery**.
- You are prompted to provide the path to the correct **connection.xml** file.
- Step 2** Select the correct **connection.xml** file and click **OK**.
- A dialog box appears, indicating that the NPC discovery process has started.
- Step 3** You are prompted if the task completes successfully. Select **OK** to finish this portion of the NPC Auto Discovery process.
- To find the discovered NPCs, go to **Service Inventory > Inventory and Connection Manager > Named Physical Circuits**.
-

Start Service Discovery

To import services with Auto Discovery from Inventory Manager, in the Task Bar choose **Tasks > Start Service Discovery** to start the service discovery process.

The Service Discovery window in [Figure 4-112](#) appears.

Figure 4-112 Service Discovery



You can choose between the following Service Discovery options:

- **MPLS VPN**—Create a MPLS VPN Service Request for each VRF-enabled interface.
- **L2VPN (Metro)**—Create a L2VPN (Metro) Service Request.
- **L2VPN (L2TPv3)**—Create a L2VPN (L2TPv3) Service Request



Note L2TPv3 auto discovery is limited to L2TPv3 L2VPN service requests.

Checking the **L2VPN (L2TPv3)** box enables the bottom L2TPv3 Options (see [Figure 4-112](#)):

Just in time configuration collection—Upload the PE configurations from the routers before auto discovery.

Select PEs—Opens the Select PE POPs window, where you can select one or more PE POPs

- Grouping Options:
 - **No Grouping**—One auto-discovered L2TPv3 session (link) will become one SR.
 - **Group by Description**—(Currently not implemented)
 - **Group by Connect Name**—More than one auto-discovered L2TPv3 session will be grouped into one SR if they share the same connect name.
- **Special Instructions**—(Currently not implemented)

You are notified when service discovery is finished.

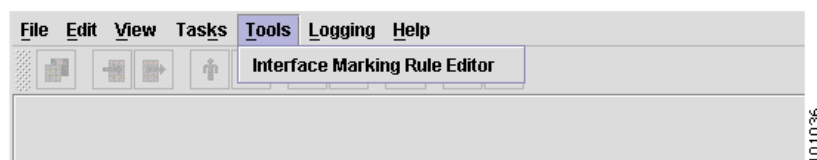
Tools Menu



Note IPsec, firewall, NAT: **These features are not supported in this release.**

To open a rule editor where you can create and modify rules for marking interfaces, import and export rule files, and specify values for IPsec, NAT, QoS, and Firewall, choose **Tools > Interface Marking Rule Editor** from the Inventory Manager Task Bar, as shown in [Figure 4-113](#).

Figure 4-113 Interface Marking Rule Editor



The Interface Rule Editor Task Bar appears with an **interface-rules** dialog box, as shown in [Figure 4-114](#).

Figure 4-114 Interface Rule Editor Task Bar

The Task Bar has the following options:

- [File](#), page 4-98
- [Edit](#), page 4-104
- [Help](#), page 4-104

File

The File option has the following options:

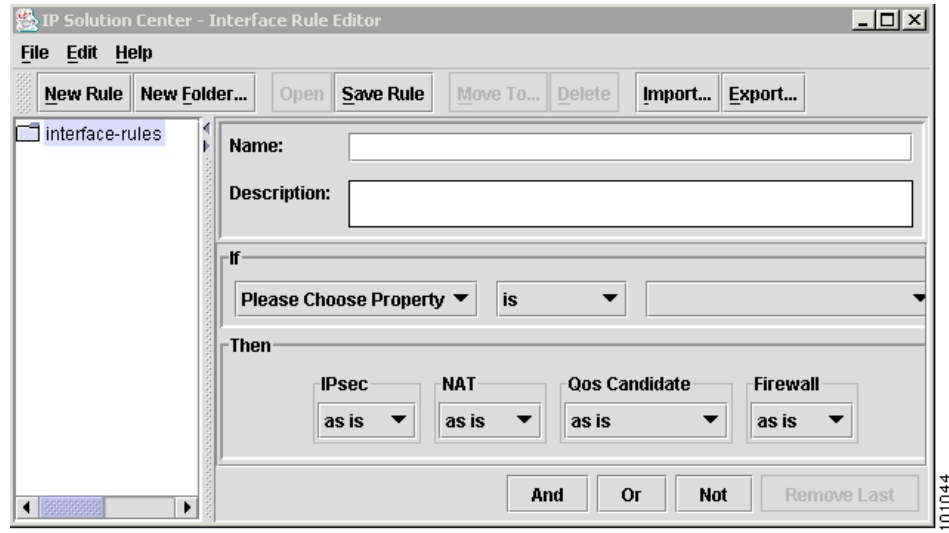
- [New Rule](#), page 4-98
- [New Folder](#), page 4-103
- [Open](#), page 4-103
- [Close](#), page 4-103
- [Import](#), page 4-103
- [Export](#), page 4-103
- [Save Rule](#), page 4-104

New Rule

To create a new rule, follow these steps:

-
- Step 1** Click the **interface-rules** folder and choose **New Rule** from the File option or New Rule icon. A dialog box appears, as shown in [Figure 4-115](#).

Figure 4-115 Interface Rule Editor Dialog Box

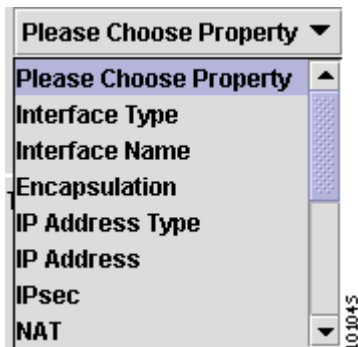


Step 2 Enter the following information:

- **Name**—Name of the rule (required).
- **Description**—Description of the rule (optional).

Step 3 From the If clause drop-down buttons, click **Please Choose Property** and a Property drop-down list appears, as shown in Figure 4-116.

Figure 4-116 Property Drop-Down List



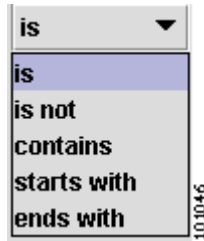
Step 4 Select a Property.



Note

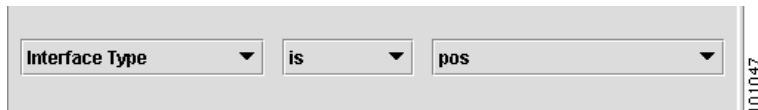
The Property that you select determines the content of subsequent drop-down lists.

Step 5 Click **is** and a Relationship drop-down list appears, as shown in Figure 4-117.

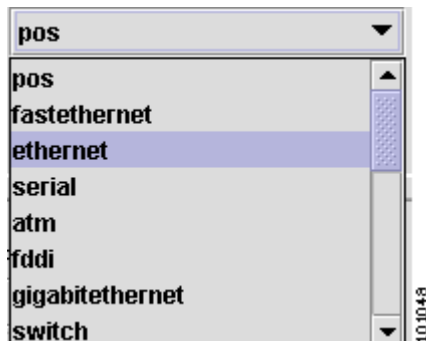
Figure 4-117 Relationship Drop-Down List

Step 6 Select a Relationship.

Step 7 If you had chosen **Interface Type** for the Property and **is** for the Relationship, the drop-down button would show **pos**, as shown in [Figure 4-118](#).

Figure 4-118 Pos Drop-Down Button

Step 8 Click **pos** and a Type drop-down list appears, as shown in [Figure 4-119](#).

Figure 4-119 Type Drop-Down List

Step 9 Select a Type.

If you chose **ethernet**, for example, you would have defined the following interface type If clause in the new rule:

- If the interface type is Ethernet

You can define how to mark the interface with the Then clause drop-down buttons, as shown in [Figure 4-120](#).

Figure 4-120 Then Clause Drop-Down List

You can create a new rule to mark interfaces for the following security and quality features:

- IPsec
- NAT
- QoS
- Firewall

Step 10 To change the interface marking for IPsec, click the IPsec drop-down list, and make the appropriate selection. An IPsec drop-down list appears, as shown in [Figure 4-121](#).

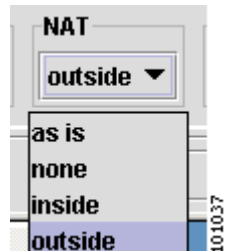
Figure 4-121 IPsec Drop-Down List



Step 11 Select a setting.

Step 12 To change the interface marking for NAT, click the NAT drop-down list, and make the appropriate selection. A NAT drop-down list appears, as shown in [Figure 4-122](#).

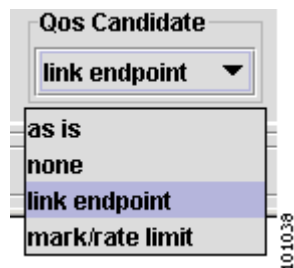
Figure 4-122 NAT Drop-Down List



Step 13 Select a setting.

Step 14 To change the interface marking for QoS, click the QoS drop-down list, and make the appropriate selection. A QoS drop-down list appears, as shown in [Figure 4-123](#).

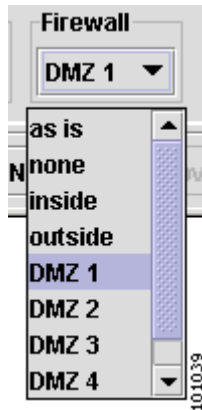
Figure 4-123 QoS Drop-Down List



Step 15 Select a setting.

- Step 16** To change the interface marking for Firewall, click the Firewall drop-down list, and make the appropriate selection. A Firewall drop-down list appears, as shown in [Figure 4-124](#).

Figure 4-124 Firewall Drop-Down List



- Step 17** Select a setting.

If you selected the security and quality features above, you would have formulated the following Then clause in the new rule:

- Set:
 - IPsec to **private**
 - NAT to **outside**
 - QoS to **Link Endpoint**
 - Firewall to **DMZ1**

The **as is** for each service shows the changed value in the Then clause drop-down buttons, as shown in [Figure 4-125](#).

Figure 4-125 Then Clause Drop-Down List



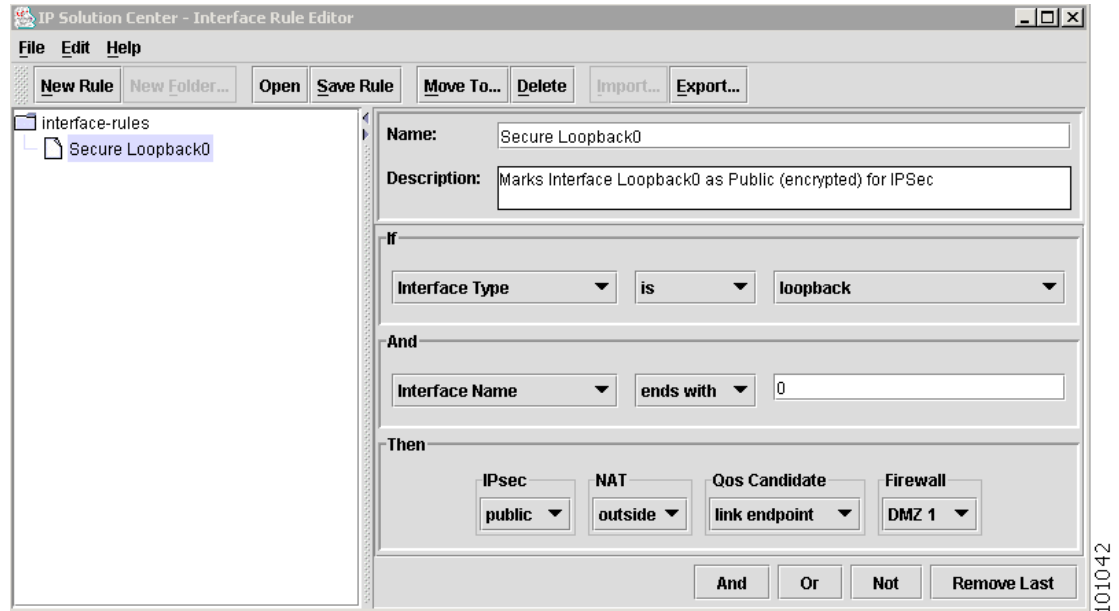
You can create additional If clause statements with more complicated logic, by using the And, Or, and Not drop-down buttons, as shown in [Figure 4-126](#).

Figure 4-126 Additional If Clause Drop-Down List



You can remove the additional statements by using the Remove Last button.

[Figure 4-127](#) show an example of a rule with an additional If clause.

Figure 4-127 Example of a Rule**Note**

One rule can mark all Loopback0 interfaces as public for IPsec, outside for NAT, link endpoint for QoS, and DMZ1 for Firewall.

New Folder

Creates a new folder under the selected folder.

Open

Opens the selected rule.

Close

Closes the selected rule.

Import

Imports external rules to an existing folder. Each rule and folder contained in the file is created under the selected folder in the tree.

Export

If you select one or more rules without a folder, the rules are exported to a file of your choice. You can then share this file with other users of Inventory Manager.

If you select a folder, all child folders and contained rules can be exported to a file of your choice. You can then share this file with other users of Inventory Manager.

If used with a single rule, it exports that rule, to a single file.

If used on a folder, it will export all the rules from that folder, to a single file.

Save Rule

Saves the modified rule.

Edit

Delete

Deletes the selected rule or folder.

Moves To

Moves a rule or folder to an existing folder.

Help

About

Contains information on Cisco Systems and the ISC software version.

License

Contains the ISC software license agreement.

Logging Menu

From the Inventory Manager Task Bar, shown in [Figure 4-25 on page 4-34](#), Logging is the sixth menu on the Task Bar. The Logging menu allows you to specify the following log output levels to the Logging UI:

- All
All log messages are sent to the Log Viewer located near the bottom of Inventory Manager
- Severe
Only severe log messages are sent to the Log Viewer located near the bottom of the Inventory Manager
- Warning
Only warning and severe log messages are sent to the Log Viewer located near the bottom of the Inventory Manager
- Info
Only informational, warning, and severe log messages are sent to the Log Viewer located near the bottom of the Inventory Manager
- Fine
Only fine, informational, warning, and severe log messages are sent to the Log Viewer located near the bottom of the Inventory Manager

- **Finer**
Only finer, fine, informational, warning, and severe log messages are sent to the Log Viewer located near the bottom of the Inventory Manager
- **Finest**
Only finest, finer, fine, informational, warning, and severe log messages are sent to the Log Viewer located near the bottom of the Inventory Manager
- **Off**
No log messages are sent to the Log Viewer located near the bottom of the Inventory Manager.

Help

From the Inventory Manager Task Bar, shown in [Figure 4-25 on page 4-34](#), Help is the seventh menu on the Task Bar. The Help menu has the following option:

- [About, page 4-105](#)

About

Loads the About dialog showing version information and some web URLs for Cisco Systems Inc.

Auto Discovery

This section describes the Auto Discovery features. It contains the following sections:

- [Auto Discovery Overview, page 4-105](#)
- [Auto Discovery Prerequisites, page 4-106](#)
- [Process Flow, page 4-106](#)
- [User Interface, page 4-106](#)

Auto Discovery Overview

With Auto Discovery, ISC can automatically perform the following operations:

- Discover all the devices and the physical links between the devices.
- Discover Ether channels, loopback addresses, interfaces, and encapsulation types for interfaces on each device.
- Discover all L2VPN/VPLS and L3VPN services.

To understand the benefits of Auto Discovery, consider the following business scenario. ISC is connected to a network that contains more than 50 devices with some L2VPN and L3VPN services already provisioned.

Without Auto Discovery, the operator would need to manually enter the following information in ISC:

- Information about all the devices and the physical links between these devices.
- Information about all the existing L2VPN services and L3VPN services.

Auto Discovery Prerequisites

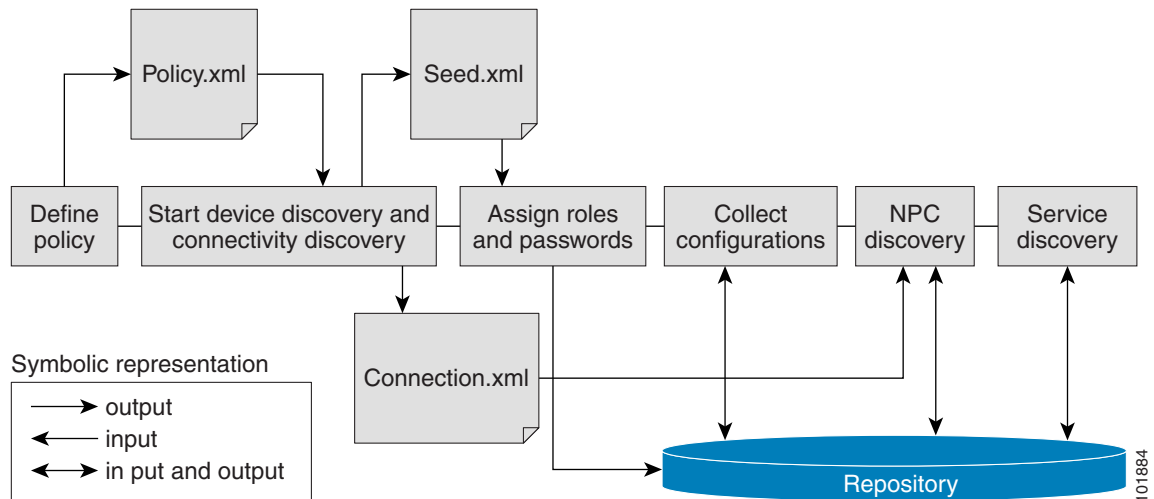
Before running Auto Discovery, you should do the following:

- Enable SNMP on all devices.
- Enable CDP on all devices you want to discover.
- Have a lab diagram that shows how the network is set up.
- Disable all NAT IP address mapping in the network. (**This feature is not supported in this release.**)
- Not have multiple installations of ISC in one subnet.

Process Flow

Figure 4-128 shows the Auto Discovery Process.

Figure 4-128 Auto Discovery Process Flow



Cornerstone Bridge Log is available for viewing from an internet browser.

User Interface

There are two user interfaces available for running Auto Discovery:

- Inventory Manager GUI
- UNIX Command Line Interface (UNIX CLI)

Inventory Manager GUI

To use Auto Discovery within Inventory Manager, follow these steps:

-
- Step 1** Choose **File > New > New Dynamic Device List** to create a **policy.xml** file.

- Step 2** Choose **Tasks > Start Auto Discovery**.
- Step 3** Choose your own location and names to save the seed file and connection output file.
- Step 4** Assign roles and passwords.
- Step 5** Choose **Tasks > Collect Latest Config Files**.
- Step 6** Choose **Tasks > Start NPC Discovery** using the connection output file.
- Step 7** Choose **Tasks > Start Service Discovery** to do Common and Service Discovery.

To see the results of the Auto Discovery and Service Discovery processes, the following screens are available:

- Choose **Service Inventory > Inventory and Connection Manager > Service Requests** to see Service Requests.
 - Choose **Service Inventory > Inventory and Connection Manager > Named Physical Circuits** to see NPC.
 - Choose **Service Inventory > Inventory and Connection Manager > NPC Rings** to see Ring Topologies.
-

UNIX Command Line Interface (UNIX CLI)

To use the UNIX CLI, follow these steps:

-
- Step 1** Edit **policy.xml** in **\$ISC_HOME/bin**.
- Step 2** Run **\$ISC_HOME/bin/invokeDiscovery.sh** for device and connection discovery.
- Step 3** Output files are saved in **\$ISC_HOME/tmp/seed.xml** and **\$ISC_HOME/tmp/connection.xml** automatically.
- Step 4** Use Inventory Manager to assign roles and passwords for devices and collect configuration files. See [Creating a New Customer with Devices, page 4-10](#).
- Step 5** Run **\$ISC_HOME/bin/runDiscoverNPC.sh** to populate connections.
- Step 6** Run **\$ISC_HOME/bin/runCommonDiscovery.sh** for all service discovery.
- Step 7** Log available via standard output.
-

Service Discovery

This section describes the types of Service Discovery that ISC currently supports. It contains the following sections:

- [MPLS Service Discovery, page 4-108](#)
- [Grey Management Discovery, page 4-110](#)
- [Layer 2 VPN Discovery, page 4-111](#)
- [VPLS Service Discovery, page 4-112](#)

MPLS Service Discovery

This section describes the process for MPLS Service Discovery. This section contains the following sections:

- [MPLS Service Discovery Overview, page 4-108](#)
- [Limitations, page 4-108](#)
- [MPLS Service Discovery Process, page 4-109](#)

MPLS Service Discovery Overview

The IP Solution Center (ISC) provides a mechanism to discover the state of the network. Using Inventory Manager, you can discover information about the following network features:

- Devices (Network hardware)
- Connections (Named Physical Circuits)
- Services (L2 VPN and L3 MPLS VPN service requests)

MPLS VPN Service Discovery provides the following benefits:

- When you create an MPLS VPN service request, less information needs to be added.
- Services provisioned by non-ISC applications can be discovered and managed by ISC.

An MPLS VPN service request consists of one or more MPLS VPN links. ISC supports Service Discovery for two types of MPLS VPN links:

- PE-CE
- PE-NoCE

The Unmanaged CE option is also supported for the PE-CE type.

Limitations

In cases where Auto Discovery is used, ISC has the following Auto Discovery limitations:

- Auto Discovery does not support creating Service Requests with an MVRF CE PE-CE links.
- Auto Discovery does not support creating Service Requests for commands not supported by ISC.

MPLS Service Discovery Process

The MPLS Service Discovery process creates one MPLS VPN Service Request for each VRF-enabled interface. A VRF-enabled interface is an interface on which the **ip vrf forwarding** command is configured on the PE.


Note

MPLS Service Discovery can be invoked only after Device Discovery and NPC Discovery have been completed *successfully*.

The following steps describe the logic MPLS Service Discovery uses to create Service Requests and populate the Repository:

- Step 1** Find all the PE devices in the Repository with the role of PE-POP.
- Step 2** Analyze the configuration file for each PE found in the previous step.
- Step 3** Identify all the VRF-enabled interfaces (these interfaces can also be sub-interfaces).
- Step 4** Check each VRF-enabled interface for valid Service Requests (SR).
- Step 5** If a valid SR exists, ignore the VRF-enabled interface.
Otherwise, for each VRF-enabled interface, find the CE connected to the interface in the Named Physical Circuit (NPC) table, which was populated by the NPC Discovery process.


Note

An NPC is a collection of physical links. By traversing the physical links, you can find the terminating logical device for the VPN link.

- Step 6** Find the sub-interface on the CE that connects the MPLS link with the PE.
- Step 7** If no terminating CE is found in the NPC table, create an SR without the CE.
- Step 8** Create a generic MPLS Service Policy for each PE-CE link, and attach it to the Customer associated with the CE.


Note

An MPLS Service Policy provides defaults to simplify the provisioning of service requests.

- Step 9** Create a generic MPLS Service Policy for each PE-Only link, and attach it to the Provider associated with the PE.
- Step 10** Analyze the PE and CE configuration files, and determine the routing protocols, based on the IP addresses of the participating interfaces.


Note

Some of the routing protocols, for example BGP and EIGRP, cannot be deduced in the PE-Only SR, because the CE configuration file is not available.

- Step 11** Analyze the configuration files, capture all the available redistribution related information, and then populate the Repository.
- Step 12** Analyze a list of export and import route targets for each VRF.
- Step 13** Create CERCs and CERC Membership.

- Step 14** Turn on the override VRF Name and RD Flag for the MPLS VPN Link. (This information is captured from the configuration file.)
- Step 15** Save the MPLS SR with the MPLS VPN Link in the Repository with a flag indicating that this service request was discovered.
-

Synchronization

The MPLS Service Discovery process does not synchronize existing services. If it is determined that an SR exists in the Repository for a particular interface, the Discovery process ignores the interface. But, if you have manually added a service on a new interface and ISC is not aware of it, the Service Discovery process creates the newly added service in the Repository.

CERC Creation

Given a list of Route Targets in the configuration files for each of the VRFs, the MPLS VPN Service Discovery module needs to re-create the CERC according to the ISC service model. MPLS VPN Service Discovery assumes that the services provisioned on the network are provisioned manually and do not follow the conventions adopted by ISC for topologies (CERC Route Target Allocation). As a result, a CERC created to fit into the service model supported by ISC is not associated with any VPN. You must create the VPN and associate it to the CERC created by discovery.

User Input After Discovery

After Service Discovery, a Policy and an SR are created. When a CE is discovered, a Customer-owned Policy is created. When no CE is discovered, a Provider-owned Policy and Global SR are created. After the Service Discovery process is complete, you cannot modify the relationship between the Customer and the SR. This restriction applies to both the Customer-owned and Global SRs.

The Service Discovery process ends with the newly created Service Requests in a PENDING state and the related objects in the Repository. After the completion of the Discovery process, you must go to the GUI, create the VPN, and connect the VPN with the CERC.

You cannot modify the Policy or the SR or associate an SR with a Customer or Provider at this point.

Because the CERC is a logical concept used within ISC to represent topologies, Service Discovery is unable to connect the way you have manually configured the services with CERC.



Note

The configuration files that Discovery processes upload from device are logged under `$ISC_HOME/tmp/autodiscovery`.

Grey Management Discovery

This section describes the process of Grey Management Discovery.

The following steps describe the logic MPLS Service Discovery uses to create Grey Management Service Requests and populate the Repository:

- Step 1** The discovery process scans the PE configuration files to determine if there is a VRF provisioned by ISC (VRF name starts with `grey_mgmt_vpn`).

- Step 2** After finding a VRF, the discovery process scans the NPC connection table to determine if there is an NPC on that interface, and if a Managed CE (MCE) is connected to the PE on this interface.
- Step 3** If an MCE is found, the discovery process scans the Route Target entries in the Management VRF for the Management CERC, and attaches it to the Management VPN.
- The discovery process also caches the route target of the Management VRF.
- Step 4** A Management SR with a corresponding Management Link for the MCE and PE connection is created in the Repository.
- Step 5** If, when the new Links are created, Management Route Targets are found, they are ignored and the join Grey Management flag is turned on.

Layer 2 VPN Discovery

This section contains the following sections:

- [Topology, page 4-111](#)
- [Logic \(MPLS Core\), page 4-111](#)
- [Logic \(L2TPv3\), page 4-112](#)

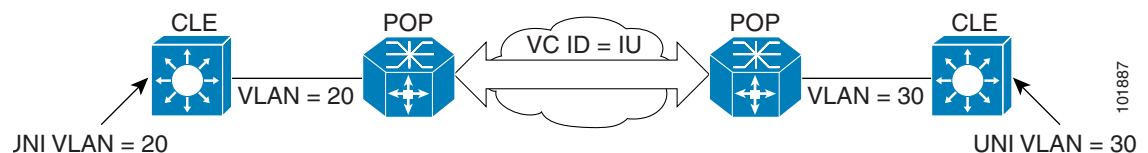
Topology

L2 VPN Discovery:

- Discovers inter-POP EWS and ERS (with No-CE) services.
- Creates all Service Requests in PENDING state. One generic VPN is generated for all discovered services.

[Figure 4-129](#) shows the L2VPN Discovery Topology.

Figure 4-129 L2VPN Discovery Topology



Logic (MPLS Core)

The following steps describe the logic that L2VPN Service Discovery uses to create Service Requests and populate the Repository for an MPLS core:

- Step 1** Gets all POPs and parses their configuration files.
- Step 2** Discovers the VCs between the POPs (a pseudo wire is discovered).
- Step 3** Discovers the VLAN ID that maps to the VC for each POP.

- Step 4** Gets all UNIs on each POP, which is associated with a VC tunnel endpoint, and the UNIs on the associated CLE (linked via trunk mode) that allows the VLAN ID to pass.
- Step 5** If there is a pair of UNIs on each side of the CORE, which shares the same VC, an SR is discovered.
-

Logic (L2TPv3)

L2TPv3 service discovery can be performed from Inventory Manager as described in [Start Service Discovery, page 4-96](#).

In the case of L2TPv3, the L2VPN Service Discovery uses the following steps to create Service Requests and populate the Repository:

-
- Step 1** Gets all POPs and parses their configuration files.
- Step 2** Looks for all ATM, Serial and MFR interfaces and gets all the VCs with L2TPv3 encapsulation (for ATM the VC is under the PVC).
- Step 3** Sets the interface containing the VC statement as the UNI interface.
-

VPLS Service Discovery

This section contains the following sections:

- [Topology, page 4-112](#)
- [Restrictions, page 4-113](#)

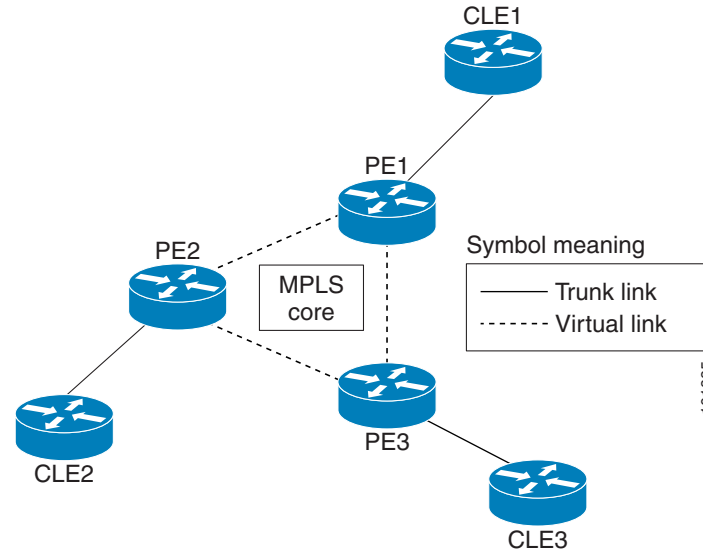
Topology

VPLS Discovery:

- Discovers only full-mesh VPLS topologies.
- Creates all Service Requests in the PENDING state.
- Creates a VPN with the name of the VPN Id for the discovered VPLS SR.

[Figure 4-130](#) shows an MPLS core topology to help demonstrate how VPLS Service Discovery creates an SR and associates it with a VPN link.

Figure 4-130 MPLS Network



Logic

The following steps describe the logic L2VPN Service Discovery uses to create Service Requests and populate the Repository:

-
Step 1	Discovers virtual links that are associated with the same VPN ID among PEs across the MPLS core.
Step 2	Discovers trunk links between the PE and its associated CLEs the same way as in L2VPN.
-

Restrictions

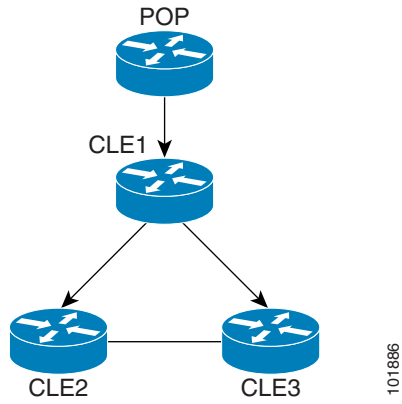
Due to the existing VPLS Policy Types, VPLS Discovery has the following limitations:

- Only EWS with CE and ERS with CE, or EWS without CE and ERS without CE types of topologies can be discovered.
- EWS or ERS with a combination of CE and no CE cannot be discovered.
- Service Requests cannot be created for the above topologies.

Ring Topology Discovery (Connection Discovery)

Connection Discovery can discover ring topology NPCs. A ring of NPCs is a group of physical links that form a loop between the logical CLE devices.

Figure 4-131 shows an sample ring topology.

Figure 4-131 Sample Ring Topology



Service Inventory > Device Console

From the Home window of Cisco IP Solution Center (ISC), you receive upon logging in, click the **Service Inventory** tab or area in the data pane of the window, and you receive a window as shown in [Figure 5-1](#), “[Service Inventory Selections](#).”

Figure 5-1 Service Inventory Selections



Click on **Device Console** and you proceed to [Figure 5-2](#), “[Device Console Selections](#)” and can choose one of the device related operations.

Device Console

Device Console is the starting point for many operations. To navigate through **Device Console**, do the following:

- Step 1** Navigate **Service Inventory > Device Console** and you receive a window as shown in [Figure 5-2](#), “[Device Console Selections](#).”

Figure 5-2 Device Console Selections

Step 2 To select one of the operations, click the radio button for one of the following selections and then click **Next**.

**Note**

All operations must be in live *not* ECHO mode.

- [Download Commands, page 5-2](#) Download operation commands and configlets. The **Select Operation Method** selections of **Simplified** and **Advanced (via wizard)** are only available for **Download Commands** and are explained in that explanation.
- [Download Template, page 5-3](#) Downloads template configlets to the specified devices.
- [Device Configuration Manager, page 5-8](#) Displays different versions of configuration files created on a repository per timestamp and writes to running-configuration or start-up configuration.
- [EXEC Commands, page 5-10](#) Allows you to send to target devices any Cisco IOS commands that can be executed in enable mode.
- [Reload, page 5-15](#) Remotely reloads devices.

Download Commands

To download commands, do the following:

- Step 1** Navigate **Service Inventory > Device Console > Download Commands**.
- Step 2** The **Select Operation Method** default is **Simplified**, which indicates that in a single window you have the options for selecting the Devices, Device Groups, and Operation Commands. You do not need to multi-click. In a single window you can submit the required parameters to complete the task. **Advanced (via wizard)** indicates you must go to multiple windows to achieve the task. In this method, you select Device, click **Next**, select Device Groups, click **Next**, select Operation Command, and then the summary.
- Step 3** Click **Next**. A window as shown in [Figure 5-3, “Device Console—Download Commands: Select Devices,”](#) appears.

Figure 5-3 Device Console—Download Commands: Select Devices

Device Console - Download Commands

Devices:		Select/Deselect
Groups:		Select/Deselect
Operation Commands:		Load File
Options:	☐ Upload Config After Download ☐ Retrieve device attributes	

OK Cancel

Note: * - Required Field

129042

- Step 4** In the **Devices** row, click **Select/Deselect**. In the new window, select the check box for each device you want. Deselect a check box if you do not want this device. Then click **Select**. [Figure 5-3](#) then reappears with the selected devices in the **Devices** row.
- Step 5** In the **Groups** row, click **Select/Deselect**. In the next window, select the check box for each group you want. Deselect a check box if you do not want this group. Then click **Select**. The selected groups appear in the **Groups** row.
- Step 6** In the **Operation Commands** field, enter the commands you want to download or click **Load File** to select a set of commands to place in the **Operation Commands** field.
- Step 7** If you leave the **Upload config after download** check box deselected, you do *not* upload the configuration file after the download.
- Step 8** Click **OK** to submit the download and you receive a window with the **Device Console Operation Result** and in the bottom left corner a **Status**. You can click **Download** or **Done**.
- Step 9** When you click **Download**, you return to [Step 6](#) to download additional commands on the selected devices.
- Step 10** When you click **Done**, you return to [Figure 5-2](#).

Download Template

To download a template, do the following:

- Step 1** Navigate **Service Inventory > Device Console > Download Template** from [Figure 5-2](#) and click **Next**. A window as shown in [Figure 5-4](#), “[Device Console—Download Template: Select Devices](#),” appears.

Figure 5-4 Device Console—Download Template: Select Devices

- Step 2** Continue with [Step 3](#) if you want to add devices; proceed to [Step 9](#) to delete devices; or click **Next** to proceed to [Step 11](#) for **3. Select Device Groups**.
- Step 3** Click **Add**, as shown in [Figure 5-4](#), to **2. Select Devices**.
- Step 4** From the resulting window, as shown in [Figure 5-5](#), “[Device Selection](#),” you can filter the choices: Device Name; Device Group; or Collection Zone from **Show Devices with**, and if you like, enter **Matching** information and click **Find**.

Figure 5-5 Device Selection

- Step 5** From the devices listed, select the check box(es) for each device you want to select or select the check box in the header row to select all the devices. Then click **Select**.

- Step 6** You return to [Figure 5-4](#) with the added devices.
- Step 7** For each device, you can click the added **Clear** button to clear the **Upload to Customer/Site** column to reflect **none selected**, or you can click the added **Select** button and a new window allows you to **Create Customer**, **Create Site**, **Select**, or **Cancel**. When you click **Select** in this new window, you return to [Figure 5-4](#) with the added customer or site.
- Step 8** You can repeat [Step 3](#) to [Step 7](#) to **Add** more devices, you can delete devices, as explained in [Step 9](#), or you can proceed by going to [Step 10](#).
- Step 9** To delete devices, you can filter the list in [Figure 5-4](#), by choosing a **Category: Any, Name, or Group** and entering the characters you want in **matching** and then clicking **Find**. From the resulting list, select the check box(es) for the devices you want to delete or select the check box in the header row to select all the devices and then click **Delete**. Select carefully, because there is no chance to confirm this deletion.
- Step 10** When you have all the devices you want, click **Next**. You proceed to **3. Select Device Groups**, starting in [Step 11](#).
- Step 11** Continue with [Step 12](#) if you want to add device groups; proceed to [Step 16](#) to delete device groups; or click **Next** to proceed to [Step 18](#) for **4. Enter Download Commands**.
- Step 12** Click **Add**, as shown in [Figure 5-6](#), to **3. Select Device Groups**. Adding Device Groups is not required.

Figure 5-6 Device Group Selection

Group name matching:

Showing 0 of 0 records

#	☒	Name	Description
Rows per page: 10			

96315

- Step 13** From the resulting window, as shown in [Figure 5-7](#), “[Group Association](#),” you can filter the choices: Device Group Name; or Description from **Show Device Groups with**.

Figure 5-7 Group Association

Groups associated with **Device Console**

Show Device Groups with matching

Showing 1-1 of 1 records

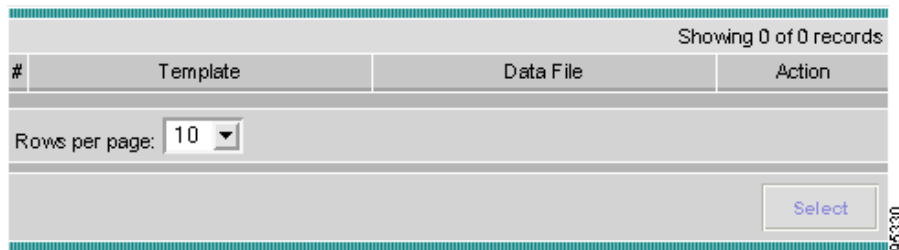
#	☐	Device Group Name	Description
1.	☐	group1	

Rows per page: 10

93831

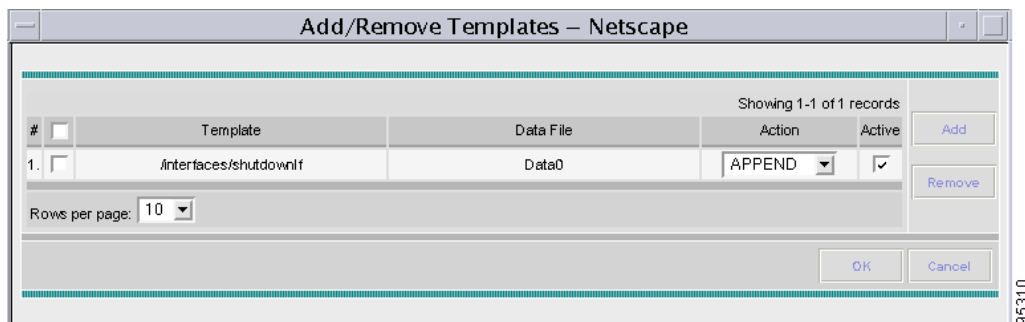
- Step 14** From the device groups listed, select the check box(es) for each device group you want to select or select the check box in the header row to select all the device groups. Then click **Select**.
- Step 15** You return to [Figure 5-6](#) with the added device groups. You can repeat [Step 12](#) to [Step 14](#) to **Add** more device groups, you can delete device groups, as explained in [Step 16](#), or you can proceed by going to [Step 18](#).
- Step 16** To delete device groups, you can filter the list in [Figure 5-6](#), by entering the characters you want in **Group name matching** and then clicking **Filter**. From the resulting list, select the check box(es) for the devices you want to delete or select the check box in the header row to select all the devices and then click **Delete**. Select carefully, because there is no chance to confirm this deletion.
- Step 17** When you have all the device groups you want, click **Next**. You proceed to **4. Select Download Template**, starting in [Step 18](#).
- Step 18** For **4. Select Download Template**, the resulting window is shown in [Figure 5-8](#), “[Select Download Template](#).”

Figure 5-8 Select Download Template



- Step 19** In [Figure 5-8](#), you can click the **Select** button.
- Step 20** A window as shown in [Figure 5-9](#), “[Add/Remove Templates](#),” appears. Click **Add** to add templates or **Remove** to remove templates. When you have the templates you want, click **OK**.
- When you click **Add** you get a Template Datafile Chooser window with the template choices in the tree. Click **+** to open the folders and subfolders in the tree, until you get the property to you want to choose. Click on that property and it is added to your list. Repeat this until all the templates you want are in your list. In each added property, you can click **View** and you receive the configlet for that data file. To return, click **OK**. In [Figure 5-9](#), select the check box(es) for the template(s) you want. In each template row, click the **Action** drop-down menu and choose **APPEND** or **PREPEND** to add information after or before; click or unclick the **Active** button; and then click **OK**.

Figure 5-9 Add/Remove Templates



- Step 21** You return to [Figure 5-9](#) with the updated information.

- Step 22** Click **Next** and you proceed to **5. Download Template Summary**, as explained in [Step 23](#).
- Step 23** For **5. Download Commands Summary**, a window as shown in [Figure 5-10](#), “**Download Template Summary**,” appears.

Figure 5-10 Download Template Summary

Device Console - Download Template: Download Template Summary

Mode: **ADDING**

- ☒ 1. Choose Operation
- ☒ 2. Select Devices
- ☒ 3. Select Device Groups
- ☒ 4. Select Download Template
- ☐ 5. Download Template Summary

Devices: mlpe2
mlce7

Device Groups:

Template:

☐ Upload Config After Download

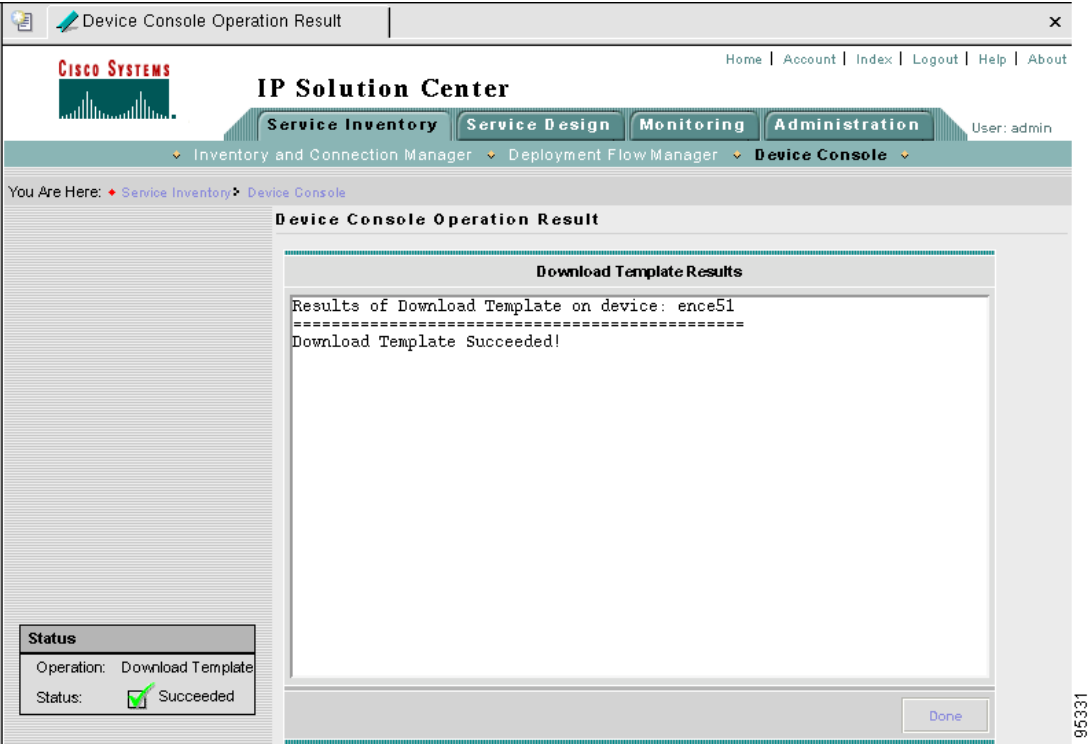
☐ Retrieve device attributes

- Step 5 of 5 -

< Back Next > Finish Cancel

- Step 24** In [Figure 5-10](#), if you leave the **Upload config after download** check box deselected, you do *not* upload the configuration file after the download. If you select the **Upload config after download** check box, you upload the new configuration file after you download the templates in [Step 20](#). If you leave the **Retrieve device attributes** check box deselected, you do not retrieve any device attributes. If you select the **Retrieve device attributes** check box, after the template is downloaded, SNMP is used to retrieve interface information and additional **show** commands, such as **show version** are issued.
- Step 25** Click **Back** until you correct any information you want to change or click **Finish** to submit the download and you receive a window with the **Download Template Results** and in the bottom left corner a **Status** with a green check for **Succeeded**, as shown in [Figure 5-11](#), “**Download Template Results**.”

Figure 5-11 Download Template Results



Step 26 Click **Done** and you return to [Figure 5-2 on page 5-2](#).

Device Configuration Manager

To display the configuration, download the configuration to the startup configuration on the device, or download the configuration to the running configuration on the device, do the following:

Step 1 Navigate **Service Inventory > Device Console > Device Configuration Manager** and from [Figure 5-2](#) click **Next**. A window as shown in [Figure 5-12, “Device Configuration Manager,”](#) appears.

Figure 5-12 Device Configuration Manager

Step 2 In the **Device** row, click **Select** and a window as shown in Figure 5-13, “Device Selection,” appears.

Figure 5-13 Device Selection

#	Select	Device Name	Management IP Address	Type
1.	☐	newdevice1		IE2100
2.	☐	ipsec-cpe-london.cisco.com	172.29.151.10	Cisco IOS Device
3.	☐	ipsec-cpe-paris.cisco.com	172.29.151.11	Cisco IOS Device
4.	☐	ence11	192.168.115.70	Cisco IOS Device
5.	☐	ence132	192.168.115.116	Cisco IOS Device
6.	☐	ence21	192.168.115.73	Cisco IOS Device
7.	☐	ence51	192.168.115.81	Cisco IOS Device
8.	☐	ence61	192.168.115.87	Cisco IOS Device
9.	☐	ipsec-cpe-london	66.66.66.66	Cisco IOS Device
10.	☐	ipsec-cpe-ny	55.55.55.55	Cisco IOS Device

Step 3 From the devices listed, click the radio button for the device you want to select. Then click **Select**.

Step 4 You return to Figure 5-12 with the added device. You can repeat Step 2 to Step 3 to change the device.

Step 5 When you have selected the device you want, go to the **Configuration to Display** row and click the **Select a Version...** drop-down menu. Click the version you want and then click **Load** to load that configuration file.

Step 6 Click one of the following radio buttons or keep the default:

- **Display only** The configuration file can only be viewed.
- **Download to startup** The configuration file is downloaded to the start up configuration of the selected router.

**Note**

For **Download to startup**, the Device Access Protocol (defined in device creation) must be either **ftp** or **tftp**. If this is not the case, the Device Configuration Manager Results window appears and indicates that you must set up either **ftp** or **tftp**.

- **Download to running** The configuration file is downloaded to the router's running configuration file.

**Note**

When the DCPL property **copy-running-to-startup** in the **GTL/ios** folder is set to the default of **true**, the router's running configuration file is also copied to the start up configuration.

Step 7 Click **Finish**. If in [Step 6](#) you chose **Display only**, you automatically return to [Figure 5-2 on page 5-2](#). If in [Step 6](#) you clicked **Download to startup** or **Download to running**, you get a Device Configuration Manager Results window. In the **Status** box, you get a green check mark for **Succeeded** or a red **Failed** status and you must click **Done** to return to [Figure 5-2 on page 5-2](#).

EXEC Commands

EXEC Commands allows you to send to target devices any Cisco IOS commands that can be executed in enable mode. You can only view the router information. You cannot edit or delete the information.

To execute EXEC Commands, do the following:

Step 1 Navigate **Service Inventory > Device Console > EXEC Commands** and [Figure 5-2](#) click **Next**. A window as shown in [Figure 5-14](#), “**Device Console—EXEC Commands: Select Devices**,” appears.

Figure 5-14 Device Console—EXEC Commands: Select Devices

The screenshot displays the Cisco IP Solution Center web interface. At the top, the Cisco Systems logo is on the left, and navigation links (Home, Shortcuts, Account, Index, Help, About, Logout) are on the right. Below the logo, the title 'IP Solution Center' is centered. A secondary navigation bar contains tabs for 'Service Inventory', 'Service Design', 'Monitoring', and 'Administration'. The 'Service Inventory' tab is active, and a sub-tab 'Device Console' is selected. The user is logged in as 'admin'. The main content area is titled 'Device Console - EXEC Commands: Select Devices'. It features a search bar with a dropdown menu set to 'Device Name' and a 'Find' button. Below the search bar, it indicates 'Showing 0 of 0 records'. A table with the following columns is shown: '#', 'Device Name', 'Management IP Address', and 'Type'. The table is currently empty. Below the table, there is a 'Rows per page' dropdown set to '10' and a 'Go to page: 1 of 1' field with a 'Go' button. At the bottom of the table area are 'Add' and 'Delete' buttons. On the left side of the main content area, there is a sidebar with a 'Mode: ADDING' header and a list of steps: '1. Choose Operation', '2. Select Devices' (highlighted), '3. Select Device Groups', '4. Enter EXEC Command', '5. EXEC Commands Summary'. At the bottom of the sidebar, it says '- Step 2 of 5 -'. At the bottom of the main content area, there are navigation buttons: '< Back', 'Next >', 'Finish', and 'Cancel'. The page number '129027' is visible in the bottom right corner.

- Step 2** Continue with [Step 3](#) if you want to add devices; proceed to [Step 7](#) to delete devices; or click **Next** to proceed to [Step 9](#) for **3. Select Device Groups**.
- Step 3** Click **Add**, as shown in [Figure 5-14](#), to **2. Select Devices**.
- Step 4** From the resulting window, as shown in [Figure 5-15](#), “[Device Selection](#),” you can filter the choices: Device Name; Device Group; or Collection Zone from **Show Devices with**.

Figure 5-15 Device Selection

Devices associated with **Device Console**

Show Devices with matching *

Showing 1–10 of 26 records

#	☐	Device Name	Management IP Address	Type
1.	☐	newdevice1		IE2100
2.	☐	ipsec-cpe-london.cisco.com	172.29.151.10	Cisco IOS Device
3.	☐	ipsec-cpe-paris.cisco.com	172.29.151.11	Cisco IOS Device
4.	☐	ence11	192.168.115.70	Cisco IOS Device
5.	☐	ence132	192.168.115.116	Cisco IOS Device
6.	☐	ence21	192.168.115.73	Cisco IOS Device
7.	☐	ence51	192.168.115.81	Cisco IOS Device
8.	☐	ence61	192.168.115.87	Cisco IOS Device
9.	☐	ipsec-cpe-london	66.66.66.66	Cisco IOS Device
10.	☐	ipsec-cpe-ny	55.55.55.55	Cisco IOS Device

Rows per page:

- Step 5** From the devices listed, select the check box(es) for each device you want to select or select the check box in the header row to select all the devices. Then click **Select**.
- Step 6** You return to [Figure 5-14](#) with the added devices. You can repeat [Step 3](#) to [Step 5](#) to **Add** more devices, you can delete devices, as explained in [Step 7](#), or you can proceed by going to [Step 8](#).
- Step 7** To delete devices, you can filter the list in [Figure 5-14](#), by choosing a **Category: Any, Name, or Group** and entering the characters you want in **Matching** and then clicking **Filter**. From the resulting list, select the check box(es) for the devices you want to delete or select the check box in the header row to select all the devices and then click **Delete**. Select carefully, because there is no chance to confirm this deletion.
- Step 8** When you have all the devices you want, click **Next**. You proceed to **3. Select Device Groups**, starting in [Step 9](#).
- Step 9** Continue with [Step 10](#) if you want to add device groups; proceed to [Step 14](#) to delete device groups; or click **Next** to proceed to [Step 16](#) for **4. Enter EXEC Commands**.
- Step 10** Click **Add**, as shown in [Figure 5-16](#), to **3. Select Device Groups**.

Figure 5-16 Device Group Selection

IP Solution Center

Service Inventory | Service Design | Monitoring | Administration

User: admin

You Are Here: Service Inventory > Device Console

Customer: None

Device Console - EXEC Commands: Select Device Groups

Show Device Groups with Device Group Name Matching * Find

Showing 0 of 0 records

#	☐	Device Group Name	Description
Rows per page: 10 Go to page: 1 of 1 Go			
		Add	Delete

- Step 3 of 5 -

< Back Next > Finish Cancel

- Step 11** From the resulting window, as shown in Figure 5-17, “Group Association,” you can filter the choices: Device Group Name; or Description from **Show Device Groups with**.

Figure 5-17 Group Association

Groups associated with Device Console

Show Device Groups with Device Group Name matching * Find

Showing 1-1 of 1 records

#	☐	Device Group Name	Description
1.	☐	group1	

Rows per page: 10

Select Cancel

938 31

- Step 12** From the device groups listed, select the check box(es) for each device group you want to select or select the check box in the header row to select all the device groups. Then click **Select**.
- Step 13** You return to Figure 5-16 with the added device groups. You can repeat Step 10 to Step 12 to **Add** more device groups, you can delete device groups, as explained in Step 14, or you can proceed by going to Step 16.

- Step 14** To delete device groups, you can filter the list in [Figure 5-16](#), by entering the characters you want in **Group name matching** and then clicking **Filter**. From the resulting list, select the check box(es) for the devices you want to delete or select the check box in the header row to select all the devices and then click **Delete**. Select carefully, because there is no chance to confirm this deletion.
- Step 15** When you have all the device groups you want, click **Next**. You proceed to **4. Enter EXEC Commands**, starting in [Step 16](#).
- Step 16** For **4. Enter EXEC Commands**, the resulting window is shown in [Figure 5-18](#), “[Operation Commands](#).”

Figure 5-18 Operation Commands

The screenshot displays the Cisco IP Solution Center interface. At the top, the Cisco logo and 'IP Solution Center' title are visible. Navigation tabs include 'Service Inventory', 'Service Design', 'Monitoring', and 'Administration'. The 'Service Inventory' tab is active, showing a breadcrumb trail: 'Inventory and Connection Manager > Device Console'. The user is logged in as 'admin'. The main window is titled 'Device Console - EXEC Commands: Enter EXEC Command'. On the left, a 'Mode: ADDING' section shows a list of steps: '1. Choose Operation', '2. Select Devices', '3. Select Device Groups', '4. Enter EXEC Command' (selected), and '5. EXEC Commands Summary'. The main content area has an 'Input File' section with a text box and 'Browse...' and 'Load File' buttons. Below this is a large 'Commands' text area. At the bottom, navigation buttons '< Back', 'Next >', 'Finish', and 'Cancel' are present. The status bar at the very bottom shows '- Step 4 of 5 -'.

- Step 17** In [Figure 5-18](#), you can click the **Browse** button to input an existing file with Cisco IOS configuration commands. Then click the **Load File** button to put the file's information in the **Commands** field. Otherwise, you can enter the Cisco IOS configuration commands directly in the **Commands** field.
- Step 18** Click **Next** and you proceed to **5. EXEC Commands Summary**, as explained in [Step 19](#).
- Step 19** For **5. EXEC Commands Summary**, a window as shown in [Figure 5-19](#), “[EXEC Commands Summary](#),” appears.

Figure 5-19 EXEC Commands Summary

Home | Shortcuts | Account | Index | Help | About | Logout

Cisco Systems

IP Solution Center

Service Inventory | Service Design | Monitoring | Administration

User: admin

Inventory and Connection Manager | Device Console

You Are Here: Service Inventory > Device Console

Customer: None

Device Console - EXEC Commands: EXEC Command Summary

Devices:	mlp2
Device Groups:	group1
Commands:	show run

Mode: ADDING

- ☒ 1. Choose Operation
- ☒ 2. Select Devices
- ☒ 3. Select Device Groups
- ☒ 4. Enter EXEC Command
- ☒ 5. EXEC Commands Summary

- Step 5 of 5 -

< Back Next > Finish Cancel

129030

- Step 20** Click **Back** until you correct any information you want to change or click **Finish** to retrieve the information from the router. You then receive a window with the **EXEC Commands Results** and a **Status** with a green check for **Succeeded**. You can click **EXEC** or **Done**.
- Step 21** When you click **EXEC**, you return to [Step 16](#) to enter additional commands on the selected devices.
- Step 22** When you click **Done**, you return to [Figure 5-2 on page 5-2](#).

Reload

To reload (reboot) the router, do the following:

- Step 1** Navigate **Service Inventory > Device Console > Reload** and from [Figure 5-2](#) click **Next**. A window as shown in [Figure 5-20](#), “**Device Console—Reload: Select Devices**,” appears.

Figure 5-20 Device Console—Reload: Select Devices

The screenshot shows the Cisco IP Solution Center interface. At the top, there's a navigation bar with 'Service Inventory', 'Service Design', 'Monitoring', and 'Administration'. Below this, a breadcrumb trail shows 'You Are Here: Service Inventory > Device Console'. The main title is 'Device Console - Reload: Select Devices'. On the left, a sidebar titled 'Mode: ADDING' lists four steps: 1. Choose Operation (checked), 2. Select Devices (selected), 3. Select Device Groups, and 4. Reload Devices Summary. The main content area features a search bar 'Show Devices with Device Name Matching *' and a 'Find' button. Below the search bar, it says 'Showing 0 of 0 records'. A table header is visible with columns: '#', 'Device Name', 'Management IP Address', and 'Type'. Below the table header, there's a 'Rows per page: 10' dropdown and a 'Go to page: 1 of 1' field with a 'Go' button. At the bottom right of the main area are 'Add' and 'Delete' buttons. The status bar at the bottom indicates '- Step 2 of 4 -' and has '< Back', 'Next >', 'Finish', and 'Cancel' buttons.

- Step 2** Continue with [Step 3](#) if you want to add devices; proceed to [Step 7](#) to delete devices; or click **Next** to proceed to [Step 9](#) for **3. Select Device Groups**.
- Step 3** Click **Add**, as shown in [Figure 5-20](#), to **2. Select Devices**.
- Step 4** From the resulting window, as shown in [Figure 5-21](#), “**Device Selection**,” you can filter the choices: Device Name; Device Group; or Collection Zone from **Show Devices with**.

Figure 5-21 Device Selection

Devices associated with **Device Console**

Show Devices with matching

Showing 1–10 of 26 records

#	☐	Device Name	Management IP Address	Type
1.	☐	newdevice1		IE2100
2.	☐	ipsec-cpe-london.cisco.com	172.29.151.10	Cisco IOS Device
3.	☐	ipsec-cpe-paris.cisco.com	172.29.151.11	Cisco IOS Device
4.	☐	ence11	192.168.115.70	Cisco IOS Device
5.	☐	ence132	192.168.115.116	Cisco IOS Device
6.	☐	ence21	192.168.115.73	Cisco IOS Device
7.	☐	ence51	192.168.115.81	Cisco IOS Device
8.	☐	ence61	192.168.115.87	Cisco IOS Device
9.	☐	ipsec-cpe-london	66.66.66.66	Cisco IOS Device
10.	☐	ipsec-cpe-ny	55.55.55.55	Cisco IOS Device

Rows per page:

- Step 5** From the devices listed, select the check box(es) for each device you want to select or select the check box in the header row to select all the devices. Then click **Select**.
- Step 6** You return to [Figure 5-20](#) with the added devices. You can repeat [Step 3](#) to [Step 5](#) to add more devices, you can delete devices, as explained in [Step 7](#), or you can proceed by going to [Step 8](#).
- Step 7** To delete devices, you can filter the list in [Figure 5-20](#), by choosing a **Category: Any, Name, or Group** and entering the characters you want in **Matching** and then clicking **Filter**. From the resulting list, select the check box(es) for the devices you want to delete or select the check box in the header row to select all the devices and then click **Delete**. There is no chance to confirm this deletion.
- Step 8** When you have all the devices you want, click **Next**. You proceed to **3. Select Device Groups**, starting in [Step 9](#).
- Step 9** Continue with [Step 11](#) if you want to add device groups; proceed to [Step 14](#) to delete device groups; or click **Next** to proceed to [Step 16](#) for **4. Reload Devices Summary**.
- Step 10** Click **Add**, as shown in [Figure 5-22](#), to **3. Select Device Groups**.

Figure 5-22 Device Group Selection

IP Solution Center

Service Inventory | Service Design | Monitoring | Administration

User: admin

You Are Here: Service Inventory > Device Console

Customer: None

Device Console - Reload: Select Device Groups

Show Device Groups with Device Group Name Matching * Find

Showing 0 of 0 records

#	☐	Device Group Name	Description
Rows per page: 10 Go to page: 1 of 1 Go			
Add Delete			

- Step 3 of 4 -

< Back Next > Finish Cancel

- Step 11** From the resulting window, as shown in Figure 5-23, “Group Association,” you can filter the choices: Device Group Name; or Description from **Show Device Groups with**.

Figure 5-23 Group Association

Groups associated with Device Console

Show Device Groups with Device Group Name matching * Find

Showing 1-1 of 1 records

#	☐	Device Group Name	Description
1.	☐	group1	

Rows per page: 10

Select Cancel

- Step 12** From the device groups listed, select the check box(es) for each device group you want to select or select the check box in the header row to select all the device groups. Then click **Select**.
- Step 13** You return to Figure 5-23 with the added device groups. You can repeat Step 10 to Step 12 to add more device groups, you can delete device groups, as explained in Step 14, or you can proceed by going to Step 16.

- Step 14** To delete device groups, you can filter the list in [Figure 5-22](#), by entering the characters you want in **Group name matching** and then clicking **Filter**. From the resulting list, select the check box(es) for the devices you want to delete or select the check box in the header row to select all the devices and then click **Delete**. Select carefully, because there is no chance to confirm this deletion.
- Step 15** When you have all the device groups you want, click **Next**. You proceed to **4. Reload Devices Summary**, starting in [Step 16](#).
- Step 16** For **4. Reload Devices Summary**, a window as shown in [Figure 5-24](#), “**Reload Summary**,” appears.

Figure 5-24 Reload Summary

The screenshot displays the 'Device Console - Reload: Reload Devices Summary' window in the Cisco IP Solution Center. The window has a header with the Cisco Systems logo and navigation links (Home, Shortcuts, Account, Index, Help, About, Logout). Below the header, there are tabs for 'Service Inventory', 'Service Design', 'Monitoring', and 'Administration'. The 'Service Inventory' tab is active, and the 'Device Console' sub-tab is selected. The main content area shows a progress bar with four steps: 1. Choose Operation, 2. Select Devices, 3. Select Device Groups, and 4. Reload Devices Summary. Step 4 is currently selected. Below the progress bar, there are two input fields: 'Devices' with the value 'mlpe2' and 'Device Groups' which is empty. At the bottom of the window, there are four buttons: '< Back', 'Next >', 'Finish', and 'Cancel'. The status bar at the bottom indicates '- Step 4 of 4 -'.

- Step 17** Click **Back** until you correct any information you want to change or click **Finish** to submit the reload and you receive a window with the **Reload Results** and a **Status** with a green check for **Succeeded**.
- Step 18** Click **Finish** and you return to [Figure 5-2 on page 5-2](#).



Service Design

From the Home window of Cisco IP Solution Center (ISC), you receive upon logging in, click the **Service Design** tab and you receive a window as shown in [Figure 6-1](#), “[Service Design Selections](#).”

Figure 6-1 Service Design Selections



Next you can navigate to the following selections:

- **Policies, page 6-2** Create and manage Policies for licensed services.
- **Templates, page 6-2** Create and manage Templates and associated data.
- **Protocols, page 6-43** Create and manage Protocols and Protocol Bundles.- **This feature is NOT SUPPORTED in this release. -**
- **Link QoS, page 6-51** Create and manage IP Link QoS settings.
- **Network Objects, page 6-57** Create and manage network objects for security services.- **This feature is NOT SUPPORTED in this release. -**

Policies

Policies is explained in each of the *User Guides* for each of the licensed services.

Templates

Templates supports the browsing, creation, and deletion of Template Folders, Templates, and Data Files as well as the viewing of Template-generated configurations. The configuration created from the template and data file can be downloaded to devices. When creating a Service Request, you can select from the list of templates and data files and associate them with the Service Request. At Deploy time, the template and data file are instantiated and the configuration is appended or prepended to the configlet generated by ISC.

ISC provides a way to integrate a template with ISC configlets.

For a given customer edge router, you specify the following:

- template name
- template data file name
- whether the template configuration file should be appended or prepended to the ISC configlet
- whether the template configuration file is active or inactive for downloading to the edge device

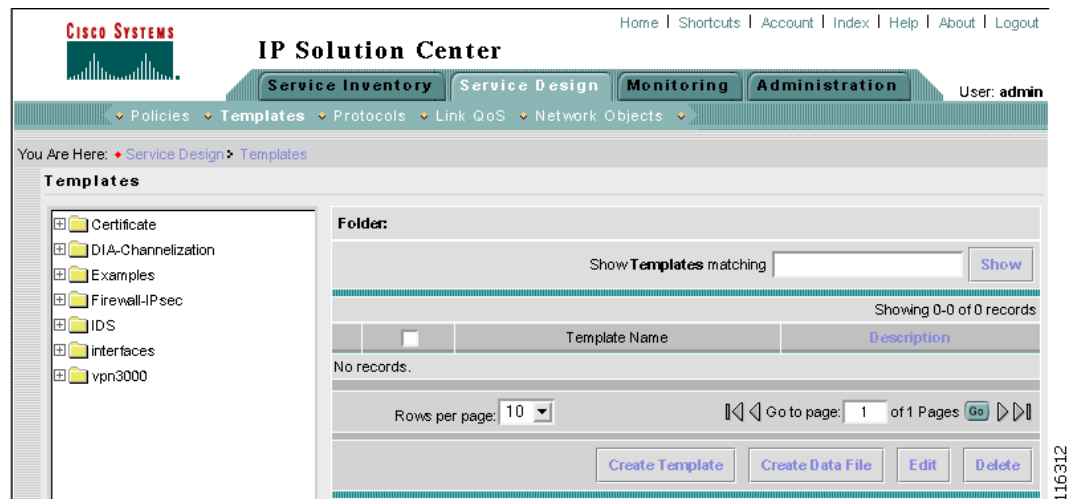
The template data files are tightly linked with the corresponding template. You can use a data file and its associated template to create a template configuration file. The template configuration file is merged with (either appended or prepended to) the ISC configlet. ISC downloads the combined ISC configlet and template configuration file to the edge device router.

- You can download a template configuration file to a router.
- You can apply the same template to multiple edge routers, assigning the appropriate template data file for each device. Each template data file includes the specific data for a particular device (for example, the management IP address or host name of each device).

To use Templates, do the following:

-
- Step 1** Navigate to **Service Design > Templates** and you receive a window as shown in [Figure 6-2](#), “[Templates](#).”

Figure 6-2 Templates



Template examples are shown in the left column. A complete list of template examples is specified in the “[Template Examples](#)” section on page 6-22. A complete list of Repository variables is shown in the “[Summary of Repository Variables](#)” section on page 6-25.

Step 2 Then you can do any of the following:

- [View Templates Tree and Data Pane, page 6-3](#)
- [Create Folders and Subfolders, page 6-4](#)
- [Create Template, page 6-5](#)
- [Create Data File, page 6-14](#)
- [Edit, page 6-19](#)
- [Delete, page 6-21](#)

View Templates Tree and Data Pane

When you navigate to **Service Design > Templates**, you receive a window as shown in [Figure 6-3, “Tree and Data Pane Structure.”](#)

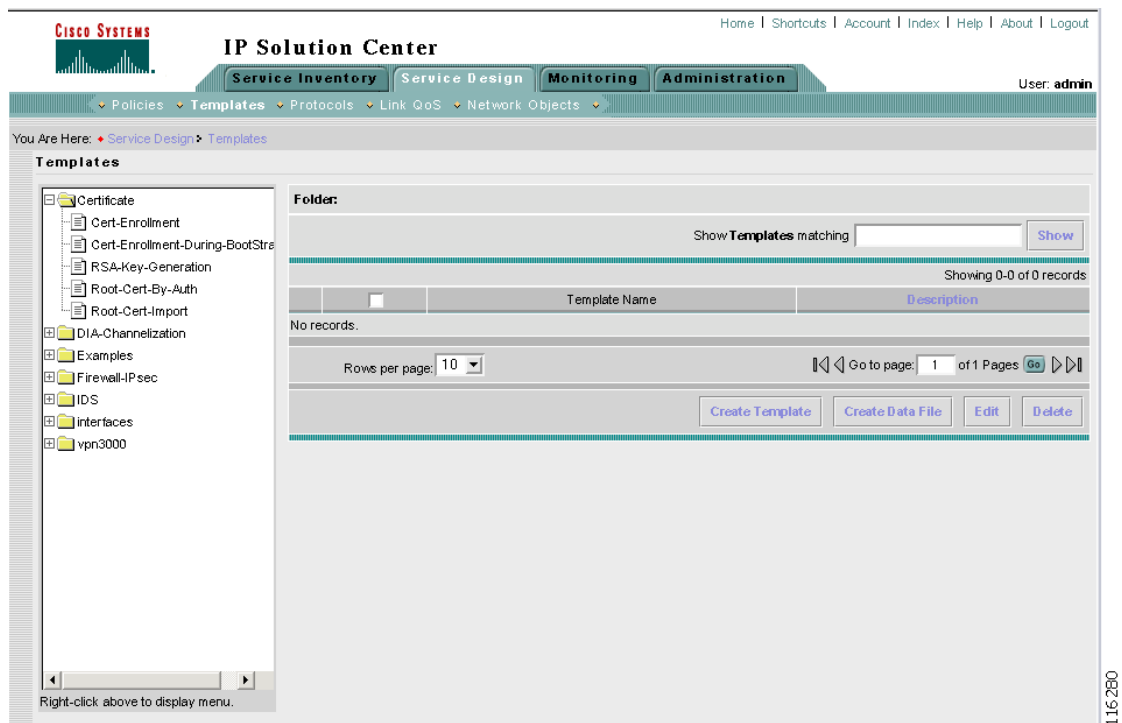
The Templates tree is in the left column. You can continue clicking the + sign next to each created folder and subfolder until you get to the last level of information. The last possible level is the template name. Data file information is not kept in the tree.

The right section of the window is the data pane. The name of the folder or template is in the upper-left corner. When you select the check box next to the template or data file information, the **Create Template**, **Create Data File**, **Edit**, or **Delete** buttons are enabled as described in the following sections.

When there are many templates in a folder or many data files in a template, the **Show Template Matching** or **Show Data File Matching** filter in the upper right hand corner of the data pane can be very useful. For example, you might just want to work with templates or data files that start with **abc**. In this case, enter **abc*** in the field and then click the **Show** button. Only the templates or data files that start with **abc** appear.

You can also **View** configurations when the table displays data files.

Figure 6-3 Tree and Data Pane Structure



Create Folders and Subfolders

To create a new folder or subfolder, do the following:

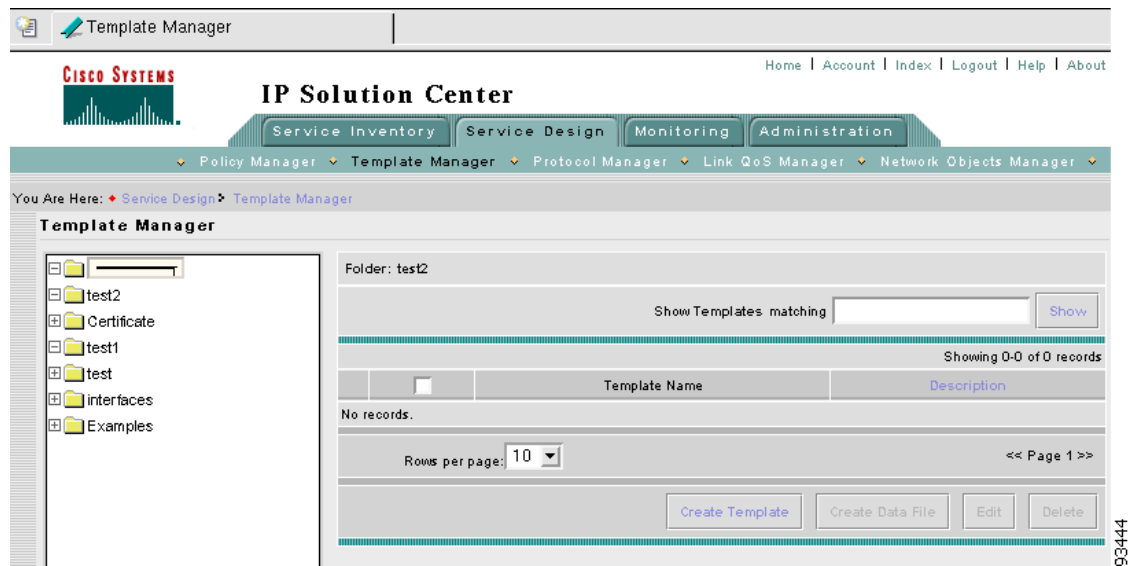
- Step 1** Navigate to **Service Design > Templates**.
- Step 2** In the **Templates** tree, right-click in the white area and select **New > Folder** to create a new folder or right-click on an existing folder or subfolder and select **New > Folder** to create a subfolder.



Note

There is no limit to the number of levels of folders and subfolders you can create.

- Step 3** In the new text field that appears in the **Templates** tree, type the new folder or subfolder name, as shown in the first entry of the **Templates** tree in [Figure 6-4, "Folder Naming."](#)

Figure 6-4 Folder Naming

Copying Folders or Subfolders

You can copy a folder or subfolder and paste it into another folder or subfolder, as follows:

- Step 1** Select a folder or subfolder and then right-click and you receive the opportunity to copy. Click **Copy**.
- Step 2** Select the folder or subfolder into which you want to paste the copied folder or subfolder and all its content. Right-click and you receive the opportunity to paste. Click **Paste**.
- Step 3** You will see the new folder or subfolder and all its content in the selected location. You can edit and rename from there.

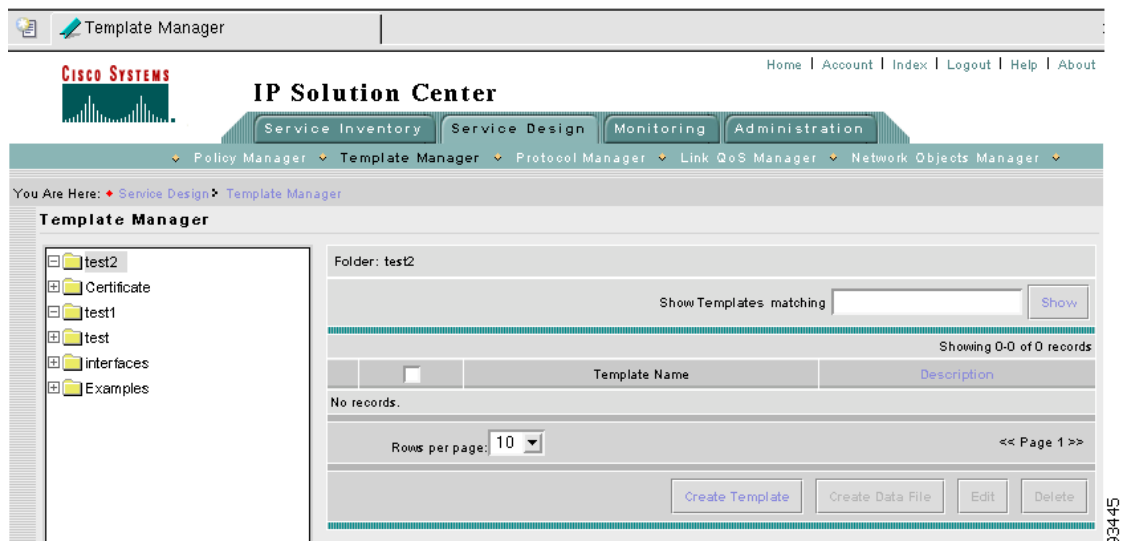
Create Template

You can either create a new template in an existing folder or you can create a new folder first and then create the template. To create a new folder, see the section [“Create Folders and Subfolders”](#).

To create a new template, do the following:

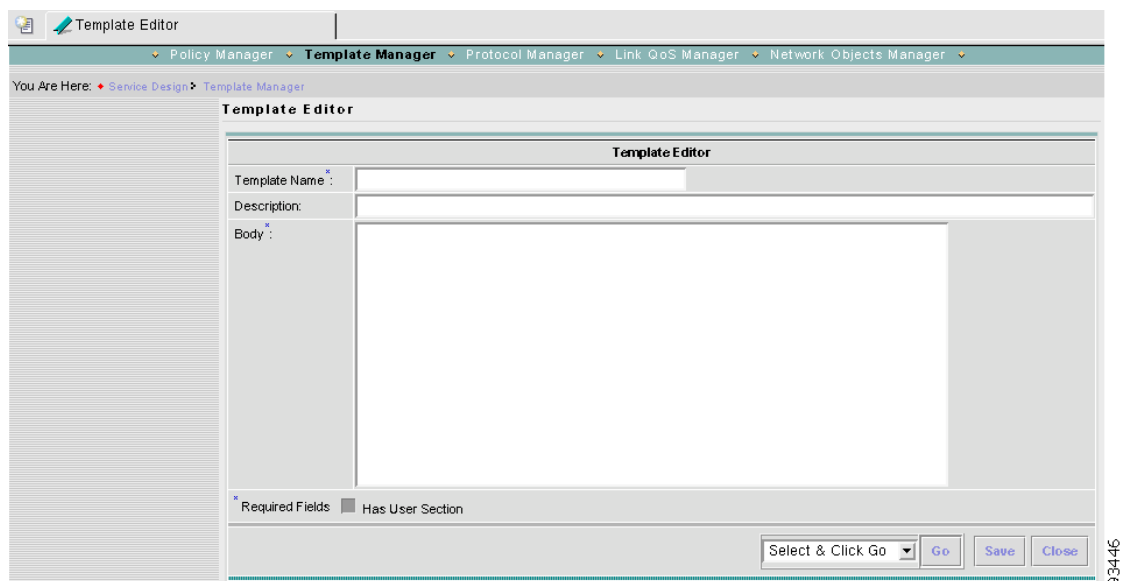
- Step 1** Navigate to **Service Design > Templates**.
- Step 2** In the **Templates** tree, click on the folder in which you want to create a new template.
- Step 3** A window appears as shown in [Figure 6-5, “Folder with Existing Templates.”](#)

Figure 6-5 Folder with Existing Templates



Step 4 Click the **Create Template** button and you receive a window as shown in Figure 6-6, “Template Editor.”

Figure 6-6 Template Editor



Step 5 Enter the following:

- **Template Name** (required) This must be a unique name within a folder. This name must begin with an alphabetic character and can only contain alphanumeric characters, underscores, and hyphens.
- **Description** (optional) You can enter any description here.
- **Body** (required) Enter the configuration text, Velocity template language directives, and variables that you want included.

**Note**

The Velocity template language is explained at <http://jakarta.apache.org/velocity/user-guide.html>.

An example template is shown in [Figure 6-7, “Example Template.”](#)

Figure 6-7 Example Template

The screenshot shows the 'Template Editor' window. It has a title bar 'Template Editor' and a menu bar. Below the menu bar, there are three fields: 'Template Name:' with the value '/Examples/CEWanCOS', 'Description:', and 'Body:'. The 'Body:' field contains the following code:

```
## This template demonstrate if-else statements, repeat statements,
## expression, 1 dimensional variables

access-list 103 permit host $CE-lo0 $mgt-prefix $mgt-mask
access-list 104 permit $protocol.get(0)
!
#foreach ($class in $class-maps)
  class-map match-all $class
    match $class-match.get($velocityCount)
  #end
!
policy-map $service-policy
#foreach ($class in $class-maps)
  class $class
    #if ($class == "business")
```

At the bottom of the window, there is a checkbox labeled '*Required Fields' and another labeled 'Has User Section'. Below these are three buttons: 'Select & Click Go', 'Go', 'Save', and 'Close'. A vertical text '93447' is visible on the right side of the window.

ISC has the template system predefined variable **\$TMSystem** that can be used within the template body text to access template system functions. The syntax is as follows, where, \$ipAddrMask is a string that contains an IP address and its mask in the format of: 10.33.4.5/30:

\$TMSystem.getAddr (\$ipAddrMask) returns: 10.33.4.5

\$TMSystem.getMask (\$ipAddrMask) returns: 255.255.255.252

\$TMSystem.getReverseMask (\$ipAddrMask) returns: 0.0.0.3

\$TMSystem.getNetworkAddr (\$ipAddrMask) returns: 10.33.4.4

\$TMSystem.getClassfulNetworkAddr (\$ipAddrMask) returns: 10.0.0.0

Step 6 Click the **Select & Click Go** drop-down button. If you want to validate the information you entered in [Step 5](#), select **Validate** and then click the **Go** button. Otherwise, select **Variables** and then click the **Go** button and you receive a window as in [Figure 6-8, Template Variables](#)".

Figure 6-8 Template Variables

Template Variables – Netscape				
Showing 1-10 of 34 records				
		Variable	Type	Description
1.	☐	class-match	String	
2.	☐	bestEffort-pct	String	
3.	☐	manag-pct	String	
4.	☐	goldBurst	Integer	
5.	☐	business-weighting-constant	Integer	
6.	☐	silverBurst	String	
7.	☐	be-mark	String	
8.	☐	rp-que-limit	String	
9.	☐	be-min-thresh	String	
10.	☐	GESubInterface	String	

Rows per page: 10 Go to page: 1 of 4 Pages

Step 7 Click the radio button for the Variable you want to edit and click **Edit**. You receive a window as in [Figure 6-9](#), “Variable Definition—Type String.”

Figure 6-9 Variable Definition—Type String

Variable a

Type: String

Description:

Required: ☒

Dimension: 0

Default:

Pattern:

Minimum Length:

Maximum Length:

Available Values (comma separated):

* Required Fields

Step 8 In [Figure 6-9](#), click the drop-down menu for **Type** to receive the following choices:

- **String** Proceed to [Step 9](#).
- **Integer** Proceed to [Step 10](#).

- **Float** Proceed to [Step 11](#).
- **IPv4 Address** Proceed to [Step 12](#).
- **Sub-Template** Proceed to [Step 13](#).
- **Dynamic Java Class** Proceed to [Step 14](#).
- **Dynamic URL** Proceed to [Step 15](#).

Step 9 The default Type to appear is **String**, a combination of ASCII characters considered as a group. The resulting Variable window is shown in [Figure 6-9](#) and its attributes are as follows:

- **Description** (optional) You can enter any descriptive statement about this variable here.
- **Required** Leave the default of the selected check box if this variable is required. Otherwise, deselect it.
- **Dimension** Choose **0** (default), which indicates a scalar or enum variable; choose **1**, in which case the variable becomes a one-dimensional array; or choose **2**, in which case the variable becomes a two-dimensional array.
- **Default** (optional) If there is a default value for the specified variable, specify it here. If you also have **Available Values** defined, this default value must be an **Available Value**.
- **Pattern** (optional) Specify a regular expression pattern of the string. For example, a pattern of **isc[0-9]+** defines a string that starts with **isc** followed by one or more digits from **0** to **9**.
- **Minimum Length** (optional) If you specify a minimum length, the string cannot be less than the length specified here.
- **Maximum Length** (optional) If you specify a maximum length, the string cannot exceed the length specified here.
- **Available Values** (optional) Enter string values for this variable. Separate the values by commas.

After you enter all the data, click **OK** to accept this information for the specified variable; continue editing all variables you want to change in this same way, then click **OK** in a window such as [Figure 6-8](#), which now includes these updated variables; click **Save** and then **Close** or click **Close** and when asked, agree to **Save** for a window such as [Figure 6-6](#). Create a Data File is shown in the “[Create Data File](#)” section on page 6-14, **Edit** is shown in the “[Edit](#)” section on page 6-19, and **Delete** is shown in the “[Delete](#)” section on page 6-21.

Step 10 When you choose the Type **Integer**, a whole number, the resulting Variable window is shown in [Figure 6-10](#) and its attributes are as follows:

- **Description** (optional) You can enter any descriptive statement about this variable here.
- **Required** Leave the default of the selected check box if this variable is required. Otherwise, deselect it.
- **Dimension** Choose **0** (default), which indicates a scalar or enum variable; choose **1**, in which case the variable becomes a one-dimensional array; or choose **2**, in which case the variable becomes a two-dimensional array.
- **Default** (optional) If there is a default value for the specified variable, specify it here. If you also have **Available Values** defined, this default value must be an **Available Value**.
- **Minimum Value** (optional) If you specify a minimum value, the integer cannot be less than the value specified here.
- **Maximum Value** (optional) If you specify a maximum value, the integer cannot exceed the value specified here.
- **Available Values** (optional) Enter integer values for this variable. Separate the values by commas.

After you enter all the data, click **OK** to accept this information for the specified variable; continue editing all variables you want to change in this same way, then click **OK** in a window such as [Figure 6-8](#), which now includes these updated variables; click **Save** and then **Close** or click **Close** and when asked, agree to **Save** for a window such as [Figure 6-6](#). Create a Data File is shown in the “[Create Data File](#)” section on page 6-14, **Edit** is shown in the “[Edit](#)” section on page 6-19, and **Delete** is shown in the “[Delete](#)” section on page 6-21.

Figure 6-10 Variable Definition—Type Integer

The screenshot shows a dialog box titled "Variable a". It contains the following fields and controls:

- Type:** A dropdown menu set to "Integer".
- Description:** An empty text input field.
- Required:** A checked checkbox.
- Dimension:** A dropdown menu set to "0".
- Default:** An empty text input field.
- Minimum Value:** An empty text input field.
- Maximum Value:** An empty text input field.
- Available Values (comma separated):** An empty text input field.
- Buttons:** "OK" and "Close" buttons at the bottom right.
- Legend:** A small blue asterisk icon next to the text "Required Fields" at the bottom left.

Step 11 When you choose the Type **Float**, a number that has no fixed number of digits before or after the decimal point, the resulting Variable window is shown in [Figure 6-11](#) and its attributes are as follows:

- **Description** (optional) You can enter any descriptive statement about this variable here.
- **Required** Leave the default of the selected check box if this variable is required. Otherwise, deselect it.
- **Dimension** Choose **0** (default), which indicates a scalar or enum variable; choose **1**, in which case the variable becomes a one-dimensional array; or choose **2**, in which case the variable becomes a two-dimensional array.
- **Default** (optional) If there is a default value for the specified variable, specify it here. If you also have **Available Values** defined, this default value must be an **Available Value**.
- **Minimum Value** (optional) If you specify a minimum value, the floating point value cannot be less than the value specified here.
- **Maximum Value** (optional) If you specify a maximum value, the floating point value cannot exceed the value specified here.
- **Available Values** (optional) Enter floating point values for this variable. Separate the values by commas.

After you enter all the data, click **OK** to accept this information for the specified variable; continue editing all variables you want to change in this same way, then click **OK** in a window such as [Figure 6-8](#), which now includes these updated variables; click **Save** and then **Close** or click **Close** and when asked, agree to **Save** for a window such as [Figure 6-6](#). Create a Data File is shown in the “[Create Data File](#)” section on page 6-14, **Edit** is shown in the “[Edit](#)” section on page 6-19, and **Delete** is shown in the “[Delete](#)” section on page 6-21.

Figure 6-11 Variable Definition—Type Float

Variable a	
Type:	Float
Description:	
Required:	☒
Dimension:	0
Default:	
Minimum Value:	
Maximum Value:	
Available Values (comma separated):	
OK Close	
* Required Fields	

Step 12 When you choose the Type **IPv4**, the resulting Variable window is shown in [Figure 6-12](#) and its attributes are as follows:

- **Description** (optional) You can enter any descriptive statement about this variable here.
- **Required** Leave the default of the selected check box if this variable is required. Otherwise, deselect it.
- **Dimension** Choose **0** (default), which indicates a scalar or enum variable; choose **1**, in which case the variable becomes a one-dimensional array; or choose **2**, in which case the variable becomes a two-dimensional array.
- **Default** (optional) If there is a default value for the specified variable, specify it here. If you also have **Available Values** defined, this default value must be an **Available Value**.
- **Subnet Mask** (optional) Enter a valid subnet mask.
- **Class** (optional) Enter the class of the IP address. The options are: **A**, **B**, or **C**.
- **Available Values** (optional) Enter IPv4 values for this variable. Separate the values by commas.

After you enter all the data, click **OK** to accept this information for the specified variable; continue editing all variables you want to change in this same way, then click **OK** in a window such as [Figure 6-8](#), which now includes these updated variables; click **Save** and then **Close** or click **Close** and when asked, agree to **Save** for a window such as [Figure 6-6](#). Create a Data File is shown in the [“Create Data File”](#) section on page 6-14, **Edit** is shown in the [“Edit”](#) section on page 6-19, and **Delete** is shown in the [“Delete”](#) section on page 6-21.

Figure 6-12 Variable Definition — Type IPv4

The image shows a 'Variable a' definition window. It contains the following fields and values:

- Type: IPv4 Address (dropdown)
- Description: (empty text box)
- Required: ☒
- Dimension: 0 (dropdown)
- Default: (empty text box)
- Subnet Mask: (empty text box)
- Class: Undefined (dropdown)
- Available Values (comma separated): (empty text box)

At the bottom right are 'OK' and 'Close' buttons. At the bottom left is a legend: 'Required Fields' with a blue asterisk icon.

Step 13 When you choose the Type **Sub-Template**, you instantiate one subtemplate into the Main template. The resulting Variable window is shown in [Figure 6-13](#) and its attributes are as follows:

- **Description** (optional) You can enter any descriptive statement about this variable here.
- **Required** Leave the default of the selected check box if this variable is required. Otherwise, deselect it.
- **Location** (required) Enter the full path name of the parent template. For example `/test2/testyy`.

The variable `varName` is defined as the subtemplate type (by selecting **Variables** and clicking **Go**). The Sub-Template defined earlier is called and you must provide the subtemplate path. The syntax is as follows:

`$<varName>.callWithDatafile (<DatafileName>)`

After you enter all the data, click **OK** to accept this information for the specified variable; continue editing all variables you want to change in this same way, then click **OK** in a window such as [Figure 6-8](#), which now includes these updated variables; click **Save** and then **Close** or click **Close** and when asked, agree to **Save** for a window such as [Figure 6-6](#). Create a Data File is shown in the “[Create Data File](#)” section on page 6-14, **Edit** is shown in the “[Edit](#)” section on page 6-19, and **Delete** is shown in the “[Delete](#)” section on page 6-21.

Figure 6-13 Variable Definition—Type Sub-Template

Step 14 When you choose the Type **Dynamic Java Class**, the resulting Variable window is shown in [Figure 6-14](#) and its attributes are as follows:

- **Description** (optional) You can enter any descriptive statement about this variable here.
- **Required** Leave the default of the selected check box if this variable is required. Otherwise, deselect it.

The variable varName is defined as the Dynamic Java Class type (by selecting **Variables** and clicking **Go**). The syntax is as follows:

```
$<varName>.<method_name_in_Java_class> ([<parameters>])
```

After you enter all the data, click **OK** to accept this information for the specified variable; continue editing all variables you want to change in this same way, then click **OK** in a window such as [Figure 6-8](#), which now includes these updated variables; click **Save** and then **Close** or click **Close** and when asked, agree to **Save** for a window such as [Figure 6-6](#). Create a Data File is shown in the “[Create Data File](#)” section on page 6-14, **Edit** is shown in the “[Edit](#)” section on page 6-19, and **Delete** is shown in the “[Delete](#)” section on page 6-21.

Figure 6-14 Variable Definition—Type Dynamic Java Class

Step 15 When you choose the Type **Dynamic URL**, the resulting Variable window is shown in [Figure 6-15](#) and its attributes are as follows:

- **Description** (optional) You can enter any descriptive statement about this variable here.
- **Required** Leave the default of the selected check box if this variable is required. Otherwise, deselect it.

The variable `varName` is defined as the Dynamic URL type (by selecting **Variables** and clicking **Go**). The syntax is as follows:

```
$<varName>.callURL (<url-address>)
```

After you enter all the data, click **OK** to accept this information for the specified variable; continue editing all variables you want to change in this same way, then click **OK** in a window such as [Figure 6-8](#), which now includes these updated variables; click **Save** and then **Close** or click **Close** and when asked, agree to **Save** for a window such as [Figure 6-6](#). Create a Data File is shown in the [“Create Data File” section on page 6-14](#), **Edit** is shown in the [“Edit” section on page 6-19](#), and **Delete** is shown in the [“Delete” section on page 6-21](#).

Figure 6-15 Variable Definition—Type Dynamic URL

The screenshot shows a dialog box titled "Variable a". It has a "Type:" dropdown menu set to "Dynamic URL". Below it is a "Description:" text field. Underneath is a "Required:" checkbox which is checked. At the bottom right are "OK" and "Close" buttons. A status bar at the bottom left says "* Required Fields". On the right side of the dialog, there is a vertical label "93455".

Copying Templates

You can copy a template and paste it into another folder, as follows:

-
- Step 1** Select a template and then right-click and you receive the opportunity to copy. Click **Copy**.
 - Step 2** Select the folder into which you want to paste the copied template and all its data files. Right-click and you receive the opportunity to paste. Click **Paste**.
 - Step 3** You will see the new template and all its data files in the selected location. You can edit and rename from there.
-

Create Data File

You can create a new data file from an existing template. If the template you want is not available, go to the [“Create Template” section on page 6-5](#).

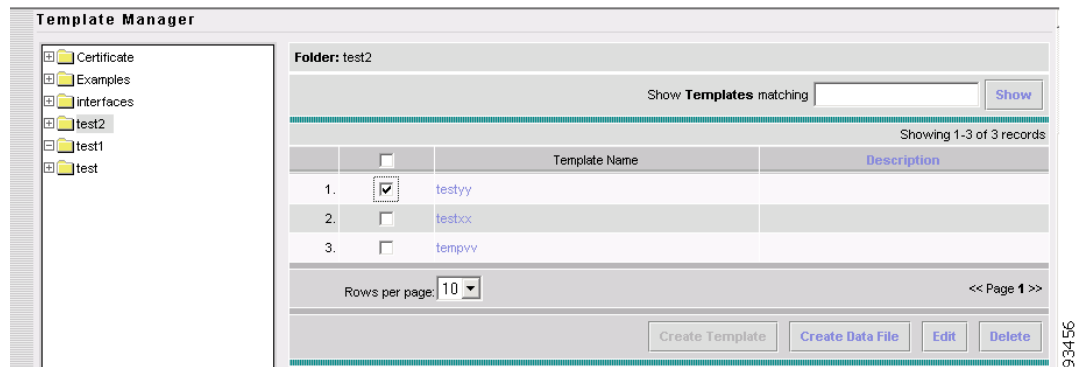
To create a data file, do the following:

-
- Step 1** Navigate to **Service Design > Templates**.
 - Step 2** In the **Templates** tree in the left part of your window, do one of the following
 1. Left-click on the folder or subfolder in which the template for which you want to create a data file exists or

- Click on the + next to the folder of choice and then click on the template for which you want to create a data file.

Step 3 If you chose 1. in [Step 2](#), a window appears as shown in [Figure 6-16](#), “Choose Existing Template > Create Data File.”

Figure 6-16 Choose Existing Template > Create Data File

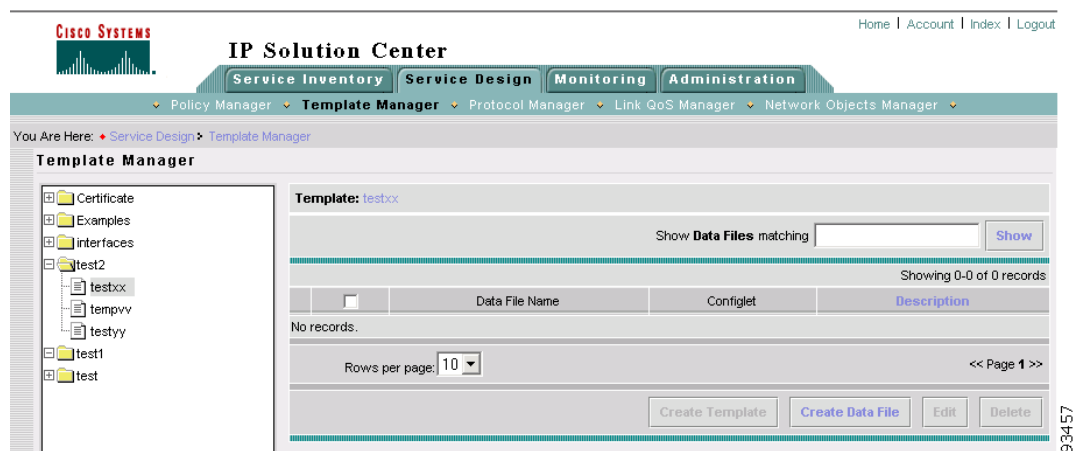


Select the check box for the template for which you want to create a data file and click **Create Data File**. Then proceed to [Step 5](#).

Otherwise, proceed to [Step 4](#).

Step 4 If you chose 2. in [Step 2](#), the buttons appear as shown in [Figure 6-17](#), “Choose Existing Template > Create Data File.”

Figure 6-17 Choose Existing Template > Create Data File



Click **Create Data File** and proceed to [Step 5](#).

Step 5 An example of a window that appears is shown in [Figure 6-18](#), “Template Data File Editor.”

Figure 6-18 Template Data File Editor

IP Solution Center

Service Inventory Service Design Monitoring Administration

Policy Manager Template Manager Protocol Manager Link QoS Manager Network Object

You Are Here: > Service Design > Template Manager

Data File Editor

Template Data File Editor

General

Template: test2/Test-Dimension

Data File Name: Data1

Description:

Variables

b : [first, second, third] Edit Vars

a : testaaaa (String) Vars

c : [[first row-first column,222],[...]] Edit Vars

* Required Fields

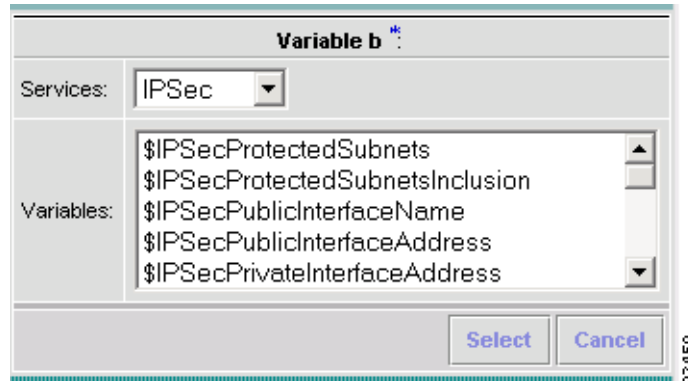
Step 6 In the **General** area, fill in the following:

- **Data File Name** (required) This must be a unique name. This name must begin with an alphabetic character and can only contain alphanumeric characters and the underscore.
- **Description** (optional) Enter any description that helps you identify this data file.

Step 7 In the example in Figure 6-18, in the **Variables** area, **a** is a string variable (**Dimension** defined when the template was created was **0**); **b** is a one-dimensional array (**Dimension** defined when the template was created was **1**); and **c** is a two-dimensional array (**Dimension** defined when the template was created was **1**).

If **a** is a Dynamic Java Class variable, you *must* enter the entire Java Class package name. For example: com.cisco.isc.class_name.

Step 8 If you click **Vars** as shown in Figure 6-18, you receive a window as shown in Figure 6-19, “Template Data File Editor.”

Figure 6-19 *Template Data File Editor*

Click the **Services** drop-down menu to have access to variables for:

- **IPsec - NOT SUPPORTED in this release. -**
- **IPsecRA (IPsec Remote Access) - NOT SUPPORTED in this release. -**
- **NAT - NOT SUPPORTED in this release. -**
- **MPLS**
- **L2VPN**

Then click the entry in **Variables** that you want to use and click **Select**.

If you have a **0** dimensional entry (set as **Dimension 0** when creating a template), you can only enter variables in the provided field.

Step 9 When you click **Edit**., as shown in [Figure 6-18](#), the resulting window depends on whether you are editing a **1** or **2** dimensional array.

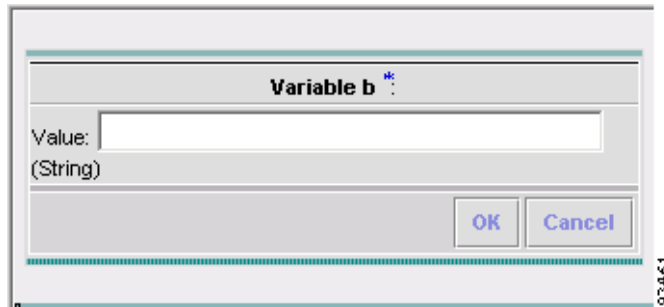
Proceed to [Step 10](#) for information about a **1** dimensional array.

Proceed to [Step 13](#) for information about a **2** dimensional array.

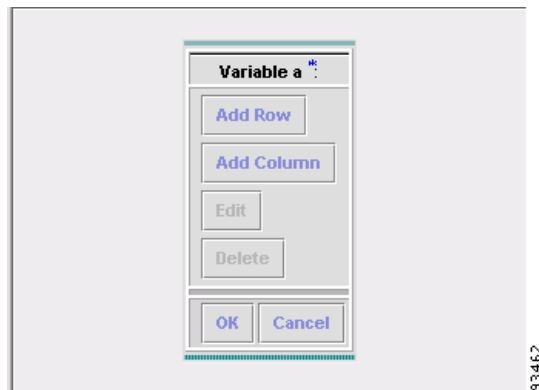
Step 10 For a one-dimensional array (set as **Dimension 1** when creating the template), when you click **Edit**, you receive a window as shown in [Figure 6-20](#), “Editing a One-Dimensional Array.”

Figure 6-20 *Editing a One-Dimensional Array*

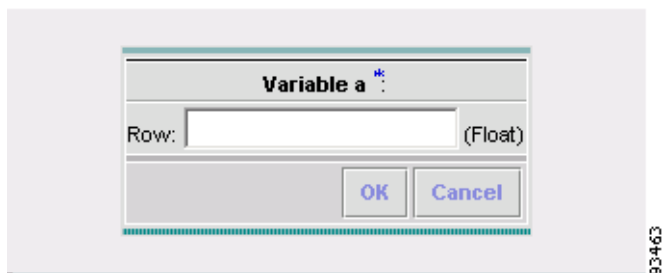
Step 11 To add a variable, click **Add** and a window, as shown in [Figure 6-21](#), “Adding a Variable,” appears in which you can add the variable. Then click **OK**.

Figure 6-21 Adding a Variable

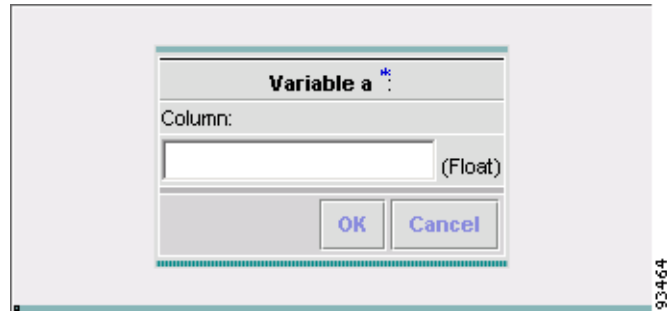
- Step 12** To edit or delete a variable, highlight the variable in [Figure 6-20](#) and click **Edit** or **Delete**. For **Edit** you receive a figure as in [Figure 6-21](#). Then click **OK**. For **Delete**, *be sure* you want to delete. After you click **Delete**, it automatically occurs and the window is updated. Proceed to [Step 19](#).
- Step 13** For a two-dimensional array (set as **Dimension 2** when creating the template), when you click **Edit**, you receive a window as shown in [Figure 6-22](#), “Editing a Two-Dimensional Array.”

Figure 6-22 Editing a Two-Dimensional Array

- Step 14** Click **Add Row** in [Figure 6-22](#) and a window, as shown in [Figure 6-23](#), “Enter Row Information,” appears. Enter a value and click **OK**.

Figure 6-23 Enter Row Information

- Step 15** Click **Add Column** in [Figure 6-22](#) and a window as shown in [Figure 6-24](#), “Enter Column Information,” appears. Enter a value and click **OK**.

Figure 6-24 Enter Column Information

Step 16 A resulting window, as shown in [Figure 6-25](#), “Two-Dimensional Array Results,” appears.

Figure 6-25 Two-Dimensional Array Results

- Step 17** You can select any of the check boxes (toggles) and you can then **Edit** or **Delete** that row or column. You can also continue to **Add Row** and **Add Column** as shown in [Step 15](#) and [Step 16](#), respectively.
- Step 18** When you complete setting up your two-dimensional array, click **OK** in [Figure 6-25](#).
- Step 19** A window as shown in [Figure 6-18](#) is updated to reflect the new data file information.
- Step 20** You can then click **Save** and then **Close** to save this information and close this file; click **Configure** to show the configuration file; or click **Close** and then be sure to click **OK**, if you want to save the information you have created. If you do not want to save this information, click **Close** and then click **Cancel**.

Edit

To edit a Template or Data File, do the following:

- Step 1** Navigate to **Service Design > Templates**.
- Step 2** In the **Templates** tree, left-click on the folder or subfolder in which the template you want to edit exists or the template in which the data file you want to edit exists. Alternatively, when the name in the upper left corner of the data pane is a template, you can click on the template name to edit the template.

- Step 3** To edit a template, a window appears as shown in [Figure 6-26](#), “Choose Existing Template > Edit.” To edit a data file, a window appears as shown in [Figure 6-27](#), “Choose Existing Data File > Edit.”

Figure 6-26 Choose Existing Template > Edit

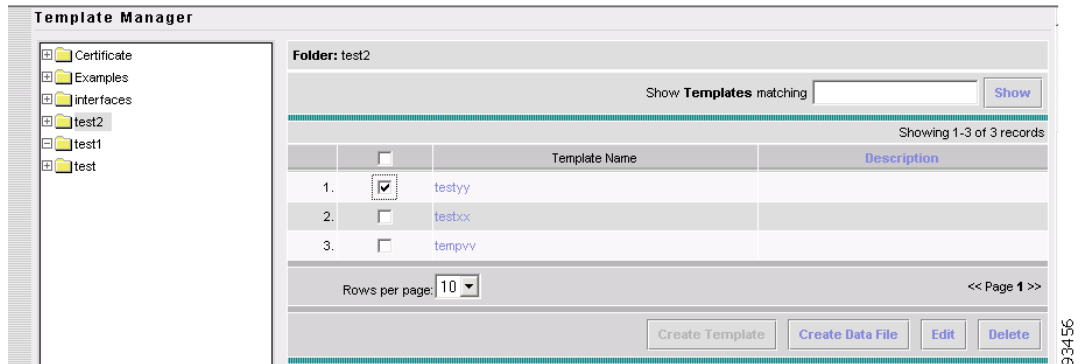
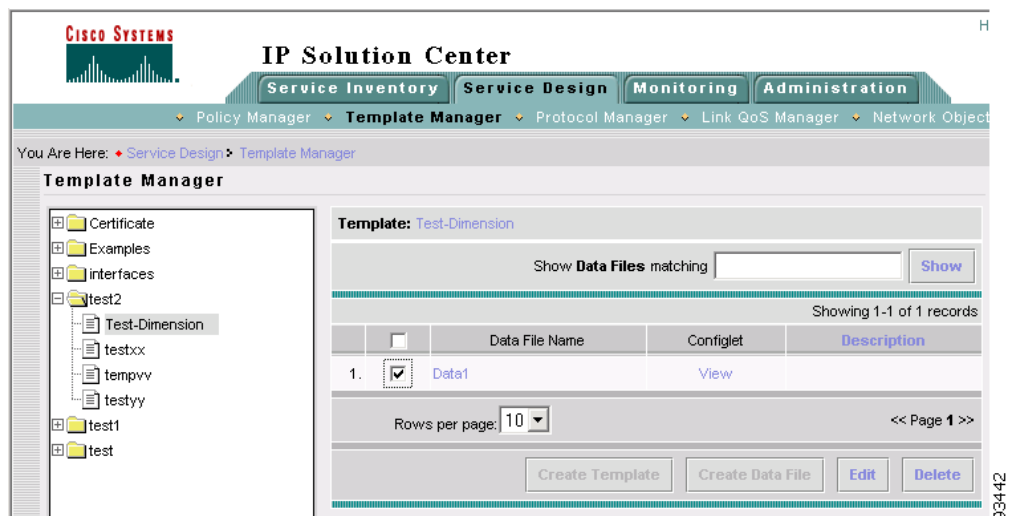


Figure 6-27 Choose Existing Data File > Edit



- Step 4** Select the check box for the template or data file you want to edit.



Note

For a data file, there is a **Configlet** column in which you can click **View** to view the configuration file.

- Step 5** Click **Edit**.

- Step 6** When editing a template, you receive a window as shown in [Figure 6-6](#), “Template Editor.” Then proceed as in the “Create Template” section on page 6-5. When editing a data file, you receive a window as shown in [Figure 6-17](#), “Choose Existing Template > Create Data File.” Then proceed as in [Step 5](#) in the “Create Data File” section on page 6-14.

Delete

To delete a Template or Data File, do the following:

- Step 1** Navigate to **Service Design > Templates**.
- Step 2** In the **Templates** tree, left-click on the folder or subfolder in which the template you want to delete exists or the template in which the data file you want to delete exists.
- Step 3** To delete a template, a window appears as shown in [Figure 6-28](#), “Choose Existing Template > Delete.” To delete a data file, a window appears as shown in [Figure 6-29](#), “Choose Existing Data File > Delete.”

Figure 6-28 Choose Existing Template > Delete

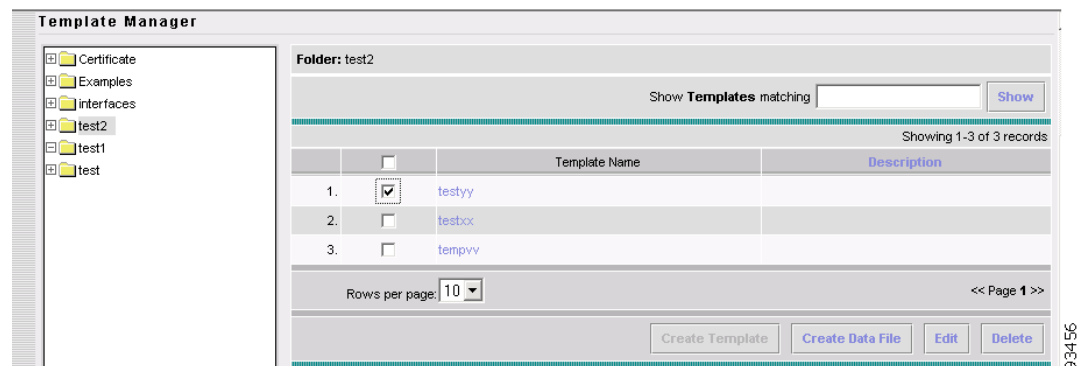
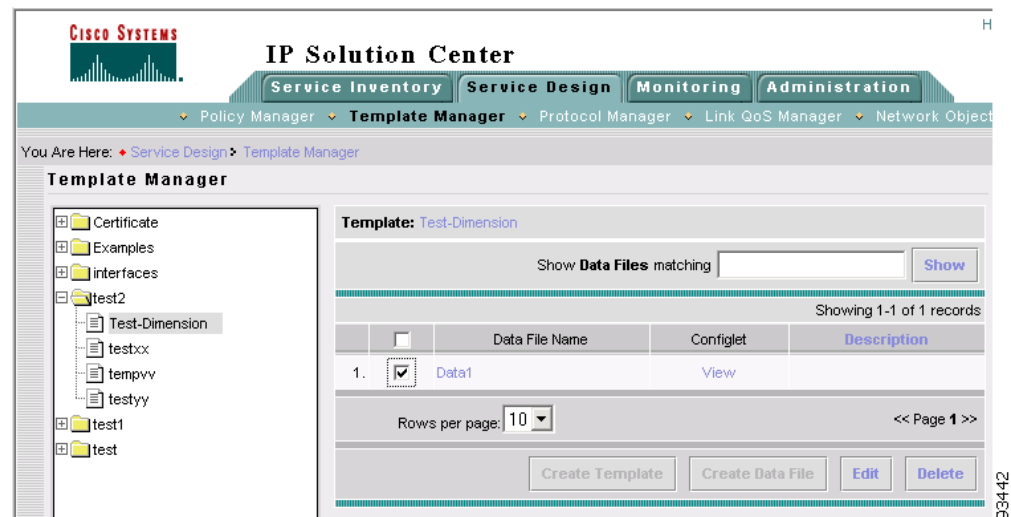


Figure 6-29 Choose Existing Data File > Delete



- Step 4** Select the check box for the template or data file you want to delete.



Note

For a data file, there is a **Configlet** column in which you can click **View** to view the configuration file.

- Step 5** Click **Delete**.
- Step 6** You receive an updated window as shown in [Figure 6-28](#), “Choose Existing Template > Delete” or [Figure 6-29](#), “Choose Existing Data File > Delete” with the deleted template or data file no longer available.

Template Examples

In the left column, the hierarchy pane, of **Service Design > Templates**, as shown in [Figure 6-2](#), “**Templates**,” template examples appear. See [Table 6-1](#), “**Template Examples and Their Descriptions**.”

Table 6-1 *Template Examples and Their Descriptions*

Folder	Template	Description
Certificate	Cert-Enrollment	Cisco IOS commands to generate private/public key pair for this router.
	Cert-Enrollment-During-BootStrap	Example that generates the PKSC12 package for the specified device and imports the package to the device. Both runscep and runscep_ms take the following parameter. \$ms_ca_server indicates if the CA server is Microsoft Certificate Server. Usage: /vob/ntg/dev/bin/runscep <FQDN of Router> <URL of CA Server> <challenge password> <common name> <privatekey size> [client-email]
	RSA-Key-Generation	Cisco IOS commands to generate private/public key pair for this router.
	Root-Cert-By-Auth	Sample Cisco IOS template to authenticate root certificate server and obtain root certificate.
	Root-Cert-Import	Sample Cisco IOS template to import root certificate to the router.
DIA-Channelization	10K-CHOC12-ST51-PATH	Sample template to break down channelized OC12 to STS-1 paths.
	10K-CT3-CHANNELIZED	Sample template creates T1 out of channelized T3 line card.
	10K-CT3-UNCHANNELIZED	Sample template Creates either a fullrate T3 or a subrate T3 interface out of a channelized T3.
	PA-MC-E3-CHANNELIZED	Sample template Creates E1 (channel groups) out of E3.
	PA-MC-STM1-AU3-CHANNELIZE	Sample template Creates E1 (channel groups) out of TUG-2. This template uses AU-3 AUG mapping that further creates TUG-2s.

Table 6-1 Template Examples and Their Descriptions (continued)

Folder	Template	Description
	PA-MC-STM1-AU4-CHANNELIZE	Sample template Creates E1 (channel groups) out of TUG-2. This template uses AU-4 AUG mapping that creates TUG-3s and TUG-2s.
	PA-MC-T3-CHANNELIZED	Sample template Creates T1 (channel groups) out of T3.
Examples	AccessList	Demonstrates templates with nested repeat loop and multi-dimension variable.
	AccessList1	Demonstrates the simplest template variable substitution.
	CEWanCOS	Demonstrates if-else statements, repeat statements, mathematical expressions, and one-dimensional variables.
Firewall-IPsec - NOT SUPPORTED in this release. -	Permit-IPsec-IOS	Allow only IPsec traffic, management traffic, and data traffic that came through an IPsec tunnel on a Cisco IOS router.
	Permit-IPsec-PIX	Sample Cisco IOS template to enroll with root certificate server and obtain certificate of this router.
IDS/ Audit	Set-Audit_Rule	Set up ACLs for the audit rule. Set up the audit rule for signatures of information and attack types. Apply the audit rule to the interfaces.
IDS/ Initialization	Set-Thresholds	Set the threshold beyond which spamming in e-mail messages is suspected. Set the threshold beyond which queued events are dropped from the event queue for sending to the NetRanger Director.
IDS/ Notification	Notify-Director	Specify the messages in NetRanger format for event notification. Specify the local Post Office parameters used when sending event notification to the NetRanger Director. Specify Post Office parameters for the NetRanger Director receiving event notification from the router.
	Notify-Syslog-Console	Specify the messages in the syslog format for event notification. Specify the syslog console as the event destination.
	Notify-Syslog-Server	Specify the messages in the syslog format for event notification. Specify the syslog server as the event destination.

Table 6-1 *Template Examples and Their Descriptions (continued)*

Folder	Template	Description
IDS/ Signature	Disable-Signatures	Disable individual signatures.
	Enable-Signatures	Enable a list of signatures or qualify the audit of the signatures with an access control list.
interfaces - NOT SUPPORTED in this release. -	noshutdownIf	Brings up all nonsecured interfaces of a given device in the IPsec Service Request.
	shutdownIf	Shuts down all nonsecured interfaces of a given device in the IPsec Service Request.
vpn3000/ Events - NOT SUPPORTED in this release. -	EmailRecipient-Create	Creates an e-mail recipient record.
	EmailRecipient-Modify	Modifies an e-mail recipient record.
	EventClass-Create	Sets up EventClass record parameters.
	EventClass-Modify	Modifies a particular event class.
	FTPLogBackup	Sets up FTP log back up parameters.
	General-Event	Sets up general event parameters.
	SMTPServer-Create	Creates an Simple Mail Transfer Protocol (SMTP) server.
	SMTPServer-Modify	Modifies SMTP server parameters.
	SyslogServer-Create	Sets up syslog server record parameters.
	SyslogServer-Modify	Modifies syslog server record parameters.
	TrapDestination-Create	Sets up Trap Destination record parameters.
	TrapDestination-Modify	Modifies a particular trap destination.
vpn3000/ Routing - NOT SUPPORTED in this release. -	Create-OSPFArea	Creates general OSPF Area parameters.
	Default-Gateway	Sets up a default gateway.
	Ethernet-OSPF	Configures an Open Shortest Path First (OSPF) interface of a particular Ethernet interface.
	Ethernet-RIP	Sets up a Routing Information Protocol (RIP) protocol for a particular Ethernet interface.
	General-OSPF	Sets up General OSPF parameters.
	Modify-OSPFArea	Modifies a particular OSPF area.

Table 6-1 Template Examples and Their Descriptions (continued)

Folder	Template	Description
	Static-Routes	Configures static route records.
	VRRP	Sets up VRRP redundancy
vpn 3000/ Servers - NOT SUPPORTED in this release. -	DHCP-Server	Sets up Dynamic Host Configuration Protocol (DHCP) server parameters.
	DHCP-Server-Modify	Modifies DHCP server parameters.
	DNS-Server	Sets up Domain Name System (DNS) server parameters.
	FTP-Server	Sets up File Transfer Protocol (FTP) server parameters.
	HTTP-Server	Sets up Hypertext Transfer Protocol (HTTP) server parameters.
	SNMP-Communities	Sets up an SNMP communities string.
	SNMP-Server	Sets up SNMP server parameters.
	SSH	Sets up SSH record parameters.
	SSL	Sets up SSL record parameters.
	TFTP-Server	Sets up Trivial File Transfer Protocol (TFTP) server parameters.
	Telnet-SSL-Server	Sets up telnet over Secure Socket Layer (SSL) parameters.
	Telnet-Server	Sets up telnet server parameters.

Summary of Repository Variables

This section contains the following tables:

- [Table 6-2 on page 6-26, “IPsec Remote Access Repository Variables - NOT SUPPORTED in this release. -”](#)
- [Table 6-3 on page 6-26, “IPsec Site-to-Site Repository Variables - NOT SUPPORTED in this release. -”](#)
- [Table 6-4 on page 6-29, “L2VPN Repository Variables”](#)
- [Table 6-5 on page 6-32, “MPLS Repository Variables”](#)
- [Table 6-6 on page 6-39, “NAT Repository Variables - NOT SUPPORTED in this release. -”](#)
- [Table 6-7 on page 6-40, “QoS Repository Variables”](#)
- [Table 6-8 on page 6-41, “VPLS Repository Variables”](#)

Table 6-2 provides a summary of the IPsec Remote Access Repository variables available from ISC Templates. - **NOT SUPPORTED in this release.** -

Table 6-2 IPsec Remote Access Repository Variables - NOT SUPPORTED in this release. -

Repository Variable	Dimension	Description	Example
RA-AA_ServerNameList	1	List of authentication server names	North_Am_AA
RA-GroupNameList	1	List of Group names	North_AM_Sales
RA-IPSecPrivateInterfaceAddress (also known as RA-UnsecureInterfaceIPAddressMaskList)	1	List of private interface IP addresses and their subnet masks	171.23.44.33/24 171.23.45.33/24
RA-IPSecPrivateInterfaceName (also known as RA-UnsecureInterfaceNameList)	1	List of private interface names	Ethernet0, Ethernet1
RA-IPSecProtectedSubnets (also known as RA-LocalProtectedIPAddressMaskList)	1	List of IP address ranges and subnet masks protected by this edge device	209.165.20.129/30 209.165.20.130/30 ...
RA-IPSecProtectedSubnetsInclusion	1	Specifies whether the current prefix is to be included or excluded	true, false
RA-IPSecPublicInterfaceAddress (also known as RA-SecureInterfaceIPAddressMaskList)	1	List of public interface IP addresses and their masks	192.209.10.10/30 192.209.11.10/30
RA-IPSecPublicInterfaceName (also known as RA-SecureInterfaceNameList)	1	List of CPE's public interface names	Serial0/0, Serial0/1
RA-SplitTunnelingNetworkLists	2	List of split-tunneling networks	List 0 (Sales Group) 10.1.1.0/24 10.1.2.0/24
RA-SplitTunnelingTypeList	1	List of split-tunneling types	Entry 0 (Acct Group) in-list Entry1 (Mkt Group) in-list

Table 6-3 provides a summary of the IPsec Site-to-Site Repository variables available from ISC Templates. - **NOT SUPPORTED in this release.** -

Table 6-3 IPsec Site-to-Site Repository Variables - NOT SUPPORTED in this release. -

Repository Variable	Dimension	Description	Example
IPSecEigrpAsNumber	0	EIGRP AS number	193
IPSecGreDeleteInterfaceName	1	DMVPN GRE interface name to be deleted	Tunnel0, Tunnel2

Table 6-3 IPsec Site-to-Site Repository Variables (continued) - NOT SUPPORTED in this release. -

Repository Variable	Dimension	Description	Example
IPSecGreInterfaceName	1	DMVPN GRE interface name to be added	Tunnel0, Tunnel2
IPSecMultipointGreDeleteInterface Name	1	List of GRE point-to-multipoint interfaces to be deleted	Tunnel0, Tunnel2
IPSecMultipointGreInterfaceName	1	List of GRE point-to-multipoint interfaces created by ISC	Tunnel0, Tunnel2
IPSecOspfAreaId	0	OSPF Area ID	0
IPSecOspfProcessId	0	OSPF router process ID	10
IPSecPrivateInterfaceAddress	1	List of private interfaces IP addresses	209.165.202.131, 209.165.203.131
IPSecPrivateInterfaceName	1	List of private interface names	Ethernet1, Ethernet0
IPSecPrivateTunnelEndptInterface Address	0	IPsec private tunnel endpoint IP address	2.2.2.2/24
IPSecPrivateTunnelEndptInterfaceName	0	IPsec private tunnel endpoint interface names	FastEthernet0/1
IPSecProtectedSubnets	1	List of IP addresses protected by this edge device	1.1.1.0/24, 1.1.1.3/0...
IPSecProtectedSubnetsInclusion	1	Specifies whether the current prefix is to be included or excluded	true, false
IPSecPublicInterfaceAddress	1	List of IP addresses for the CPE's public interfaces	209.165.202.129/24, 209.165.203.129/24
IPSecPublicInterfaceName	1	List of public interface names	Serial1/1, Serial1/2
IPSecPublicTunnelEndptInterface Address	0	IPsec tunnel endpoint interface address	1.1.1.1/24
IPSecPublicTunnelEndptInterfaceName	0	IPsec tunnel endpoint interface name	Serial1/1
IPSecRemoteAddress	1	List of IPsec endpoint's IP addresses for remote peers	209.165.202.131/28, 209.165.203.131/24
IPSecRemoteDeviceType	1	Type of the remote device	Cisco IOS, PIX, VPN 3000

Table 6-3 IPsec Site-to-Site Repository Variables (continued) - NOT SUPPORTED in this release. -

Repository Variable	Dimension	Description	Example
IPSecRemoteFailoverAddress	2	IPsec tunnel endpoint IP address for the remote peers	209.165.202.131/28, 209.165.203.131/24
IPSecRemoteFailoverDeviceType	2	Remote failover device type	PIX, Cisco IOS, VPN 3000,...
IPSecRemoteFailoverGreInterfaceName	2	Name of the GRE point-to-point interface created to the remote failover devices	Tunnel1, Tunnel2,...
IPSecRemoteFailoverHostName	2	List of failover devices for the remote peers	IPsec_Atlanta, IPsec_NY,...
IPSecRemoteFailoverWildcardPreshared Key	2	Wildcard preshared key for remote failover devices	<my_secret1>, <my_secret2>,...
IPSecRemoteGreInterface Name	1	Name of the GRE point-to-point interface created for the remote peer	Tunnel1, Tunnel2
IPSecRemoteHostName	1	List of remote peer host names	IPsec_Atlanta, IPsec_NY
IPSecRemoteOpType	1	Operation type for the current tunnel	ADD, DELETE
IPSecRemotePresharedKey	1	List of preshared keys to be used to establish tunnels with remote peers	<secret_value1>, <secret_value2> Note: Keys are 128 alphanumeric characters
IPSecRemoteSiteName	1	Names of remote sites	San Jose, New York
IPSecRemoteSubnets	2	List of IP addresses protected by remote peers	209.165.202.129 209.165.202.130...
IPSecRemoteSubnetsInclusion	2	Specifies whether the current remote prefix is to be included or excluded	true, false,...
IPSecRemoteWildcardPresharedKey	1	Wildcard preshared key for remote devices	<secret_value1>, <secret_value2> Note: Keys are 128 alphanumeric characters
IPSecRoutingProtocol	0	IPsec VPN routing protocol	NONE or OSPF

Table 6-3 IPsec Site-to-Site Repository Variables (continued) - NOT SUPPORTED in this release. -

Repository Variable	Dimension	Description	Example
IPSecStaticAdminDistance	0	Administration distance for static routes	1
IPSecTopologyRole	0	Topology role for the current device	HUB, SPOKE

Table 6-4 provides a summary of the L2VPN Repository variables available from ISC Templates.

Table 6-4 L2VPN Repository Variables

Repository Variable	Dimension	Description
AC_Loopback_Address	0	PE loopback address also known as the router ID
CE_DLCI	0	DLCI value on CE for Frame Relay encapsulation
CE_Encap	0	Encapsulation of the CE interface
CE_Intf_Desc	0	Interface description for the CE interface
CE_Intf_Main_Name	0	Major interface name for the CE interface
CE_Intf_Shutdown	0	Shutdown flag for the CE interface
CE_VCD	0	VCD value on CE for ATM encapsulation
CE_VCI	0	VCI value on CE for ATM encapsulation
CE_Vlan_ID	0	VLAN ID on CE for Ethernet encapsulation
CE_VPI	0	VPI value on CE for ATM encapsulation
L2VPNCLECeFacingEncapsulation	0	Encapsulation of the UNI
L2VPNCLECeFacingInterfaceName	0	Name of the UNI
L2VPNCLEPeFacingEncapsulation	0	Encapsulation of the NNI (should always be dot1q)
L2VPNCLEPeFacingInterfaceName	1	Name of the NNI (uplinks) (the number can be more than 1 in case of a ring topology, hence any array)
L2VPNDFBIT_SET	0	Indicates not to fragment the bit set (for L2TPv3 only)
L2VPNDynamicModeUseDefaults	0	Dynamic session setup using ISC default values (for L2TPv3 only)
L2VPN_intf_main_name	1	The main interface name for a CE or PE port
L2VPNIP_PMTU	0	Enable the discovery of the path MTU for tunneled traffic (for L2TPv3 only)
L2VPNIP_TOS	0	Configure the value of the TOS byte in IP headers of tunneled packets or reflects the TOS byte value from the inner IP header (for L2TPv3 only)

Table 6-4 L2VPN Repository Variables (continued)

Repository Variable	Dimension	Description
L2VPNIP_TTL	0	Configure the value of the time to live byte in the IP headers (for L2TPv3 only)
L2VPNL2TP_CLASS_NAME	0	The L2TP class name to overwrite the default L2TP class name (for L2TPv3 only)
L2VPNL2TPv3Sequence	0	Specifies the direction in which sequencing of data packets in a pseudo wire is enabled (for L2TPv3 only)
L2VPNLocalCookieHighValue	0	Specifies the last 4 bytes of the value that the peer PE must include in the cookie field of incoming L2TP packets (for L2TPv3 only)
L2VPNLocalCookieLowValue	0	Specifies the first 4 bytes of the value that the peer PE must include in the cookie field of incoming L2TP packets (for L2TPv3 only)
L2VPNLocalCookieSize	0	Specifies the size (0, 4, or 8) of the cookie field of incoming L2TP packets (for L2TPv3 only)
L2VPNLocalLoopBack	1	The head of the L2TPv3 tunnel
L2VPNLocalSessionId	0	Specifies the ID for the local L2TPv3 session (for L2TPv3 only)
L2VPNLocalSwitchLoopBack1	1	The loopback1 for the local switch (for L2TPv3 only)
L2VPNLocalSwitchLoopBack2	1	The loopback2 for the local switch (for L2TPv3 only)
L2VPNRemoteCookieHighValue	1	Specifies the last 4 bytes of the value that this PE must include in the cookie field of incoming L2RP packets (for L2TPv3 only)
L2VPNRemoteCookieLowValue	1	Specifies the first 4 bytes of the value that this PE must include in the cookie field of incoming L2RP packets (for L2TPv3 only)
L2VPNRemoteCookieSize	1	Specifies the size (0, 4, or 8) of the cookie field of outgoing L2TP packets (for L2TPv3 only)
L2VPNRemoteLoopback	0	The tail of the L2TPv3 tunnel
L2VPNRemoteSessionID	1	Specifies the ID for the remote L2TPv3 session (for L2TPv3 only)
L2VPNSessionSetupMode	0	Defines how the L2TPv3 session is set up (static or dynamic) (for L2TPv3 only)
L2VPNTransportMode	0	Defines how the L2TPv3 data is transferred (for Frame Relay: DLCI or Port; for ATM: VP or VC) (for L2TPv3 only)
L2VPNUniMajorInterfaceName	0	The main interface name of the UNI
L2VPNVCId	0	The virtual circuit ID of the L2TPv3 or AToM tunnel

Table 6-4 L2VPN Repository Variables (continued)

Repository Variable	Dimension	Description
PE_DLCI	0	DLCI value on PE for Frame Relay encapsulation
PE_Encap	0	Encapsulation of the PE interface
PE_Intf_Desc	0	Interface description for the PE interface
PE_Intf_Main_Name	0	Major interface name for the PE interface
PE_VCD	0	VCD value on PE for ATM encapsulation
PE_VCI	0	VCI value on PE for ATM encapsulation
PE_Vlan_ID	0	VLAN ID on PE for Ethernet encapsulation
PE_VPI	0	VPI value on PE for ATM encapsulation
PseudoWire_Class_Type_Of_Core	0	Core type of the Service Provider over which L2VPN is provisioned
Uni_Aging	0	Length of time the MAC address can stay on the port security table
Uni_Cdp_Enable	0	Flag to enable or disable layer 2 tunnelling on a Cisco Discover Protocol (CDP)
Uni_Cdp_Threshold	0	Number of packets per second to be received before the interface is shut down for the CDP protocol
Uni_Mac_Address	0	Number of MAC addresses allowed for port security
Uni_Port_Security	0	Flag to enable or disable security on a UNI interface
Uni_Protocol_Tunnelling	0	Flag to enable or disable Layer 2 Bridge Protocol Data Unit (BPDU) protocol tunnelling on a UNI interface
Uni_Recovery_Interval	0	Amount of time to wait before recovering a UNI port
Uni_Shutdown	0	Flag indicating whether the User Network Interface (UNI) is shutdown
Uni_Speed	0	Value of the UNI link speed
Uni_Stp_Enable	0	Flag to enable or disable layer 2 tunnelling on a Spanning Tree Protocol (STP)
Uni_Stp_Threshold	0	Flag to enable or disable layer 2 tunnelling on an STP
Uni_Violation_Access	0	Action taken when a port security violation is detected
Uni_Vtp_Enable	0	Flag to enable or disable layer 2 tunnelling on a VLAN Trunk Protocol (VTP)
Uni_Vtp_Threshold	0	Flag to enable or disable layer 2 tunnelling on a VTP

Table 6-5 provides a summary of the MPLS Repository variables available from ISC Templates.

Table 6-5 MPLS Repository Variables

Repository Variable	Dimension	Description
Advertised_Routes_To_CE	2	List of one or more IP addresses of the advertised static route to be placed on the PE to define the CE's address space
CE_BGP_AS_ID	0	BGP AS ID on a CE when the routing protocol between a CE and a PE is BGP
CE_DLCI	0	DLCI value on CE for Frame Relay encapsulation
CE_EIGRP_AS_ID	0	EIGRP AS ID on a CE when the routing protocol between a CE and a PE is EIGRP
CE_Facing_MVRFCE_BGP_AS_ID	0	BGP AS ID on an MVRFCE when the routing protocol between a CE and an MVRFCE is BGP, when an MPLS link includes an MVRFCE
CE_Facing_MVRFCE_DLCI	0	DLCI value on CE facing MVRFCE interface for Frame Relay encapsulation, when an MPLS link includes an MVRFCE
CE_Facing_MVRFCE_EIGRP_AS_ID	0	EIGRP AS ID on an MVRFCE when the routing protocol between a CE and an MVRFCE is EIGRP, when an MPLS link includes an MVRFCE
CE_Facing_MVRFCE_Intf	0	Name of the CE facing interface on an MVRFCE, when an MPLS link includes an MVRFCE
CE_Facing_MVRFCE_Intf_Address	0	IP address assigned to the CE facing MVRFCE interface, when an MPLS link includes an MVRFCE
CE_Facing_MVRFCE_Intf_Encap	0	Encapsulation for CE facing of an MVRFCE interface, when an MPLS link includes an MVRFCE
CE_Facing_MVRFCE_Intf_Name	0	Name of the CE facing MVRFCE interface, when an MPLS link includes an MVRFCE
CE_Facing_MVRFCE_Intf_Type	0	Interface type for CE facing of an MVRFCE interface, when an MPLS link includes an MVRFCE
CE_Facing_MVRFCE_Ospf_Process_ID	0	OSPF process ID on MVRFCE when the routing protocol between a CE and an MVRFCE is OSPF, when an MPLS link includes an MVRFCE
CE_Facing_MVRFCE_Tunnel_Src_Addr	0	Tunnel source address on CE facing MVRFCE interface for GRE encapsulation when an MPLS link includes an MVRFCE

Table 6-5 MPLS Repository Variables (continued)

Repository Variable	Dimension	Description
CE_Facing_MVRFCE_VCD	0	VCD value on CE facing MVRFCE interface for ATM encapsulation, when an MPLS link includes an MVRFCE
CE_Facing_MVRFCE_VCI	0	VCI value on CE facing MVRFCE interface for ATM encapsulation, when an MPLS link includes an MVRFCE
CE_Facing_MVRFCE_VLAN_ID	0	VLAN ID on CE facing MVRFCE interface for Ethernet encapsulation, when an MPLS link includes an MVRFCE
CE_Facing_MVRFCE_VPI	0	VPI value on CE facing MVRFCE interface for ATM encapsulation, when an MPLS link includes an MVRFCE
CE_Intf_Address	0	IP address assigned to the CE interface
CE_Intf_Encap	0	Encapsulation of the CE interface
CE_Intf_Name	0	Name of the CE interface
CE_MVRFCE_Bandwidth_Metric_For_Redistribution	0	Bandwidth metric for redistribution of EIGRP when the routing protocol between a CE and an MVRFCE is EIGRP, when an MPLS link includes an MVRFC
CE_MVRFCE_BGP_AS_ID	0	BGP AS ID on a CE when the routing protocol between a CE and an MVRFCE is BGP, when an MPLS link includes an MVRFCE
CE_MVRFCE_Delay_Metric_For_Redistribution	0	Delay metric for redistribution of EIGRP when the routing protocol between a CE and an MVRFCE is EIGRP, when an MPLS link includes an MVRFC
CE_MVRFCE_EIGRP_AS_ID	0	EIGRP AS ID on a CE when the routing protocol between a CE and an MVRFCE is EIGRP, when an MPLS link includes an MVRFCE
CE_MVRFCE_Loading_Metric_For_Redistribution	0	Loading metric for redistribution of EIGRP when the routing protocol between a CE and an MVRFCE is EIGRP, when an MPLS link includes an MVRFC
CE_MVRFCE_MTU_Metric_For_Redistribution	0	MTU metric for redistribution of EIGRP when the routing protocol between a CE and an MVRFCE is EIGRP, when an MPLS link includes an MVRFC
CE_MVRFCE_Ospf_Process_ID	0	OSPF process ID on CE when the routing protocol between a CE and an MVRCE is OSPF, when an MPLS link includes an MVRFCE

Table 6-5 MPLS Repository Variables (continued)

Repository Variable	Dimension	Description
CE_Ospf_Process_ID	0	OSPF process ID on CE when the routing protocol between a CE and a PE is OSPF
CE_Tunnel_Src_Addr	0	Tunnel source address on CE for GRE encapsulation
CE_VCD	0	VCD value on CE for ATM encapsulation
CE_VCI	0	VCI value on CE for ATM encapsulation
CE_Vlan_ID	0	VLAN ID on CE for Ethernet encapsulation
CE_VPI	0	VPI value on CE for ATM encapsulation
Export_Map	0	Name of the export map associated with the VRF
Extra_CE_Loopback_Required	0	Flag to indicate whether an extra loopback request is required on the CE
Import_Map	0	Name of the import map associated with the VRF
Is_Default_Info_Originate	0	Flag to indicate whether the default-information originate command for BGP on the PE when STATIC is a running protocol between a CE and a PE
Is_Default_Routes_Sent_To_CE	0	Flag to indicate whether the default routes are sent to a remote CE
Join_Grey_Mgmt_Vpn	0	Flag to indicate whether MPLS will join a Grey Management VPN
Max_route_threshold	0	Percentage of the maximum number of routes that can be imported into the VRF
Max_Routes	0	Maximum number of routes than can be imported into the VRF
MPLSExportRouteTargets	1	List of Route Targets that are exported for a particular VRF associated with the MPLS VPN link
MPLSImportRouteTargets	1	List of Route Targets that are imported for a particular VRF associated with the MPLS VPN link
MPLSCLEPeFacingInterfaceName	0	The name of the interface on the device facing the PE for that particular MPLS VPN link
MPLSCLEPeFacingEncapsulation	0	The encapsulation of the interface on the device facing the PE for that particular MPLS VPN link
MPLSCLECeFacingInterfaceName	0	The name of the interface on the device facing the CE for that particular MPLS VPN link
MPLSCLECeFacingEncapsulation	0	The encapsulation of the interface on the device facing the CE for that particular MPLS VPN link

Table 6-5 MPLS Repository Variables (continued)

Repository Variable	Dimension	Description
MPLSCeInterfaceMask	0	The mask of the IP address assigned to the CE interface for a particular MPLS VPN link
MPLSPeInterfaceMask	0	The mask of the IP address assigned to the PE interface for a particular MPLS VPN link
MPLSCeLoopbackAddress	0	The IP address of the extra CE loopback address for a particular MPLS VPN link
MVRFCE_CE_Advertised_Routes_To_CE	2	List of one or more IP addresses of the advertised static route to be placed on the PE to define the CE's address space, when the MPLS link includes an MVRFCE
MVRFCE_CE_IP_Unnumbered	0	Flag to indicate whether the MVRCE to CE link is unnumbered, when an MPLS link includes an MVRFCE
MVRFCE_CE_Is_Default_routes_Sent_To_CE	0	Flag to indicate whether the default routes are sent to a remote CE, when an MPLS link includes an MVRFCE
MVRFCE_CE_NBR_ALLOW_AS_IN	0	AllowASIn flag when the routing protocol between a CE and an MVRFCE is BGP, when an MPLS link includes an MVRFCE
MVRFCE_CE_NBR_AS_OVERRIDE	0	ASOverride flag when the routing protocol between a CE and an MVRFCE is BGP, when an MPLS link includes an MVRFCE
MVRFCE_CE_Ospf_Area_Number	0	OSPF area number when the routing protocol between a CE and an MVRCE is OSPF, when an MPLS link includes an MVRFCE
MVRFCE_CE_Routes_To_Reach_Other_Sites	2	List of one or more IP addresses to specify the static routes to put on the CE, when the MPLS link includes an MVRFCE
MVRFCE_CE_Routing_Protocol	0	Routing protocol between MVRFCE and CE
PE_BGP_AS_ID	0	BGP AS ID on a PE when the routing protocol between a CE and a PE is BGP
PE_Cable_Both_Helper_Address_List	1	List of DHCP server IP addresses to which both cable modem and host UDP broadcasts are forwarded
PE_Cable_Modem_Helper_Address_list	1	List of DHCP server IP addresses to which cable modem UDP broadcasts are forwarded
PE_Cable_Modem_Host_Helper_Address_List	1	List of DHCP server IP addresses to which host UDP broadcasts are forwarded
PE_Cable_Modem_Secondary_Address_List	1	List of cable modem secondary addresses for cable interfaces
PE_CE_Bandwidth_Metric_For_Redistribution	0	Bandwidth metric for redistribution of EIGRP when the routing protocol between a CE and a PE is EIGRP

Table 6-5 MPLS Repository Variables (continued)

Repository Variable	Dimension	Description
PE_CE_Delay_Metric_For_Redistribution	0	Delay metric for redistribution of EIGRP when the routing protocol between a CE and a PE is EIGRP
PE_CE_IP_Unnumbered	0	Flag to indicate whether the PE to CE link is unnumbered
PE_CE>Loading_Metric_For_Redistribution	0	Loading metric for redistribution of EIGRP when the routing protocol between a CE and a PE is EIGRP
PE_CE_MTU_Metric_For_Redistribution	0	MTU metric for redistribution of EIGRP when the routing protocol between a CE and a PE is EIGRP
PE_CE_NBR_Allow_AS_In	0	AllowASIn flag when the routing protocol between a CE and a PE is BGP
PE_CE_NBR_AS_Override	0	ASOverride flag when the routing protocol between a CE and a PE is BGP
PE_CE_Ospf_Area_Number	0	OSPF area number when the routing protocol between a CE and a PE is OSPF
PE_CE_Reliability_Metric_For_Redistribution	0	Reliability metric for redistribution of EIGRP when the routing protocol between a CE and a PE is EIGRP
PE_CE_Routing_Protocol	0	Routing protocol between PE and CE
PE_DLCI	0	DLCI value on PE for Frame Relay encapsulation
PE_EIGRP_AS_ID	0	EIGRP AS ID on a PE when the routing protocol between a CE and a PE is EIGRP
PE_Facing_MVRFCE_BGP_AS_ID	0	BGP AS ID on an MVRFCE when the routing protocol between a PE and an MVRFCE is BGP, when an MPLS link includes an MVRFCE
PE_Facing_MVRFCE_DLCI	0	DLCI value on PE facing MVRFCE interface for Frame Relay encapsulation, when an MPLS link includes an MVRFCE
PE_Facing_MVRFCE_EIGRP_AS_ID	0	EIGRP AS ID on an MVRFCE when the routing protocol between a PE and an MVRFCE is EIGRP, when an MPLS link includes an MVRFCE
PE_Facing_MVRFCE_Intf	0	Name of the PE facing interface on an MVRFCE, when an MPLS link includes an MVRFCE
PE_Facing_MVRFCE_Intf_Address	0	IP address assigned to the PE facing MVRFCE interface, when an MPLS link includes an MVRFCE

Table 6-5 MPLS Repository Variables (continued)

Repository Variable	Dimension	Description
PE_Facing_MVRFCE_Intf_Encap	0	Encapsulation for PE facing of an MVRFCE interface, when an MPLS link includes an MVRFCE
PE_Facing_MVRFCE_Intf_Name	0	Name of the PE facing MVRFCE interface, when an MPLS link includes an MVRFCE
PE_Facing_MVRFCE_Intf_Type	0	Interface type for PE facing of an MVRFCE interface, when an MPLS link includes an MVRFCE
PE_FACING_MVRFCE_OSPF_Process_ID	0	OSPF process ID on an MVRFCE when the routing protocol between a PE and an MVRCE is OSPF, when an MPLS link includes an MVRFCE
PE_Facing_MVRFCE_Tunnel_Src_Addr	0	Tunnel source address on PE facing MVRFCE interface for GRE encapsulation when an MPLS link includes an MVRFCE
PE_Facing_MVRFCE_VCD	0	VCD value on PE facing MVRFCE interface for ATM encapsulation, when an MPLS link includes an MVRFCE
PE_Facing_MVRFCE_VCI	0	VCI value on PE facing MVRFCE interface for ATM encapsulation, when an MPLS link includes an MVRFCE
PE_Facing_MVRFCE_VLAN_ID	0	VLAN ID on PE facing MVRFCE interface for Ethernet encapsulation, when an MPLS link includes an MVRFCE
PE_Facing_MVRFCE_VPI	0	VPI value on PE facing MVRFCE interface for ATM encapsulation, when an MPLS link includes an MVRFCE
PE_Intf_Address	0	IP address assigned to the PE interface
PE_Intf_Desc	0	Interface description for the PE interface
PE_Intf_Encap	0	Encapsulation of the PE interface
PE_Intf_Name	0	Name of the PE interface
PE_Intf_Shutdown	0	Shutdown flag for the PE interface
PE_IS_Cable_Modem_Maintenance_Interface	0	Flag to indicate whether the interface is a maintenance interface
PE_MVRFCE_Bandwidth_Metric_For_Redistribution	0	Bandwidth metric for redistribution of EIGRP when the routing protocol between a PE and an MVRFCE is EIGRP, when an MPLS link includes an MVRFCE
PE_MVRFCE_BGP_AS_ID	0	BGP AS ID on a PE when the routing protocol between a PE and an MVRFCE is BGP, when an MPLS link includes an MVRFCE

Table 6-5 MPLS Repository Variables (continued)

Repository Variable	Dimension	Description
PE_MVRFCE_Delay_Metric_For_Redistribution	0	Delay metric for redistribution of EIGRP when the routing protocol between a PE and an MVRFCE is EIGRP, when an MPLS link includes an MVRFCE
PE_MVRFCE_EIGRP_AS_ID	0	EIGRP AS ID on a PE when the routing protocol between a PE and an MVRFCE is EIGRP, when an MPLS link includes an MVRFCE
PE_MVRFCE_IP_Unnumbered	1	Flag to indicate whether the PE to MVRFCE link is unnumbered, when an MPLS link includes an MVRFCE
PE_MVRFCE>Loading_Metric_For_Redistribution	0	Loading metric for redistribution of EIGRP when the routing protocol between a PE and an MVRFCE is EIGRP, when an MPLS link includes an MVRFCE
PE_MVRFCE_MTU_Metric_for_redistribution	0	MTU metric for redistribution of EIGRP when the routing protocol between a PE and an MVRFCE is EIGRP, when an MPLS link includes an MVRFCE
PE_MVRFCE_NBR_ALLOW_AS_IN	0	AllowASIn flag when the routing protocol between a PE and an MVRFCE is BGP, when an MPLS link includes an MVRFCE
PE_MVRFCE_NBR_AS_OVERRIDE	0	ASOverride flag when the routing protocol between a PE and an MVRFCE is BGP, when an MPLS link includes an MVRFCE
PE_MVRFCE_Ospf_Area_Number	0	OSPF area number when the routing protocol between a PE and an MVRFCE is OSPF, when an MPLS link includes an MVRFCE
PE_MVRFCE_OSPF_Process_ID	0	OSPF process ID on PE when the routing protocol between a PE and an MVRFCE is OSPF, when an MPLS link includes an MVRFCE
PE_MVRFCE_Reliability_Metric_For_Redistribution	0	Reliability metric for redistribution of EIGRP when the routing protocol between a PE and an MVRFCE is EIGRP, when an MPLS link includes an MVRFCE
PE_MVRFCE_Routing_Protocol	0	Routing protocol between PE and MVRFCE, when an MPLS link includes an MVRFCE
PE_OSPF_PROCESS_ID	0	OSPF process ID on PE when the routing protocol between a CE and a PE is OSPF
PE_Tunnel_Src_Addr	0	Tunnel source address on PE for GRE encapsulation
PE_VCD	0	VCD value on PE for ATM encapsulation
PE_VCI	0	VCI value on PE for ATM encapsulation

Table 6-5 MPLS Repository Variables (continued)

Repository Variable	Dimension	Description
PE_Vlan_ID	0	VLAN ID on PE for Ethernet encapsulation
PE_VPI	0	VPI value on PE for ATM encapsulation
rd	0	Route Distinguisher value for the VRF
Redistribute_Connected	0	Flag to indicate whether the connected routes are redistributed into BGP on the PE
Redistribute_Static	0	Flag to indicate whether the static routes are redistributed into BGP on the PE
Redistributed_Protocol	1	List of routing protocols to be redistributed
Rip_Metrics	0	Metric for redistribution associated with RIP
Routes_To_Reach_Other_Sites	2	List of one or more IP addresses to specify the static routes to put on the CE.
vrfName	0	Name of the VRF

Table 6-6 provides a summary of the NAT Repository variables available from ISC Templates. - **NOT SUPPORTED in this release.** -

Table 6-6 NAT Repository Variables - NOT SUPPORTED in this release. -

Repository Variable	Dimension	Description	Example
InsideInterfaceNameList	1	List of NAT inside interface names, empty for non-Cisco IOS devices	Ethernet0, Ethernet1, ...
NATIsOverlapping	0	If the site behind this device is overlapping with others. The value is either true or false .	true, false
NATLocalExPrefixList	1	List of exclusion prefixes (IP address ranges) behind this device.	10.10.1.5/32 10.11.1.0/30...
NATLocalPrefixList	1	List of prefixes (IP address ranges) behind this device	10.10.1.0/24 10.11.1.0/24...
NATPeerExPrefixList	1	List of peer's exclusion prefixes (IP address ranges)	10.12.1.1/32 10.13.1.8/30
NATPeerPrefixList	1	List of peer's prefixes (IP address ranges)	10.12.1.0/24 10.13.1.0/24
OutsideInterfaceNameList	1	List of NAT outside interface names, empty for non-Cisco IOS devices	Serial0, Serial1, ...

Table 6-7 provides a summary of the QoS Repository variables available from ISC Templates.

Table 6-7 QoS Repository Variables

Repository Variable	Dimension	Description	Example
QoS_Customer	0	Name of the customer	ABC
QoS_Policy	0	Name of the QoS policy	Gold
QoS_Supported_MPLS	0	Boolean flag to indicate whether MPLS is supported in the core. The value is either true or false .	true false
QoS_PE_Remarking_ReRateLimiting	0	Boolean flag to indicate whether re-marking and re-rate-limiting is required on PE. The value is either true or false .	true false
QoS_CE_Marking_RateLimiting_Interfaces	1	List of marking and rate-limiting interfaces on CE	serial0 serial1 ethernet1
QoS_CE_Marking_RateLimiting_Interface_Encap	1	List of interface encapsulation types of the marking and rate-limiting interfaces on CE (same order as QoS_CE_Marking_RateLimiting_Interfaces)	HDLC HDLC ethernet
QoS_PECLE_Marking_RateLimiting_Interface	0	Name of the marking and rate-limiting interface on PECLE (for Ethernet QoS)	ethernet1
QoS_PECLE_Marking_RateLimiting_Interface_Encap	0	Interface encapsulation type of the marking and rate-limiting interface on PECLE (for Ethernet QoS)	ethernet
QoS_Link_Bandwidth	0	Bandwidth of the CE and PE link (bps)	128000
QoS_LinkEndpoint_Role	0	Role of the link endpoint (that is, CPE or PE)	CPE_Endpt PE_Endpt
QoS_LinkEndpoint_Hostname	0	Hostname of the link endpoint	enpe1
QoS_LinkEndpoint_Platform	0	Platform type of the link endpoint	7206
QoS_LinkEndpoint_Linecard_Model	0	Line-card model of the link endpoint	8OC03_ATM_TS-IR-B

Table 6-7 QoS Repository Variables (continued)

Repository Variable	Dimension	Description	Example
QoS_LinkEndpoint_Interface	0	Interface name of the link endpoint	FastEthernet8/10.700
QoS_LinkEndpoint_Interface_Encap	0	Interface encapsulation type of the link endpoint interface	DOT1Q
QoS_LinkEndpoint_Type	0	Enumerator to indicate the type of the link endpoint (“Interface”, “ATM”, or “FRAME_RELAY”)	FRAME_RELAY
QoS_LinkEndpoint_FR_Dlci	0	Frame-Relay DLCI number of the link endpoint	102
QoS_LinkEndpoint_ATM_VPI	0	VPI value of the ATM VC of the link endpoint	110
QoS_LinkEndpoint_ATM_VCI	0	VCI value of the ATM VC of the link endpoint	256
QoS_LinkEndpoint_ATM_VCD	0	VCD value of the ATM VC of the link endpoint	Atm1
QoS_LinkEndpoint_ATM_PA_Model	0	The ATM port adaptor model of the link endpoint	PA-A1-OC3MM
QoS_LinkEndpointVLAN_Id	0	The VLAN ID of the link endpoint (Ethernet QoS)	800

Table 6-8 provides a summary of the VPLS Repository variables available from ISC Templates.

Table 6-8 VPLS Repository Variables

Repository Variables	Dimension	Description
VPLSCeEncapsulation	0	The encapsulation of the CE interface for a particular VPLS link
VPLSCeInterfaceName	0	The name of the CE interface for a particular VPLS link
VPLSCeMajorInterfaceName	0	The name of a major interface on a CE for a particular VPLS link
VPLSCLECeFacingEncapsulation	0	The encapsulation of interfaces for a particular device facing the CE
VPLSCLECeFacingInterfaceName	0	The interface name for a particular device facing the CE (the number can be more than 1 in case of a ring topology, hence any array)
VPLSCLEPeFacingEncapsulation	0	The encapsulation of interfaces for a particular device facing the PE

Table 6-8 VPLS Repository Variables (continued)

Repository Variables	Dimension	Description
VPLSCLEPeFacingInterfaceName	1	The list of interface names for a particular device facing the PE (the number can be more than 1 in case of a ring topology, hence any array)
VPLSDisableCDP	0	The flag to specify if the CDP has been disabled on a UNI for a particular VPLS link
VPLSFilterBPDU	0	The flag to specify whether the BPDUs will be filtered on a UNI for a particular VPLS link
VPLSPeEncapsulation	0	The encapsulation of the PE interface for a particular VPLS link
VPLSPeInterfaceDescription	0	The description assigned to the PE interface for a particular VPLS link
VPLSPeInterfaceName	0	The name of the PE interface for a particular VPLS link
VPLSPeMajorInterfaceName	0	The name of a major interface on a PE for a particular VPLS link
VPLSPeNeighbors	1	The list of PE POPs participating in a particular VPLS VPN
VPLSPeVfiName	0	The VFI name assigned to a particular VPLS instance existing on the PE POP
VPLSPeVlanId	0	The VLAN ID assigned to the PE for a particular VPLS link
VPLSPeVpnId	0	The VPN ID assigned to a particular VPLS VPN
VPLSSystemMTU	0	The maximum MTU value for a packet arriving on a UNI for a particular VPLS link
VPLSTunnelCDPEnable	0	The flag to specify if the CDP packets will be tunneled to the remote site for a particular VPLS link
VPLSTunnelCDPThreshold	0	The threshold value assigned for a CDP protocol before a violation action is reported on a UNI for a particular VPLS link
VPLSTunnelRecoveryInterval	0	Interval for the UNI to recover from a shutdown scenario
VPLSTunnelSTPEnable	0	The flag to specify if the STP packets will be tunneled to the remote site for a particular VPLS link
VPLSTunnelSTPThreshold	0	The threshold value assigned for a STP protocol before a violation action is reported on a UNI for a particular VPLS link
VPLSTunnelVTPEnable	0	The flag to specify if the VTP packets will be tunneled to the remote site for a particular VPLS link

Table 6-8 VPLS Repository Variables (continued)

Repository Variables	Dimension	Description
VPLSTunnelVTPThreshold	0	The threshold value assigned for a VTP protocol before a violation action is reported on a UNI for a particular VPLS link
VPLSUniAging	0	The aging timer set on a UNI for a particular VPLS link
VPLSUniDuplex	0	The duplex assigned to the UNI for a particular VPLS link
VPLSUniMajorInterfaceName	0	The name of a major interface on a UNI device for a particular VPLS link
VPLSUniMaxMacAddress	0	The maximum number of Mac addresses that can be learned on a UNI for a particular VPLS link
VPLSUniPortSecurity	0	The port security option on a UNI for a particular VPLS link
VPLSUniProtocolTunneling	0	The flag to specify if the protocols will be tunneled to the remote site for a particular VPLS link
VPLSUniSecureMacAddresses	1	The explicit list of Mac addresses that can be learned on a UNI for a particular VPLS link
VPLSUniShutdown	0	The shutdown flag on a UNI for a particular VPLS link
VPLSUniSpeed	0	The speed assigned to the UNI for a particular VPLS link
VPLSUniViolationAction	0	The violation action option on a UNI for a particular VPLS link
VPLSUseNativeVlan	0	The flag to specify if the native VLAN will be used on a UNI for a particular VPLS link

Protocols

- This feature is NOT SUPPORTED in this release. -

Protocols allows you to define customized protocol(s) that are not predefined. ISC defines most commonly used protocols. This Protocol Manager is used to customize protocol definition(s). The protocol is used by access rules in an ISC Firewall policy.

From [Figure 6-1 on page 6-1](#), navigate **Service Design > Protocols** and you can choose either of the following:

- [Protocols, page 6-44](#) Create and manage protocols.
- [Protocol Bundles, page 6-49](#) Create and manage protocol bundles.

Protocols

The Protocols feature allows you to create customized protocols for TCP, UDP, ICMP, IGMP, and IP protocols.

All the possible choices for **Protocols** can be handled as follows:

- Step 1** Navigate **Service Design > Protocols** and then choose **Protocols**. A window such as [Figure 6-30](#), “**Protocols**,” appears.

Figure 6-30 Protocols

Protocols

Show: Any protocols with name matching: A* Find

Showing 1-7 of 7 records

#	☐	Protocol Name	Category	Port Number	Protocol Number	ICMP Type	IGMP Type
1.	☐	AH	ip_plug		51		
2.	☐	ALL_ICMP	icmp				
3.	☐	ALL_IGMP	igmp				
4.	☐	ALL_IP	ip_plug				
5.	☐	ALL_TCP	tcp				
6.	☐	ALL_UDP	udp				
7.	☐	AOL	tcp	5190			

Rows per page: 10

Create ▼ Edit Delete

Proceed to one of the following:

- [Create TCP, page 6-44](#) Make no selections. From the **Create** drop-down menu, click **TCP**.
- [Create UDP, page 6-45](#) Make no selections. From the **Create** drop-down menu, click **UDP**.
- [Create ICMP, page 6-47](#) Make no selections. From the **Create** drop-down menu, click **ICMP**.
- [Create IGMP, page 6-47](#) Make no selections. From the **Create** drop-down menu, click **IGMP**.
- [Create IP, page 6-48](#) Make no selections. From the **Create** drop-down menu, click **IP**.
- [Edit, page 6-48](#) Select one check box to select one protocol, and then click **Edit** to modify it.
- [Delete, page 6-49](#) Select one or more check boxes to select one or more protocols, and then click **Delete** to delete the chosen protocols (you can select all the listed protocols by selecting the check box in the header row).

Create TCP

To create a TCP protocol, navigate **Service Design > Protocols**, choose **Protocols**, and follow these steps:

- Step 1** Click the **Create** button and from the drop-down menu, click **TCP**.
- Step 2** A window as shown in [Figure 6-31](#), “**Create TCP Protocol**,” appears.

Figure 6-31 Create TCP Protocol

Create TCP Protocol

Protocol Name ^{*} :

Source Port Start [?] : (0 - 65535)

Source Port End [?] : (0 - 65535)

Source Port Operation :

Destination Port Start ^{*} : (0 - 65535)

Destination Port End ^{??} : (0 - 65535)

Destination Port Operation :

Note: ^{*} - Required Field
[?] - Required field when "Source Port Operation" is "range".
^{??} - Required when "Destination Port Operation" is "range".

Enter the following fields:

- **Protocol Name** (required)
- **Source Port Start** (optional) If the **Source Port Operation** is **range**, this field is required. Specify the **Source Port Start** (0-65535).
- **Source Port End** (optional) If the **Source Port Operation** is **range**, this field is required. Specify the **Source Port End** (0-65535).
- **Source Port Operation** (optional) The drop-down menu choices are **eq** for equal; **gt** for greater than; **lt** for less than; **neq** for not equal; and **range** for a range of values. The check is for the port number and these qualifiers are for that port. For example, checking only for a port number equal (**eq**) to the port number specified, checking only for port numbers greater than (**gt**) the port specified, and so on.
- **Destination Port Start** (required) Specify the **Destination Port Start** (0-65535).
- **Destination Port End** (optional) If the **Destination Port Operation** is **range**, this field is required. Specify the **Destination Port End** (0-65535).
- **Destination Port Operation** (required when **Source Port Start** is specified) The drop-down menu choices are **eq** for equal; **gt** for greater than; **lt** for less than; **neq** for not equal; and **range** for a range of values. The check is for the port number and these qualifiers are for that port. For example, checking only for a port number equal (**eq**) to the port number specified, checking only for port numbers greater than (**gt**) the port specified, and so on.

Click **Save**.

- Step 3** You return to an updated [Figure 6-30 on page 6-44](#) and a **Status** block with a green check mark for **Succeeded**.

Create UDP

To create a UDP protocol, navigate **Service Design > Protocols**, choose **Protocols**, and follow these steps:

- Step 1** Click the **Create** button and from the drop-down menu, click **UDP**.

Step 2 A window as shown in [Figure 6-32](#), “Create UDP Protocol,” appears.

Figure 6-32 Create UDP Protocol

Create UDP Protocol

Protocol Name *		
Source Port Start ?		(0 - 65535)
Source Port End ?		(0 - 65535)
Source Port Operation :	eq ▼	
Destination Port Start *		(0 - 65535)
Destination Port End ??		(0 - 65535)
Destination Port Operation :	eq ▼	

Save Cancel

Note: * - Required Field
 ? - Required field when "Source Port Operation" is "range".
 ?? - Required when "Destination Port Operation" is "range".

116264

Enter the following fields:

- **Protocol Name** (required)
- **Source Port Start** (optional) If the **Source Port Operation** is **range**, this field is required. Specify the **Source Port Start** (0-65535).
- **Source Port End** (optional) If the **Source Port Operation** is **range**, this field is required. Specify the **Source Port End** (0-65535).
- **Source Port Operation** (required) The drop-down menu choices are **eq** for equal; **gt** for greater than; **lt** for less than; **neq** for not equal; and **range** for a range of values. The check is for the port number and these qualifiers are for that port. For example, checking only for a port number equal (**eq**) to the port number specified, checking only for port numbers greater than (**gt**) the port specified, and so on.
- **Destination Port Start** (required) Specify the **Destination Port Start** (0-65535).
- **Destination Port End** (optional) If the **Destination Port Operation** is **range**, this field is required. Specify the **Destination Port End** (0-65535).
- **Destination Port Operation** (required when **Source Port Start** is specified) The drop-down menu choices are **eq** for equal; **gt** for greater than; **lt** for less than; **neq** for not equal; and **range** for a range of values. The check is for the port number and these qualifiers are for that port. For example, checking only for a port number equal (**eq**) to the port number specified, checking only for port numbers greater than (**gt**) the port specified, and so on.

Click **Save**.

Step 3 You return to an updated [Figure 6-30 on page 6-44](#) and a **Status** block with a green check mark for **Succeeded**.

Create ICMP

To create an ICMP protocol, navigate **Service Design > Protocols**, choose **Protocols**, and follow these steps:

-
- Step 1** Click the **Create** button and from the drop-down menu, click **ICMP**.
- Step 2** A window as shown in [Figure 6-33](#), “Create ICMP Protocol,” appears.

Figure 6-33 Create ICMP Protocol

Create ICMP Protocol

Protocol Name * :

Type * : (0 - 255)

Save Cancel

Note: * - Required Field

Enter the following fields:

- **Protocol Name** (required)
- **Type** (required) This must be a valid ICMP type (0-255).

- Step 3** Click **Save**.
- Step 4** You return to an updated [Figure 6-30 on page 6-44](#) and a **Status** block with a green check mark for **Succeeded**.
-

Create IGMP

To create an IGMP protocol, navigate **Service Design > Protocols**, choose **Protocols**, and follow these steps:

-
- Step 1** Click the **Create** button and from the drop-down menu, click **IGMP**.
- Step 2** A window as shown in [Figure 6-34](#), “Create IGMP Protocol,” appears.

Figure 6-34 Create IGMP Protocol

Create IGMP Protocol

Protocol Name * :

Type * : (0 - 15)

Save Cancel

Note: * - Required Field

Enter the following fields:

- **Protocol Name** (required)
- **Type** (required) This must be a valid IGMP type (0-15).

Step 3 Click **Save**.

Step 4 You return to an updated [Figure 6-30 on page 6-44](#) and a **Status** block with a green check mark for **Succeeded**.

Create IP

To create an IP protocol, navigate **Service Design > Protocols**, choose **Protocols**, and follow these steps:

Step 1 Click the **Create** button and from the drop-down menu, click **IP**.

Step 2 A window as shown in [Figure 6-35, “Create IP Protocol,”](#) appears.

Figure 6-35 Create IP Protocol

Protocol Name * :

Protocol Number * : (0 - 255)

Note: * - Required Field

Enter the following fields:

- Protocol Name (required)
- **Protocol Number** (required) For example, for the GRE protocol, the protocol number is 47 (0-255).

Step 3 Click **Save**.

Step 4 You return to an updated [Figure 6-30 on page 6-44](#) and a **Status** block with a green check mark for **Succeeded**.

Edit

From [Figure 6-30 on page 6-44](#), do the following to edit a protocol:

Step 1 Select one check box, thus selecting only one protocol.

Click the **Edit** button and a window as shown in the create section for this protocol type appears, except that this is an Edit window and the **Name** cannot be changed. Complete the remaining fields as explained in the Create sections. And then click **Save**.

Step 2 [Figure 6-30](#) appears with the updated information.

Delete

From [Figure 6-30](#), do the following to delete protocols:

- Step 1** Select one or more check boxes (to choose all the listed protocols, select the check box in the header row), thus selecting protocol(s).
- Click the **Delete** button and a Confirm Delete window gives you the opportunity to continue, by clicking **Delete** or cancel the delete process by clicking **Cancel**.
- Step 2** [Figure 6-30](#) appears with the updated information.

Protocol Bundles

Protocol Bundles allows you to group Protocols and to use them as a single entity.

All the possible choices for **Protocols Bundles** can be handled as follows:

- Step 1** Navigate **Service Design > Protocols** and then choose **Protocol Bundles**. A window such as [Figure 6-36](#), “**Protocols Bundles**,” appears.

Figure 6-36 Protocols Bundles

Protocol Bundles

Show protocol bundles with name matching

Showing 1-4 of 4 records

#	☐	Protocol Bundle Name	Description
1.	☐	IPsecTraffic	The protocol used by IPsec, includes isakmp, esp and ah
2.	☐	ManagementTraffic	The protocols manages the device, includes telnet, ssh, snmp, ping
3.	☐	protbun1	User created protocol bundle. Includes: icmp1, ip1, and tcp1
4.	☐	Routing Protocols	The routing protocols, includes rip, igmp, eigrp, ospf and bgp

Rows per page:

Proceed to one of the following:

- [Create Protocol Bundles, page 6-50](#) Make no selection. Click **Create**.
- [Edit, page 6-48](#) Select one check box to select one protocol bundle, and then click **Edit** to modify it.
- [Delete, page 6-49](#) Select one or more check boxes to select one or more protocol bundles, and then click **Delete** to delete the chosen protocol bundles (you can select all the listed protocol bundles by selecting the check box in the header row).

Create Protocol Bundles

Navigate **Service Design > Protocols**, choose **Protocol Bundles**, and follow these steps:

-
- Step 1** Click the **Create** button.
- Step 2** A window as shown in [Figure 6-37](#), “Create Protocol Bundles,” appears.

Figure 6-37 Create Protocol Bundles

The screenshot shows a 'Create Protocol Bundle' window. It has a title bar with the text 'Create Protocol Bundle'. Inside, there are three main sections: 'Protocol Bundle Name' with a text field and an asterisk, 'Protocols' with a text field, an asterisk, and a list box containing 'Add' and 'Remove' buttons, and 'Description' with a text field. At the bottom of the window are 'Save' and 'Cancel' buttons. A small note at the bottom left says '* - Required field.'

Enter the following fields:

- **Protocol Bundle Name** (required)
- **Protocols** (required) Click **Add** and a list of protocols appears. Select one or more protocols for this protocol bundle and then click **Select**. The protocols are listed. You can select highlight one or more protocols and then click **Remove** to remove these selections.

Description (optional) This information is for clarity of description of the protocol bundle.

- Step 3** Click **Save**.
- Step 4** You return to an updated [Figure 6-36 on page 6-49](#) and a **Status** block with a green check mark for **Succeeded**.
-

Edit Protocol Bundles

From [Figure 6-36](#), do the following to edit a protocol bundle:

-
- Step 1** Select one check box, thus selecting only one protocol bundle.
- Click the **Edit** button and a window as shown in [Figure 6-37](#) appears, except that this is an Edit Protocol Bundle window and the **Name** cannot be changed. Complete the remaining fields as explained in the “Create Protocol Bundles” section on page 6-50. And then click **Save**.
- Step 2** [Figure 6-36](#) appears with the updated information.
-

Delete Protocol Bundles

From [Figure 6-36](#), do the following to delete protocol bundles:

- Step 1** Select one or more check boxes (to choose all the listed protocol bundles, select the check box in the header row), thus selecting protocol bundle(s).
Click the **Delete** button and a Confirm Delete window gives you the opportunity to continue, by clicking **Delete** or cancel the delete process by clicking **Cancel**.
- Step 2** [Figure 6-36](#) appears with the updated information.

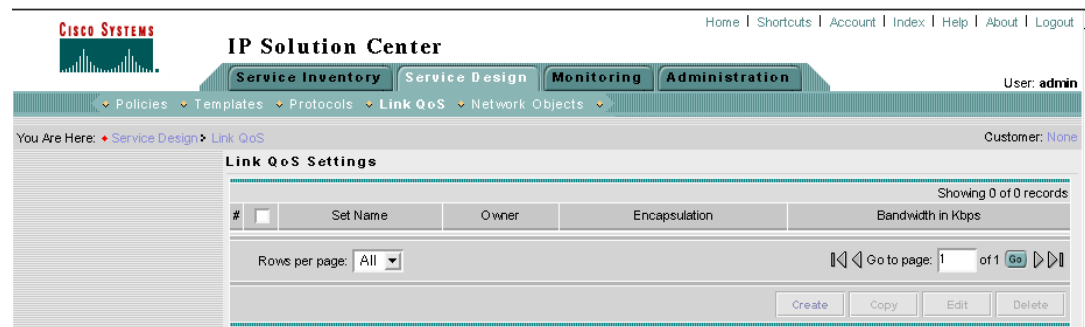
Link QoS

The Link QoS deals with link-level QoS settings such as Aggregate Shapers (FRTS; ATM Shapers, parent-level cb-shaper), Link Efficiency Mechanisms (FRF.12, LFIoMLPPP, and cRTP), and Interface-based CAR, those that depend on Layer2 encapsulation and link bandwidth.

You can create a link QoS setting for a network independent of a VPN service. To create a Link QoS setting for an MPLS service, see [Cisco IP Solution Center Quality of Service User Guide, 4.0](#).

When you navigate **Service Design > Link QoS**, a window appears, as shown in [Figure 6-38](#), “Link QoS Settings.”

Figure 6-38 Link QoS Settings



The current Link QoS settings are available for QoS service requests, including the following information about each Link QoS setting:

- **Set Name** the name of your link QoS settings
- **Owner** Customer or Provider
- **Encapsulation**
- **Bandwidth (in kbps)** for IP Link QoS Setting

The explanation of the buttons and subsequent drop-down menus is given as follows:

- [Create, page 6-52](#) This section explains how to create IP Link QoS Settings.
- [Copy, page 6-56](#) This section explains how to copy an IP Link QoS Setting.

- [Edit, page 6-56](#) This section explains how to edit an IP Link QoS Setting.
- [Delete, page 6-56](#) This section explains how to delete an IP Link QoS Setting.

Create

When you navigate **Service Design > Link QoS**, click the **Create** button at the bottom of the window, as shown in [Figure 6-38](#). To create IP Link QoS settings, proceed as follows:

- Step 1** When you click the **Create** button, you receive a window as shown in [Figure 6-39](#), “**IP Link Settings Editor**.”

Figure 6-39 IP Link Settings Editor

IP Link QoS Settings Editor

Set Name * : testqos

Owner * : ☒ Customer ☐ Provider [Select](#)

Link Bandwidth (kbps) * : 10

Aggregated Traffic Shaper: None

Link Efficiency: FR Fragmentation Size: None
LFI on MLPPP: OFF
Header Compression: OFF

Interface-based Aggregated Rate Limiter: 0 Interface-based Aggregated Rate Limiter(s)

[Save](#) [Cancel](#)

Note: * - Required Field

116269

- Step 2** Fill in the following:

- **Set Name** (required) The name of the link QoS settings. Specify a name that describes the service offered by the settings. Examples: Frame_64K_Gold; ATM_2Mb_Silver. The name Frame_64K_Gold indicates that this set should be used on a CPE-PE link of bandwidth 64kbps, whose layer-2 encapsulation is Frame Relay and to meet an SLA of Gold.
- **Owner** (required) Keep the **Customer** radio button selected (default) or click the **Provider** radio button. Then click **Select** and you receive a list of the customers or providers, as applicable. You can filter this list. From the selected customers or providers, click the radio button for the customer or provider you want to select and click **Select**. You can repeat this procedure if you want to change your selection.
- **Link Bandwidth** (required) The link bandwidth specifies the maximum amount of bandwidth allocated for packets belonging to this link.
- **Aggregated Traffic Shaper** Applies traffic shaping QoS parameters to the device interface. Use this method instead of applying traffic shaping parameters with a service class. Click on the words **Aggregated Traffic Shaper** and you receive a window as shown in [Figure 6-40](#), “**Aggregated Traffic Shaper**.”

Figure 6-40 Aggregated Traffic Shaper

Aggregated Traffic Shaper

CE Aggregated traffic shaper type * : None

Attribute	Value

PE Aggregated traffic shaper type * : None

Attribute	Value

OK Cancel

Note: * - Required Field

129043

- Click the drop-down menu for the **CE** and for the **PE** and select one of the following traffic shaper types. You receive another window in which to specify more information for **Attribute** and **Value**.

FR Traffic Shaper Frame Relay Traffic Shaper. Class-based Parent-level Shaper that operates only in distributed mode on VIP-based routers, such as the Cisco 7500 series platforms.

FR Traffic Shaper (non-MQC) Frame Relay Traffic Shaper. This shaper operates on 72xx and low-end routers.

Parent-level Class-based Shaper Used in the context of nested policy. A nested policy consists of a bottom-level policy that identifies one or more classes of traffic, and a top-level policy that shapes the output of the traffic classes into a single shape rate. You can apply a nested policy to an interface or subinterface.

ATM Traffic Shaper (VBR-rt) Variable bit rate-real time Intended for real-time applications, such as compressed voice over IP and video conferencing, that require tightly constrained delays (cell transfer delay or cell delay variation).

ATM Traffic Shaper (VBR-nrt) Variable bit rate-non real time Follows a leaky bucket or token bucket algorithm.

ATM Traffic Shaper (CBR) Constant bit rate Designed for ATM virtual circuits (VCs) that need a static amount of bandwidth that is continuously available for the duration of the active connection.

ATM Traffic Shaper (ABR) Configures a router to transmit at a rate that varies with the amount of bandwidth available in the network or along the end-to-end transmission path.

None

- Click **OK**. The updated information appears in [Figure 6-39](#).
- **Link Efficiency** Based on the bandwidth of CPE-PE link. Link efficiency features work with queueing and traffic shaping to improve the efficiency and predictability of the application service levels. Click on the words **Link Efficiency** and you receive a window as shown in [Figure 6-41](#), “[Link Efficiency Settings](#).”

Figure 6-41 Link Efficiency Settings

Link Efficiency Settings	
LFI on Frame-Relay (FRF.12):	☒
FRF.12 fragmentation size in bytes : (16-1600)	IOS-DEFAULT
LFI on MLPPP:	☐
ppp multilink fragment-delay in ms : (1-1000)	
Header Compression	
cRTP:	☒
OK Cancel	

- Select the check box for one of the following:

LFI on Frame Relay (FRF.12) (default) Supports the transport of real-time voice and data traffic on Frame Relay virtual circuits (VCs) without causing excessive delay to the real-time traffic. If you choose this, you can override the following field with a number (16 - 1600), which specifies the fragmentation size in bytes.

or

LFI on MLPP Multilink PPP (MLPPP) provides a method of splitting, recombining, and sequencing datagrams across multiple logical data links. MLPPP allows packets to be fragmented and the fragments to be sent at the same time over multiple point-to-point links to the same remote address.
- Leave the **cRTP** check box for Header Compression selected (default) or deselect it. cRTP compresses the IP/UDP/RTP header in an RTP data packet from 40 bytes to approximately 2 to 5 bytes. Use cRTP on a WAN interface where bandwidth is an issue and much of the traffic is RTP traffic.
- Click **OK**. The updated information appears in [Figure 6-39](#).
- **Interface-based Aggregated Rate Limiter** This provides rate limiting for the traffic on a particular interface for the CPE-PE link. Click on the words **Interface-based Aggregated Rate Limiter** and you receive a window as shown in [Figure 6-42](#), “Interface-based Aggregated Rate Limiter List.”

Figure 6-42 Interface-based Aggregated Rate Limiter List

Interface-based Aggregated Rate Limiter List								
Showing 0 of 0 records								
#	☒	Traffic Classification	Direction	Mean Rate	Conformed Burst Size	Extended Burst Size	Conformed Action	Exceed Action
Rows per page: 10								
Add Edit Delete OK Cancel								

- **Add** is available when no choice is made. Click **Add** and you receive a window that lets you enter the following information. Then click **OK** to return to Figure 6-42 with updated information.

Traffic Classification (required) Specifies the method for classifying traffic. Click **Edit** to access the Traffic Classification Editor and choose from these selections.

Direction (required) Click the drop-down menu and choose **OUTPUT** (default) or **INPUT**. This specifies the direction of traffic to apply rate limiting parameters to.

Mean Rate in bps: (8000 - 2000000000) (required).

Conformed burst size in bytes: (1000 - 512000000) (required).

Extended burst size in bytes: (2000 - 1024000000) (required).

Conform—Action (required) Click the drop-down menu and choose: **Transmit**, which sends the packet; **Drop**, which drops the packet; **Set-dscp-transmit**, which sets the DSCP value and transmits the packet (must additionally specify a DSCP value in the drop-down menu); **Set-prec-transmit**, which sets the IP Precedence (0 to 7) values and sends the packet (must additionally specify an IP Precedence value in the drop-down menu); **Set-mpls-exp-transmit**, which sets the mpls experimental (0 to 7) values and sends the packet (must additionally specify an mpls experimental value in the drop-down menu); **Set-dscp-continue**, which sets the DSCP value and transmits the packet (must additionally specify a DSCP value in the drop-down menu); **Set-prec-continue**, which sets the IP Precedence (0 to 7) values and sends the packet (must additionally specify an IP Precedence value in the drop-down menu); or **Set-mpls-exp-continue**, which sets the mpls experimental (0 to 7) values and sends the packet (must additionally specify an mpls experimental value in the drop-down menu).

Exceed—Action (required) Click the drop-down menu and use the same choices as in **Conform—Action** to specify how to handle packets that exceed the configured rate limit.

- **Edit** is available when one check box is selected. You can edit the information that is specified for **Add**. Click **Edit**. After you make your edits, click **OK**.
- **Delete** is available when one or more check boxes are selected. Click **Delete**. The selection is deleted without confirmation.



Note Be careful that you are sure you want to delete before clicking **Delete**. The deletion occurs automatically without confirmation.

- **OK** returns you to Figure 6-39.
- **Cancel** is available to cancel this process.

- Step 3** After making all the selections in [Step 2](#), click **Save** in [Figure 6-39](#).
- Step 4** [Figure 6-38](#) reappears with the new IP Link QoS Setting and a **Status** box in the lower left corner with a green check mark for **Succeeded**.
-

Copy

The **Copy** button at the bottom of [Figure 6-38](#), allows you to create a copy of a Link QoS and then make changes and save it with a new name.

Edit

The **Edit** button, at the bottom of [Figure 6-38](#), allows you to edit a specific link QoS setting. Follow these steps:

-
- Step 1** Navigate **Service Design > Link QoS Settings**.
- Step 2** Select the check box for the row of the link QoS setting that you want to edit.
- Step 3** Click the **Edit** button and a window appears as in [Figure 6-39](#). Edit, following the windows in [Create, page 6-52](#).
- The **Owner** cannot be changed.
- Step 4** Click **Save** and [Figure 6-38](#) reappears with the new Link QoS Setting and a **Status** box in the lower left corner with a green check mark for **Succeeded**.
-

Delete

The **Delete** button, at the bottom of [Figure 6-38](#), allows you to delete one or more link QoS settings. Follow these steps:

-
- Step 1** Navigate **Service Design > Link QoS Settings**.
- Step 2** Select the check box(es) for the row(s) of the link QoS setting(s) you want to delete or select the check box in the header row to select all the link QoS settings for deletion.
- Step 3** Click the **Delete** button and the selected link QoS settings are deleted without a chance to confirm. Otherwise click **Cancel**.



Note

You receive no opportunity to confirm what you want to delete, so be sure you want to delete what you have selected.

Network Objects

- This feature is NOT SUPPORTED in this release. -

Network Objects allows you to create network objects. When you define a network object, you can use this object in a QoS policy or Firewall policy- **Firewall policy is NOT SUPPORTED in this release.** - rather than using the actual address itself. This simplifies Firewall policy- **Firewall policy NOT SUPPORTED in this release.** - or QoS policy creation.

From [Figure 6-1 on page 6-1](#), navigate **Service Design > Network Objects** and follow these steps:

Step 1 The first window to appear is as shown in [Figure 6-43](#), “**Network Objects**.”

Figure 6-43 Network Objects

The screenshot shows the 'Network Objects' window. At the top, there is a search bar with the text 'ShowNetwork Objects with' followed by a dropdown menu set to 'Name', the word 'matching', and a text input field with an asterisk. A 'Find' button is to the right. Below this, it says 'Showing 1-2 of 2 records'. The main area contains a table with the following data:

#	☐	Name	Value	Type	Container Name	Container Type
1.	☐	Mgmt_Network	[0.0.0.0/0]	NETWORK	Global	Global
2.	☐	netobj1	[10.10.10.0/24]	NETWORK	Customer2	Customer

Below the table, there is a 'Rows per page:' dropdown set to '10'. At the bottom right, there are three buttons: 'Create', 'Edit', and 'Delete'. A vertical text '95357' is visible on the right side of the window.

Step 2 From this window, you can do any of the following:

- [Create Network Objects, page 6-57](#) This is enabled when no network objects are selected.
- [Edit Network Objects, page 6-59](#) This is enabled when only one network object is selected.
- [Delete Network Objects, page 6-59](#) This is enabled when one or more network objects are selected.

Create Network Objects

From [Figure 6-43](#), do the following to create a network object:

Step 1 Select no check box, thus selecting no network objects.

Step 2 Click the **Create** button and a window as shown in [Figure 6-44](#), “**Create Network Object**,” appears.

Figure 6-44 Create Network Object

95352

Enter the following information:

- **Name** (required)
- **Type** (required) Click the drop-down menu and choose **STRING** (a free-style string object), **NETWORK** (a range of IP addresses), or **HOST** (a specific IP address).
- **Values** (required) Enter a valid IP address in the format of a.b.c.d/e or a list of valid IP addresses in that format.
- **Container Type** (required) Click the drop-down menu and choose **Global**, **Customer**, **Site**, or **CPE**.
- **Container** (required) If you chose **Customer** (proceed to [Step 3](#)), **Site**, (proceed to [Step 4](#)), or **CPE** (proceed to [Step 5](#)) as the **Container Type**, then **Select** is enabled here. After you make your selection in the resulting window, click **Select** and you return to the updated [Figure 6-44](#).

- Step 3** If you set the **Container Type** to **Customer**, when you click **Select** for **Container**, a Customer for Container Selection window occurs, in which you can click one of the radio buttons and then click **Select**. This customer is added to your **Container**.
- Step 4** If you set the **Container Type** to **Site**, when you click **Select** for **Container**, a Site for Container Selection window appears in which you can select one radio button for a site and then click **Select**. This site is added to your **Container**.
- Step 5** If you set the **Container Type** to **CPE**, when you click **Select** for **Container**, a CPE for Container Selection window appears in which you can select one radio button for a CPE and then click **Select**. This CPE is added to your **Container**.
- Step 6** Click **Save** in [Figure 6-44](#) and you return to an updated [Figure 6-43 on page 6-57](#).

Edit Network Objects

From [Figure 6-43](#), do the following to edit a network object:

-
- Step 1** Select one check box, thus selecting only one network object.
- Click the **Edit** button and a window as shown in [Figure 6-44](#) appears, except that this is an Edit Network Object window and the **Name** cannot be changed. Complete the remaining fields as explained in the “[Create Network Objects](#)” section on page 6-57. And then click **Save**.
- Step 2** [Figure 6-43](#) appears with the updated information.
-

Delete Network Objects

From [Figure 6-43](#), do the following to delete network objects:

-
- Step 1** Select one or more check boxes (to choose all the listed network objects, select the check box in the header row), thus selecting network object(s).
- Click the **Delete** button and a Confirm Delete window gives you the opportunity to continue, by clicking **Delete** or cancel the delete process by clicking **Cancel**.
- Step 2** [Figure 6-43](#) appears with the updated information.
-



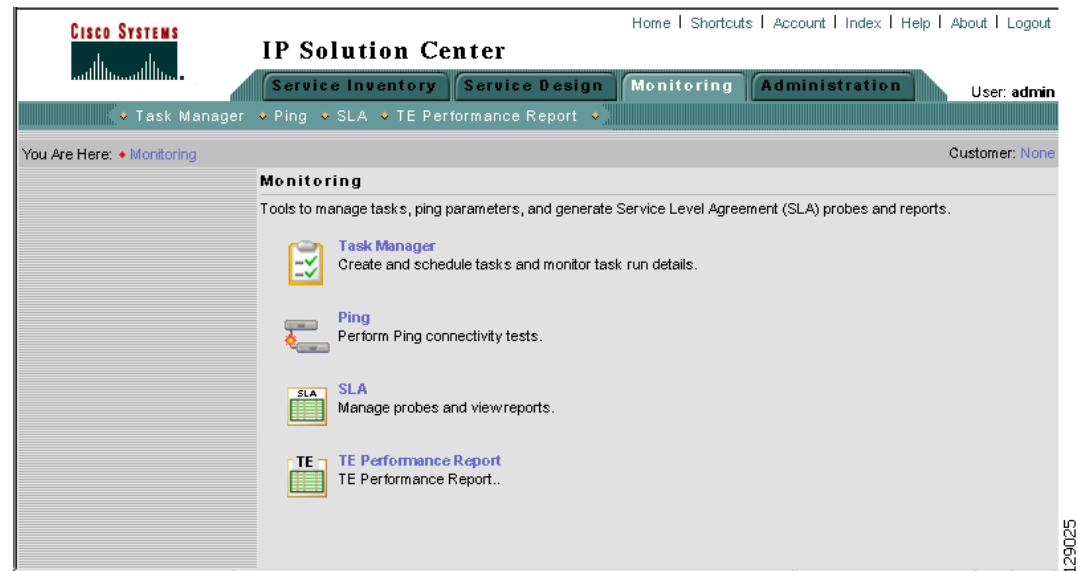
CHAPTER

7

Monitoring

From the Home window of Cisco IP Solution Center (ISC), you receive upon logging in, click the **Monitoring** tab and you receive a window as shown in [Figure 7-1](#), “**Monitoring Selections**.”

Figure 7-1 Monitoring Selections



Next you can navigate to the following selections:

- [Task Manager, page 7-1](#) Create and schedule tasks and monitor task run details.
- [Ping, page 7-8](#) Perform Ping connectivity tests.
- [SLA, page 7-14](#) Manage probes and view reports.
- [TEM Performance Report, page 7-59](#) TEM performance report.

Task Manager

ISC provides a Task Manager that allows you to view pertinent information about both current and expired tasks of all types, and to create and schedule new tasks, delete specified tasks, and delete the active and expired tasks.

This section contains the following subsections:

- [Tasks, page 7-2](#)
- [Task Logs, page 7-6](#)

Tasks

Starting Task Manager

To start Task Manager, follow these steps:

- Step 1** Click the **Task Manager** icon. The Tasks list page appears, as shown in [Figure 7-2, “Tasks.”](#)

Figure 7-2 Tasks

Tasks					
Show Tasks with Task Name matching * of Type * Find					
Showing 1 - 10 of 11 records					
#	☐	Task Name	Type	Schedule	Creator Created on
1.	☐	Task Created 2004-09-28 10:07:55.103	Service Deployment	Single run at 2004-09-28 10:00:00.0	SD 2004-09-28 10:07:57.424
2.	☐	Task Created 2004-09-28 10:03:09.686	Service Deployment	Single run at 2004-09-28 10:00:00.0	SD 2004-09-28 10:03:14.736
3.	☐	Task Created 2004-09-28 09:58:02.981	Service Deployment	Single run at 2004-09-28 09:58:00.0	SD 2004-09-28 09:58:05.343
4.	☐	Task Created 2004-09-28 09:51:34.271	Service Deployment	Single run at 2004-09-28 09:51:00.0	SD 2004-09-28 09:51:37.044
5.	☐	Collect Config 2004-09-27 17:05:47.503	Collect Config	Single run at 2004-09-27 17:06:00.0	ENG 2004-09-27 17:05:50.164
6.	☐	Task Created 2004-09-22 11:37:56.332	Service Deployment	Single run at 2004-09-22 11:37:00.0	SD 2004-09-22 11:37:58.719
7.	☐	Task Created 2004-09-22 11:35:10.21	Service Deployment	Single run at 2004-09-22 11:35:00.0	SD 2004-09-22 11:35:12.59
8.	☐	Task Created 2004-09-22 11:29:16.333	Service Deployment	Single run at 2004-09-22 11:29:00.0	SD 2004-09-22 11:29:18.964
9.	☐	Task Created 2004-09-22 11:24:33.102	Service Deployment	Single run at 2004-09-22 11:24:00.0	SD 2004-09-22 11:24:36.146
10.	☐	Task Created 2004-09-22 11:17:14.623	Service Deployment	Single run at 2004-09-22 11:17:00.0	SD 2004-09-22 11:17:22.207
Rows per page: 10 Go to page: 1 of 2 Go					
Auto Refresh: ☒ Create Audit Details Schedules Delete					

129023

The Tasks window displays information about each task by **Task Name**, **Type**, **Schedule** date and time, the user name of the **Creator** who created those tasks, and the date **Created on**. To view, schedule, or delete the listed tasks, select the corresponding check box.

New Tasks can also be created or audited using this window.

Creating a New Task

To create a new task, follow these steps:

- Step 1** From the **Tasks** page, as shown in [Figure 7-2](#), “**Tasks**,” click **Create**. From the resulting drop-down list, you can choose from the following and that choice becomes the **Type** in [Figure 7-3](#), “**Create Tasks**,”:
- **Collect Config** - collects configuration from devices.
 - **Password Management** - manages user passwords and SNMP community strings.
 - **SLA Collection** - collects data from SLA enabled devices.
 - **Service Deployment** - deploys an existing SR.
 - **TE Discovery** - populates the repository with tunnel and route data from the Traffic Engineering network.
 - **TE Interface Performance** - calculates tunnel/interface bandwidth utilization using SNMP.

Figure 7-3 Create Tasks

Create Task

Name *	Certificate Enrollment Audit 2004-02-29 22:46:50.689
Type	Certificate Enrollment Audit
Description:	Created on 2004-02-29 22:46:50.689
Task Configuration Method:	☒ Simplified ☐ Advanced (via wizard)

Note: * - Required Field

- Step 2** **Name:** Enter the name of the task. You can accept the default value.
- Step 3** **Type:** Defined in [Step 1](#).
- Step 4** **Description:** (optional) Enter a description.
- Step 5** **Task Configuration Method** (default: **Simplified**) Choose **Simplified** or **Advanced (via wizard)**.

116270

- Step 6** Click **Next** to continue. Depending on what type of task you select, the Task Devices or Task Service Requests page appears, as shown in [Figure 7-4](#), “Task Devices” and [Figure 7-5](#), “Task Service Requests,” respectively, with variations.

Figure 7-4 Task Devices

Devices:		Select/Deselect
Groups:		Select/Deselect
Options:	☒ Retrieve device attributes ☒ Retrieve Interfaces	
Schedule:	☐ Now ☒ Later ☐ None	
Later Schedule * :		Edit
Task Owner:	☐ Customer ☐ Provider ☒ None	
		Submit Cancel

Note: * - Required Field

116271

Figure 7-5 Task Service Requests

Service Requests * :		Select/Deselect
Options:	☐ Include device certificates only Include certificates for following trustpoint only: 	
Schedule:	☒ Now ☐ Later ☐ None	
Task Owner:	☐ Customer ☐ Provider ☒ None	
		Submit Cancel

Note: * - Required Field

116272

- Step 7** Click **Select/Deselect** to add devices or service requests.
- Step 8** In the resulting selection window, select the devices or service requests and click **Select**. The selected devices or service requests appear in [Figure 7-4](#), “Task Devices” or [Figure 7-5](#), “Task Service Requests,” respectively.
- Step 9** **Groups** might or might not appear depending on the task you specify in the previous step. If it does appear, you can add groups of devices, similarly to [Step 7](#) and [Step 8](#). If it doesn’t appear or after you complete this device group selection, proceed to [Step 11](#).
- Step 10** Choose the **Options**.

- Step 11** For **Schedule**, click **Now**, **Later**, or **None**. If you choose **Later**, a Later Schedule category appears. You are then required to click the **Edit** button and the Task Scheduler page appears, as shown in [Figure 7-6](#), “Task Schedule Details.”

Figure 7-6 Task Schedule Details

The **Task Schedule** dialog box contains the following sections:

- Single Run:** Radio buttons for **Now** (selected), **Once**, **Periodic Run:** Radio buttons for **Minute**, **Hourly**, **Daily**, **Weekly**, and **Monthly**.
- Periodic Run Attributes:** Fields for **Run Interval:** and **Run Limits:**.
- Start Date and Time:**
 - Date:** Month (March), Day (28), Year (2003).
 - Time:** Hour (4), Minute (49), AM/PM (PM).
- End Date and Time (Default is unlimited):**
 - Date:** Month, Day, Year.
 - Time:** Hour, Min, AM/PM.

At the bottom right are **OK** and **Cancel** buttons. A small number 93470 is visible on the right side of the dialog box.

- Step 12** Select information to schedule the task and click **OK** (default is to schedule **Now**).

- Step 13** Click **Submit** to continue. The new task is added to the list of tasks.

Audit

To get audit information, follow these steps:

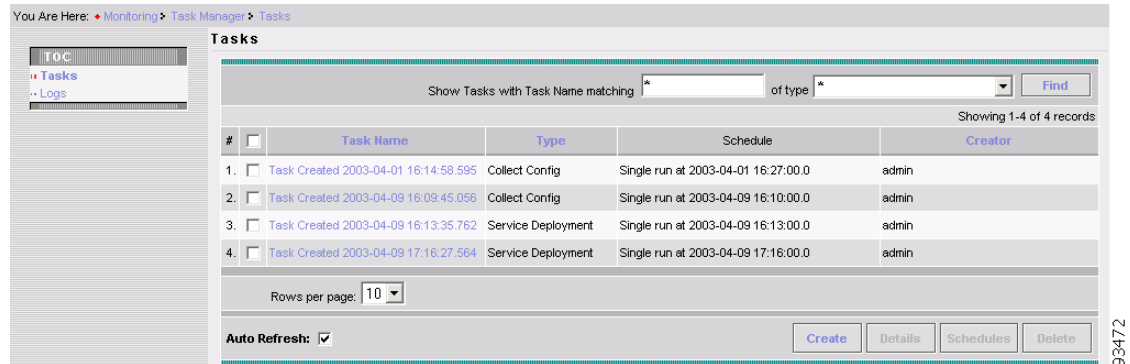
- Step 1** From the **Tasks** page, as shown in [Figure 7-2](#), “Tasks,” click **Audit**. From the resulting drop-down list, you can choose from the following and that choice becomes the **Type** in [Figure 7-3](#), “Create Tasks,”:
- **Certificate Enrollment Audit** - verifies certificate enrollment.
 - **Config Audit** - compares ISC generated configlet against the one in the device.
 - **IPsec Functional Audit** - audits IPsec functionality.- **This feature is NOT SUPPORTED in this release.** -
 - **L2VPN (L2TPv3) Functional Audit** - audits L2TPv3 functionality.
 - **MPLS Functional Audit** - audits MPLS functionality.
 - **TE Functional Audit** - checks the Label-Switch Path (LSP) on a router against the LSP stored in the repository.

Task Logs

Task Logs can be used to understand the status of a task, whether or not it completed successfully. You can also use the Task Logs to troubleshoot why a task has failed. To view the Task Logs, follow these steps:

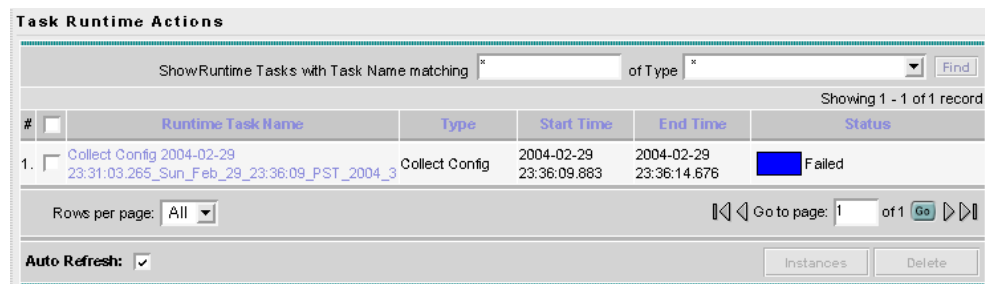
- Step 1** Click **Task Manager**. The Tasks page appears, as shown in [Figure 7-7](#), “Tasks.”

Figure 7-7 Tasks



- Step 2** Click **Logs** under the TOC heading located on the left-hand side. The Task Runtime Actions page appears, as shown in the [Figure 7-8](#), “Task Runtime Actions.”

Figure 7-8 Task Runtime Actions



This window displays the task by Runtime Task Name, and the Type, Start Time, End Time and the Status of the task. You can use this window to view or delete the logs.

- Step 3** To view the log, select the check box for the row that represents the task.
- Step 4** Click **Instances**. The Runtime Actions page appears, as shown in [Figure 7-9](#), “Runtime Actions.”



Note

If you want to delete a runtime task, click **Delete**.

Figure 7-9 Runtime Actions

Runtime Actions

Task: Task Created 2003-03-28 13:55:33.38_Fri_Mar_28_13:55:44_PST_2003_9 [Refresh](#)

Showing 1-2 of 2 records

#	☐	Action	Start Time	End Time	Status
1.	☐	Deployment	2003-03-28 13:55:46.163	2003-03-28 13:56:11.19	Completed successfully
2.	☐	ConfigAudit	2003-03-28 13:56:11.238	2003-03-28 13:56:29.841	Completed successfully

Rows per page:

[Log](#) [OK](#)

93474

Step 5 Select the log you want to view in detail and select the check box for that row of information.

Step 6 Click **Log**. The Task Log page appears, as shown in [Figure 7-10, “Task Log.”](#)

Figure 7-10 Task Log

Task Log

Deployment Log for Task Task Created 2003-03-28 13:55:33.38_Fri_Mar_28_13:55:44_PST_2003_9

Log Level: Component: [Filter](#)

Date	Level	Component	Message
2003-03-28 13:55:46	INFO	Provisioning.ProvDrv	The argument to the ProvDrv are: IsForceRedeploy = false IsProvision = true ipsec-rekey = false JobIdList = 4 targets = []
2003-03-28 13:55:46	INFO	Provisioning.ProvDrv	Opening repository ...
2003-03-28 13:55:46	INFO	Provisioning.ProvDrv	Open repository succeeded
2003-03-28 13:55:46	INFO	Provisioning.ProvDrv	===== Creating ProvDrvSR for Job#4SR#5
2003-03-28 13:55:46	INFO	Provisioning.ProvDrv	Filter to getLogicalDevices: 1
2003-03-28 13:55:46	INFO	repository.firewallSR	add ProvMem: com.cisco.vpnsc.repository.firewall.RepDevMembership@535b73
2003-03-28 13:55:46	INFO	Provisioning.ProvDrv	Number of logicalDevices got: 1
2003-03-28 13:55:47	INFO	repository.firewallSR	add ProvMem: com.cisco.vpnsc.repository.firewall.RepDevMembership@98f4d4
2003-03-28 13:55:47	INFO	Provisioning.ProvDrv	Processing logical device 2 with physical id 3
2003-03-28 13:55:47	INFO	Provisioning.ProvDrv	Service blade for this device: com.cisco.vpnsc.prov.firewall.FWServiceBlade
2003-03-28 13:55:47	INFO	Provisioning.ProvDrv	Create blade the first time: com.cisco.vpnsc.prov.firewall.FWServiceBlade
2003-03-28 13:55:47	INFO	prov.FWServiceBlade	Debug = true
2003-03-28 13:55:47	INFO	prov.FWServiceBlade	Debug is on: temporary directory = /export/home/vpnadm/isc/tmp/firewall/1048686547147
2003-03-28 13:55:47	INFO	Provisioning.ProvDrv	Filter to generateXML: 1
2003-03-28 13:55:47	INFO	repository.firewallSR	generating firewall SR XML
2003-03-28 13:55:48	INFO	repository.firewallSR	add ProvMem: com.cisco.vpnsc.repository.firewall.RepDevMembership@f4d59a
2003-03-28 13:55:49	INFO	Provisioning.ProvDrv	Cache input.xml with preferred value: 1

[Return to Logs](#)

93475

It is possible to set the types of log level you want to view. Specify the Log Level and click on the Filter button to view that information you want to view.

Step 7 Click **Return to Logs** to specify another log to view.

Ping

Ping is the way ISC monitors the VPN connectivity, that is verify the connectivity among various edge devices comprising the VPN. To achieve this, you can perform a series of pings among these devices. Ping has the following benefits:

- Ping is service independent and therefore can be used for functional auditing of MPLS applications.
- Ping can establish whether a service is working without doing a functional audit for that service.
- Ping can be used to verify IPv4 connectivity among CPEs prior to VPN or Firewall- **This feature is NOT SUPPORTED in this release.** - service deployment.
- Ping fits well with Firewall service in conjunction with a VPN service for ensuring the firewall service did not break the VPN service.- **This feature is NOT SUPPORTED in this release.** -

However, Ping does not do the following:

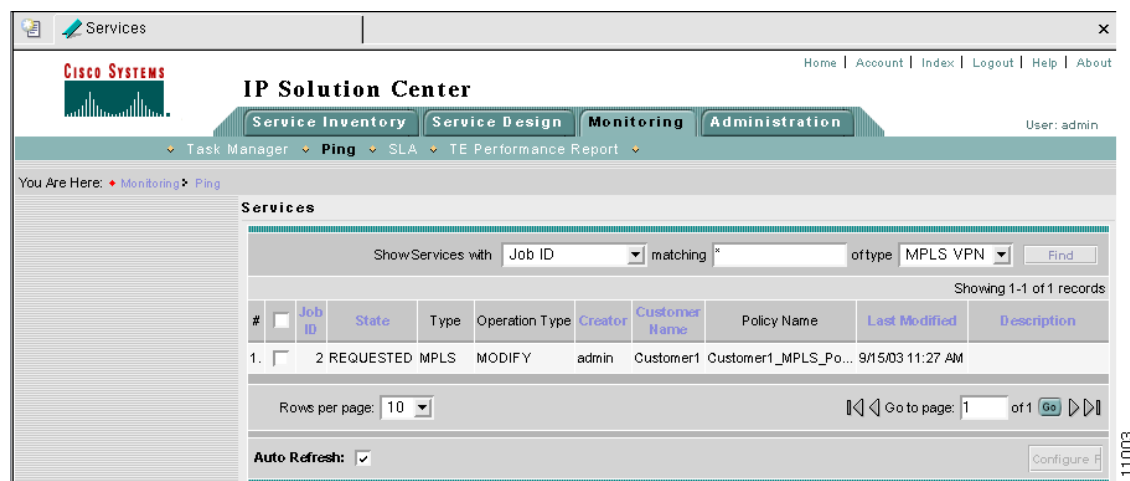
- Ping does not work in environments where ICMP traffic is blocked, for example, in an Cisco IOS router with an access-list denying all ICMP traffic or a PIX firewall which by default does not permit ICMP.
- Ping can only inform you that there is a connectivity problem. It does not offer any service-specific information. The connectivity problem can be due to many reasons, such as device failure, misconfiguration, and so on, which ping cannot distinguish.
- Only the immediate subnet behind the router's customer-facing (also, inside or nonsecured) interface is supported. Campus subnets cannot be supported.

The Ping GUI supports all possible pings for MPLS service requests.

This section explains how to ping MPLS service requests.

After you navigate **Monitoring > Ping**, you receive a window as shown in [Figure 7-11](#), “Services.”

Figure 7-11 Services



From here you can use the **Show Services with** drop-down menu to select:

- **Job ID**
- **Customer Name**
- **VPN Name**

- **State**
- **Description**

Then for **matching**, enter the beginning characters of the names you want to match followed by *.

Then before clicking **Find**, from **of type** select **MPLS** or **IPsec** (**This feature is NOT SUPPORTED in this release**). -and proceed as follows:

- [MPLS, page 7-9](#) explains the flow after choosing the type **MPLS**.
- [IPsec, page 7-11](#) explains the flow after choosing the type **IPsec**.- **This feature is NOT SUPPORTED in this release.** -

**Note**

At the bottom of many windows, you can change the number of rows shown on this window in **Rows per page**. Click the drop-down menu and you can select **5, 10, 20, 30, 40**, or **All**.

**Note**

At the bottom of many windows you can click the **Auto Refresh** button to automatically refresh after **n** seconds, where **n** is the refresh rate set in DCPL, or you can unclick this button and not automatically refresh.

MPLS

After you navigate **Monitoring > Ping** and select **MPLS** as the **type**, follow these steps:

- Step 1** Select the check box next to each row for which you want to configure ping parameters or select the check box in the heading row to select all the rows.
- Step 2** Click the **Configure Ping Parameters** button which becomes enabled. A window as shown in [Figure 7-12](#), “**MPLS Parameters**,” appears.

Figure 7-12 MPLS Parameters

MPLS Parameters

Ping Type: ☒ Do PE to CE Ping ☐ Do CE to CE Ping

Two-way Ping: ☐

Packet Repeat Count: (5 - 1,000)

Datagram Size: (36 - 18,024)

Note: * - Required Field

116273

Fill in the following and then click **Start Ping**:

- **Ping Type—Do PE to CE** When this radio button is chosen, a VRF ping occurs for all PE CE pairs that form an MPLS VPN link. The IP addresses taken for this ping are the link end-point addresses. For example, assume that an MPLS service request has two linked PE1<>CE1 and PE2<>CE2. Then this selection initiates four VRF pings: (PE1, CE1), (PE2, CE2), (PE1, CE2), and (PE2, CE1). When this selection is chosen, then after you click **Start MPLS Ping**, you go directly to [Step 6](#) and receive a result page.
- **Ping Type—Do CE to CE ping** When this radio button is chosen, a ping occurs between all CEs that make the end-point in the service request. When this selection is chosen, then after you click **Start MPLS Ping**, proceed to [Step 3](#).
- **Two-way Ping** (default: unavailable and deselected) This check box is only available when you select **Do CE to CE ping**. When a ping occurs from device1 to device2 and this check box is selected, then a ping from device2 to device1 also occurs.
- **Packet Repeat count** (valid values: 5 - 1000) (default: 5) This value indicates how many ICMP packets to use for a ping.
- **Datagram size** (valid values: 36-18024) (default: 100) This value is the packet size of ICMP used for pinging.

Step 3 For **Do CE to CE ping**, you proceed to a window as shown in [Figure 7-13](#), “MPLS CE Selection.”

Figure 7-13 MPLS CE Selection

Showing 1-1 of 1 records								
#	☐	Job ID	Source CE	Source IP Address	Source Site	Destination CE	Destination IP Address	Ping Result
1.	☐	2	ence51		Site-ence51	ence61		Incomplete
Rows per page: 10								
Start MPLS CE Ping								

- Step 4** Select the check box next to each row for which you want to select a CE or select the check box in the heading row to select all the rows.
- Step 5** Click the **Start MPLS CE Ping** button which becomes enabled.
- Step 6** You receive a results window as shown in [Figure 7-14](#), “MPLS Ping Test Results.”

Figure 7-14 MPLS Ping Test Results

ping test results

Showing 1-4 of 4 records								
#	Property Name					Property Value		
1.	Packet repeat count					5		
2.	Datagram size					100		
3.	Two-way Ping					no		
4.	Do PE to CE ping					no		
Showing 1-2 of 2 records								
#	Job ID	PE	Source IP Address	Source Region	CE	Destination IP Address	Destination Site	Ping Result
1.	12	mlpe2	40.40.40.13	West	mlce3	40.40.40.14	SJ	0/5 success
2.	27	mlpe2	40.40.40.29	West	mlce1	40.40.40.30	SF	0/5 success
Rows per page: 10								
Auto Refresh: ☐								
Redo Ping			View Job Logs		Refresh		Close	

Step 7 The buttons at the bottom of the window are as follows:

- **Redo Ping** When you click this button, you restart all the pings. The parameters used are the same as those specified in the last request.
- **View Job Logs** When you click this button, you receive logs of all the ISC jobs created for doing ping. The ping application creates one job per selected service request.
- **Auto Refresh** If this check box is selected, a result refreshes every **n** seconds, where **n** is defined in DCPL as the refresh rate.
- **Refresh** To selectively refresh, turn off the **Auto Refresh** button and click this button whenever you want to update the results.
- **Close** Click this button to close the current ping request. You return to the **Monitoring** page.

**Note**

Any column heading in blue indicates that by clicking that column header, you can sort on that column.

Step 8 Click **Close** and you are finished with this Ping session.

IPsec

- This feature is NOT SUPPORTED in this release. -

After you navigate **Monitoring > Ping** and select **IPsec** as the **type**, follow these steps:

- Step 1** Select the check box next to each row for which you want to configure ping parameters or select the check box in the heading row to select all the rows.
- Step 2** Click the **Configure Ping Parameters** button which becomes enabled. A window as shown in [Figure 7-15](#), “**IPsec Parameters**,” appears.

Figure 7-15 IPsec Parameters

IPsec Parameters	
Using IPsec Tunnels:	☒ Ping Inside IPsec Tunnels ☐ Ping Outside IPsec Tunnels
Mirror Ping:	☐
Full Mesh Ping:	☐
Select Subset of Devices to Ping:	☐
Packet Repeat Count:	5 (5 - 1,000)
Datagram Size:	100 (36 - 18,024)
Start Ping	
Note: * - Required Field	

Fill in the following and then click **Start Ping**. If you select **Select subset of devices to ping**, you proceed to [Step 3](#). If not, you proceed to [Step 6](#).

- **Using IPsec tunnels** (required) (default: **Ping inside IPsec tunnels**) If you select the **Ping inside IPsec tunnels** radio button, you use nonsecure interfaces for ping. If you select the **Ping outside IPsec tunnels** radio button, you use secure interfaces for the ping.
- **Mirror Ping** (default: deselected) When a ping occurs from device1 to device2 and this check box is selected, then a ping from device2 to device1 also occurs.
- **Full mesh ping** (default: deselected) In a scenario like DMVPN, where spokes of a hub and spoke service request can talk to each other without going through the hub, you might be required to do a full-mesh ping, that is ping as though the service request is full-mesh. In this case, select this check box.
- **Select subset of devices to ping** (default: deselected) When this check box is selected, you receive the ability to select the pings you require rather than pinging all the choices.

**Note**

Full mesh ping and **Select subset of devices to ping** can be used in conjunction to verify that the DMVPN is working. For example, for a hub and spoke service request with three spokes, if spoke1 and spoke2 are connected, you are interested in following pings: (hub, spoke1), (hub, spoke2), (hub, spoke3), and (spoke1,spoke2). You can select both check boxes **Full mesh ping** and **Select subset of devices to ping**. Then on the CE selection page you receive all possible ping combinations between a hub and four spokes. You can select the four required pings and view the result.

- **Packet repeat count** (valid values: 5 - 1000) (default: 5) This value indicates how many ICMP packets to use for a ping.
- **Datagram size** (valid values: 36-18024) (default: 100) This value is the packet size of ICMP used for pinging.

Step 3 If you selected **Select subset of devices to ping**, you receive a window as shown in [Figure 7-16](#), “**IPsec CE Selection**.”

Figure 7-16 IPsec CE Selection

Showing 1-2 of 2 records

#	☐	Job ID	Source CE	Source IP Address	Source Site	Destination CE	Destination IP Address	Destination Site	Ping Result
1.	☐	4	carson	10.128.0.254	SJ	barnes.cisco.com	10.128.16.1	Boulder	Incomplete
2.	☐	4	barnes	10.128.16.1	Boulder	carson.cisco.com	10.128.0.254	SJ	Incomplete

Rows per page: 10

Start IPsec CE Ping

93740

- Step 4** Select the check box next to each row for which you want to select a CE or select the check box in the heading row to select all the rows.
- Step 5** Click the **Start IPsec CE Ping** button which becomes enabled.
- Step 6** You receive a results window as shown in Figure 7-17, “IPsec Ping Test Results.”

Figure 7-17 IPsec Ping Test Results

Showing 1-5 of 5 records

#	Property Name	Property Value
1.	Two-way Ping	yes
2.	Ping inside IPsec tunnels	yes
3.	Packet repeat count	5
4.	Datagram size	100
5.	Full mesh ping	yes

Showing 1-2 of 2 records

#	Job ID	Source Device	Source IP Address	Source Location	Destination Device	Destination IP Address	Destination Location	Ping Result
1.	2	ipsec-cpe-geneva	10.10.130.2	Customer1::Site1	ipsec-cpe-milan	10.10.110.2	Customer1::Site2	0/5 success
2.	2	ipsec-cpe-milan	10.10.110.2	Customer1::Site2	ipsec-cpe-geneva	10.10.130.2	Customer1::Site1	0/5 success

Rows per page: 10

Auto Refresh: ☐ Redo Ping View Job Logs Refresh Close

93741

- Step 7** The buttons at the bottom of the window are as follows:
- **Redo Ping** When you click this button, you restart all the pings. The parameters used are the same as those specified in the last request.
 - **View Job Logs** When you click this button, you receive logs of all the ISC jobs created for doing ping. The ping application creates one job per selected service request.
 - **Auto Refresh** If this check box is selected, a result refreshes every **n** seconds, where **n** is defined in DCPL as the refresh rate.
 - **Refresh** To selectively refresh, turn off the **Auto Refresh** button and click this button whenever you want to update the results.
 - **Close** Click this button to close the current ping request. You return to the **Monitoring** page.

**Note**

Any column heading in blue indicates that by clicking that column header, you can sort on that column.

Step 8

Click **Close** and you are finished with this Ping session.

SLA

A service-level agreement (SLA) defines a level of service provided by a service provider to any customer. Performance is monitored through the SLA server. ISC monitors the service-related performance criteria by provisioning, collecting, and monitoring SLAs on Cisco IOS routers that support the Service Assurance Agent (SA Agent) devices. To provision the SLAs and to collect statistics for each SLA, the data collection task requires minimal user input.

The SLA collection task collects the relevant performance data, stores it persistently, aggregates it, and presents useful reports. The SLA collection task collects from the SA Agent MIB on devices. ISC leverages the SA Agent MIB to monitor SLA performance on a 24 x 7 basis. Using the MIB, you can monitor network traffic for the popular protocols: Dynamic Host Configuration Protocol (DHCP), Domain Name System (DNS), File Transfer Protocol (FTP), Hyper text Transfer Protocol (HTTP), Internet Control Message Protocol Echo (ICMP Echo), Jitter (voice jitter), Transmission Control Protocol Connect (TCP Connect), and User Datagram Protocol Echo (UDP Echo).

**Note**

SLA uses the embedded Sybase database, independent of whether you choose Oracle as your database.

**Note**

The SLA operations **Create**, **Delete**, **Enable Probes**, **Disable Probes**, **Enable Traps**, and **Disable Traps** automatically result in the creation of a task, which executes the actual operation. You can view the status of the task by navigating **Monitoring > Task Manager > Logs**.

This section explains how to configure SLA probes, collect SLA data, and view SLA reports about these SLA probes.

Before you navigate **Monitoring > SLA**, implement the setup procedures in the “[Setup Prior to Using SLA](#)” section on page 7-14.”

Then navigate **Monitoring > SLA** and you can select one of the following:

- [Probes, page 7-15](#) is the default selection.
- [Reports, page 7-54](#)

Setup Prior to Using SLA

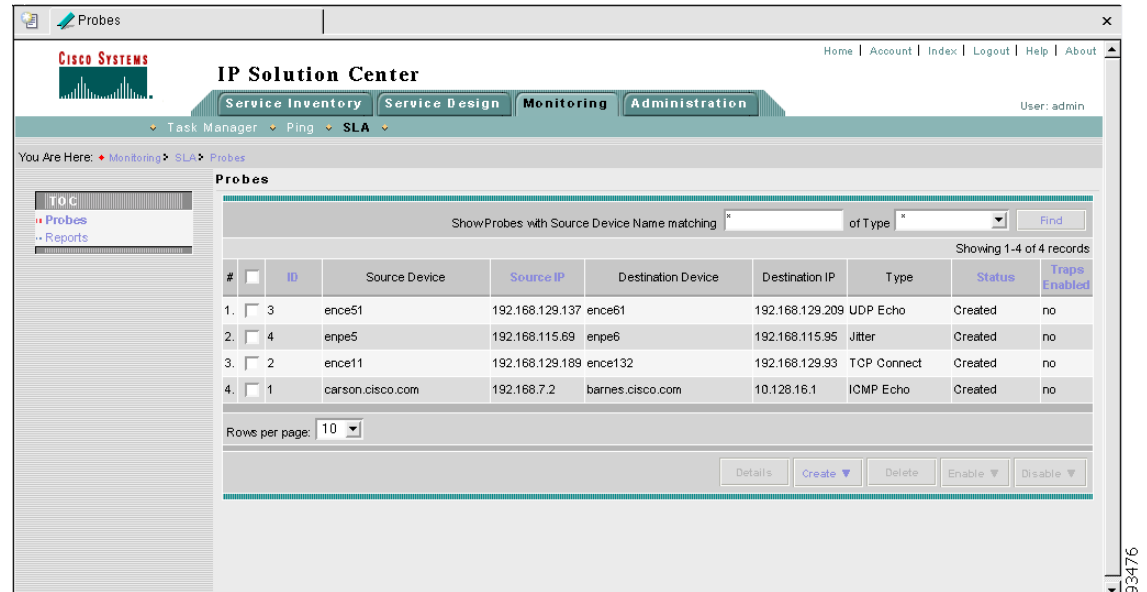
SLA is an SNMP activity. Be sure SNMP is enabled and the SNMP settings on the router match the settings in the repository.

When creating an SLA **From MPLS CPE**, **From MPLS PE**, or **From IPsec CPE (This feature is NOT SUPPORTED in this release.)**, the service requests associated with the devices *must* be in the Deployed state.

Probes

When you navigate **Monitoring > SLA > Probes**, you receive a window as shown in [Figure 7-18](#), “SLA Probes.”

Figure 7-18 SLA Probes



The default button that is enabled is **Create** and from the **Create** drop-down menu, you can choose to create SLA probes **From Any SA Agent Device(s)**; **From MPLS CPE**; **From MPLS PE**; or **From IPsec CPE (This feature is NOT SUPPORTED in this release.)**. However, if you select one or more existing probes by clicking the row(s) of existing probe(s), to select the specific probe(s), or you click the box in the header row, to select all the probes, then you have access to the other buttons, **Details**, **Delete**, **Enable**, and **Disable**. For **Enable** and **Disable**, the drop-down menu contains options to enable or disable SLA **Probes** and SLA **Traps**.

At the top of this window, for **Show Probes with Source Device Name matching** you can enter the beginning characters of the names you want to match followed by *; then for **of Type**, you can keep the default of *, which searches for all the protocol types, or you can select the drop-down menu to select a specific protocol type; and then click **Find**.

At the bottom of the window, you can change the number of rows shown on this window in **Rows per page**. Click the drop-down menu and you can select **5**, **10**, **20**, **30**, **40**, or **All**.

The explanations of the buttons and subsequent drop-down menus is given as follows:

- [Create From Any SA Agent Device\(s\), page 7-16](#) This section explains how to create probes from any SA Agent device(s).
- [Create from MPLS CPE, page 7-22](#) This section explains how to create probes from an MPLS CPE.
- [Create From MPLS PE or MVRP-CE, page 7-29](#) This section explains how to create probes from an MPLS PE.
- [Create from IPsec CPE, page 7-36](#) - **This feature is NOT SUPPORTED in this release.** -
- [Protocols, page 7-41](#) This section is common Probes information for each of the **Create** paths.
- [Details, page 7-46](#) This section gives details about a specified probe or all the probes.

- [Delete, page 7-47](#) This section explains how to delete a probe.
- [Enable Probes, page 7-49](#) This section explains how to enable the Status and move it from Created to Active.
- [Enable Traps, page 7-50](#) This section explains how to enable traps.
- [Disable Probes, page 7-51](#) This section explains how to disable the Status and move it from Active to Created.
- [Disable Traps, page 7-53](#) This sections explains how to disable traps.

Create From Any SA Agent Device(s)

When you navigate **Monitoring > SLA > Probes**, the default is the **Probes** page with only the **Create** button enabled. From the **Create** drop-down menu, you can select **From Any SA Agent Device(s)**, as shown in [Figure 7-19](#), “[SLA Probes > Create > From Any SA Agent Device\(s\)](#).”



Note

IP connectivity must be available between the SA Agent devices.

Figure 7-19 *SLA Probes > Create > From Any SA Agent Device(s)*

You then proceed through the following steps:

- Step 1** The first window to appear is as shown in [Figure 7-20](#), “[SLA Common Parameters](#).”

Figure 7-20 SLA Common Parameters

Accept the defaults or change the information in the fields of the common SLA parameters, as follows, and then click **Next**:

- **SLA Life** (required) is the number of seconds that the probe is active (with the maximum value of a 32-bit integer in seconds). If the value is set to **-1**, the typical and default value, the probe is active forever.
- **Threshold** (required) is an integer that defines the threshold limit in milliseconds. When this threshold is exceeded and traps are enabled, a trap is sent. The maximum value is the maximum value of a 32-bit integer. If the SA Agent operation time exceeds this limit, the threshold violation is recorded by the SA Agent. The value for **Threshold** must not exceed the value for **Timeout**. The default value is **5000**.
- **Timeout** (required) is the duration in milliseconds to wait for an SA Agent operation completion. The value for **Timeout** must be less than or equal to the value for **Frequency** and greater than or equal to the value for **Threshold**. The default value is **5000**.
- **Frequency (0 - 604800)** (required) is the duration in seconds between initiating each SA Agent operation. The value for **Frequency** must be greater than or equal to the value for **Timeout**. The default value is **60**.
- **TOS Category** (default: **Precedence**) If you select the **Precedence** radio button for **TOS Category**, you have one set of type of service (TOS) values. If you select the **DSCP** radio button for **TOS Category**, you have a different set of TOS values.
- **TOS** (required) is an integer. The range and meanings of the values depend on whether the radio button in the **TOS Category** is set to **Precedence** (values: 0 to 7) or **DSCP** (values: 0 to 63).
 - When the **TOS Category** is set to **Precedence**, the valid values are **0** to **7**. These values represent the three most significant bits of the ToS field in an IP header. The default value is **0**. The meanings of the **Precedence** values are specified in [Table 7-1, “Meanings of Precedence Values.”](#)

**Note**

Type of Service does not apply to the **DNS** and **DHCP** types of SLA probes. ISC ignores any ToS value set for these two types of SLA probes. For example, if you first select a ToS value of 5, then select the **DNS**, **DHCP**, and **ICMP Echo** protocols for an SLA probe, ISC applies the selected ToS value to the **ICMP Echo** probe only.

Table 7-1 Meanings of Precedence Values

ToS Value	Binary Value	Meaning
7	111	Network Control
6	110	Internetwork Control
5	101	CRITIC/ECP
4	100	Flash Override
3	011	Flash
2	010	Immediate
1	001	Priority
0	000	Routine

- When the **TOS Category** is set to **DSCP**, the valid values are **0** to **63**. These values represent the six most significant bits of this ToS field in an IP header. The default value is **0**. The interpretation of these **TOS** values is user specified.

**Note**

ISC maps the 0 - 7 PRECEDENCE values to the three most significant ToS bits by left-shifting the value by five positions. Similarly, the 0 - 63 DSCP values are left-shifted by two positions.

- **Keep History** (default: deselected) If you select the **Keep History** check box, you indicate to keep the recent History Table on the router. Specifically, it is kept in the SA Agent MIB that keeps the raw round-trip time (RTT) SLA measurement. This selection also enables you to indicate the **Number of Buckets** of raw history data to keep. If you leave the default of a deselected check box for **Keep History**, no raw history data is kept. **Keep History** is not supported for **HTTP** and **Jitter**.
- **Number of Buckets (1 - 60)** (required) The default is **15** when the **Keep History** box is selected. The range is 1 to 60 and indicates the number of most recent raw data entries to be kept in the raw history data. When the specified **Number of Buckets** is surpassed, removal of buckets starts with the oldest bucket to keep only the number of raw data entries specified.
- **Enable Traps** (default: deselected, which means No) If you select the **Enable Traps** box, the created SLA is configured to send three types of traps. This selection also enables you to indicate the **Falling Threshold**. If you leave the **Enable Traps** box deselected, the traps are disabled on the SLAs created in this task.
- **Falling Threshold (1 - Threshold)** (required) The default is **3000** in milliseconds when the **Enable Traps** box is selected. The range is **1** to the **Threshold** value in milliseconds. When traps are enabled and the delay meets the specified number of milliseconds, a trap is sent.

Step 2 The next window to appear is as shown in [Figure 7-21](#), “SLA Source Devices.”

Figure 7-21 SLA Source Devices

The screenshot shows the 'SLA Source Devices' configuration window in the Cisco IP Solution Center. The window has a title bar 'SLA Source Devices' and a navigation bar with tabs: 'Service Inventory', 'Service Design', 'Monitoring' (selected), and 'Administration'. Below the navigation bar, there are links for 'Task Manager', 'Ping', and 'SLA'. The main content area is titled 'SLA Source Devices' and shows a 'Mode: ADDING' sidebar with steps 1 through 5. Step 2, 'Source Devices', is selected. The main area displays a table with columns for '#', 'Device Name', 'Interface', and 'Type'. Below the table is a 'Rows per page' dropdown set to 10, and 'Add' and 'Delete' buttons. At the bottom are '< Back', 'Next >', 'Finish', and 'Cancel' buttons. The status bar indicates '- Step 2 of 5 -'.

- Step 3** Click the **Add** button and a window appears as shown in Figure 7-22, “SLA Devices > Add,” which lists all the devices in the database that have a minimum of one interface. At the top of this window you can select the drop-down menu for **Show Devices with** and select **Device Name**, **Device Group**, or **Collection Zone**; then for **matching**, enter the beginning characters of the names you want to match followed by *; and then click **Find**. Click the box next to each row for the device you want to select or click the box in the heading row to select all the devices. Then click **Select**.

**Note**

At the bottom of the window, you can change the number of rows shown on this window in **Rows per page**. Click the drop-down menu and you can select **5**, **10**, **20**, **30**, **40**, or **All**. At the bottom of the page, you can also click on other pages to view and make all your choices.

Figure 7-22 SLA Devices > Add

Devices associated with SLA

Show Devices with matching

Showing 1-10 of 23 records

#	☐	Device Name	Management IP Address	Type
1.	☐	ence11	192.168.115.70	Cisco IOS Device
2.	☐	ence132	192.168.115.116	Cisco IOS Device
3.	☐	ence21	192.168.115.73	Cisco IOS Device
4.	☐	ence51	192.168.115.81	Cisco IOS Device
5.	☐	ence61	192.168.115.87	Cisco IOS Device
6.	☐	ipsec-cpe-london	66.66.66.66	Cisco IOS Device
7.	☐	ipsec-cpe-ny	55.55.55.55	Cisco IOS Device
8.	☐	barnes.cisco.com	10.128.32.1	Cisco IOS Device
9.	☐	carson.cisco.com	10.128.32.254	Cisco IOS Device
10.	☐	enpe1	192.168.115.64	Cisco IOS Device

Rows per page:

Step 4 You return to [Figure 7-21](#) and the newly added source device(s) appear. The information about this source device is specified in the following columns:

- **Device Name** You can click this heading and the device names are organized alphabetically.
- **Interface** You can click **Select** and from the resulting window, you can update the IP address. At the top of the window, you can click the drop-down menu for **Show Device Interfaces with** and select either **Interface Name** or **IP Address** and for **matching** you can enter the beginning characters of the names you want to match followed by *; and then click **Find**. At the bottom of the window, you can click the drop-down menu for **Rows per page** and select **5**, **10**, **20**, **30**, **40**, or **All**. You can select one radio button for an interface and click **Select** and the IP address changes in [Figure 7-21](#).
- **Type** Gives you the type of the source device.

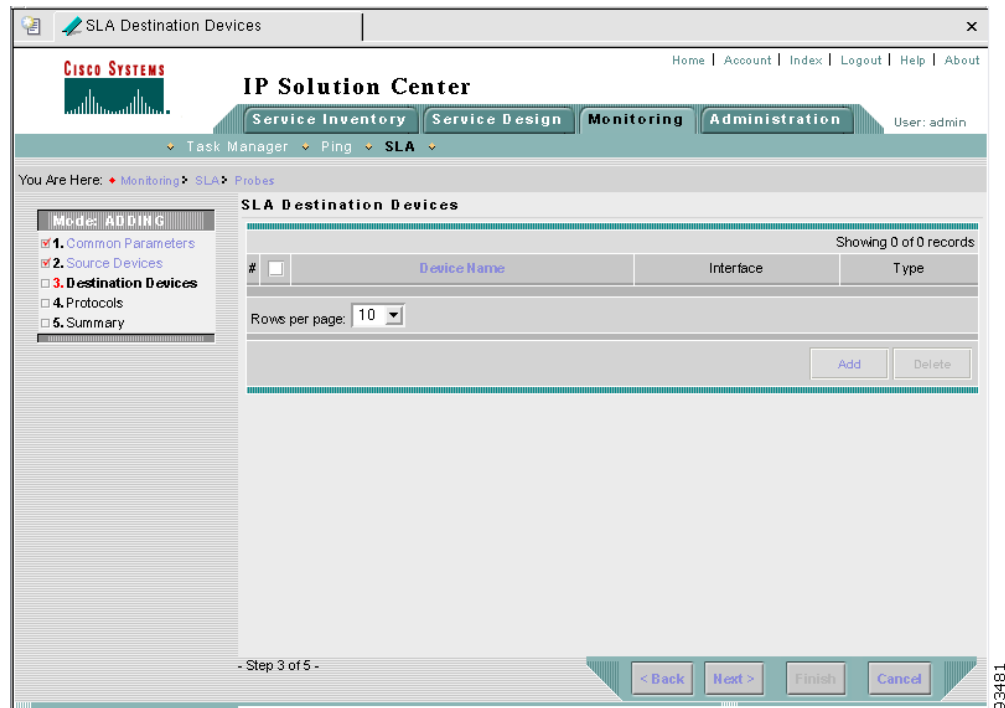
Step 5 You can repeat [Step 3](#) to **Add** more devices, or you can **Delete** any of the currently selected source devices. To **Delete**, click the box next to each row for the device you want to delete or click the box in the heading row to select all the devices; then click **Delete**.

**Note**

There is no second chance for deleting source devices. There is no confirm window.

Step 6 Click **Next**. The next window to appear is as shown in [Figure 7-23](#), “SLA Destination Devices.”

Figure 7-23 SLA Destination Devices



- Step 7** Click the **Add** button and a window appears as shown in Figure 7-22, “SLA Devices > Add.” At the top of this window you can select the drop-down menu for **Show Devices with** and select **Device Name**, **Device Group**, or **Collection Zone**; then for **matching**, enter the beginning characters of the names you want to match followed by *; and then click **Find**. Click the box next to each row for the device you want to select or click the box in the heading row to select all the devices. Then click **Select**.

**Note**

At the bottom of the window, you can change the number of rows shown on this window in **Rows per page**. Click the drop-down menu and you can select **5**, **10**, **20**, **30**, **40**, or **All**. At the bottom of the page, you can also click on other pages to view and make all your choices.

- Step 8** You return to Figure 7-23 and the newly added destination device(s) appear. The information about this destination device is specified in the following columns:
- **Device Name** You can click this heading and the device names are organized alphabetically.
 - **Interface** You can click **Select** and from the resulting window, you can update the IP address. At the top of the window you can click the drop-down menu for **Show Device Interfaces with** and select either **Interface Name** or **IP Address** and for **matching** you can enter the beginning characters of the names you want to match followed by *; and then click **Find**. At the bottom of the window, you can click the drop-down menu for **Rows per page** and select **5**, **10**, **20**, **30**, **40**, or **All**. You can **Select** one radio button for an interface and click **Select** and the IP address changes in Figure 7-23.
 - **Type** Gives you the type of the source device.

- Step 9** You can repeat [Step 7](#) to **Add** more devices, or you can **Delete** any of the currently selected source devices. To **Delete**, click the box next to each row for the device you want to delete or click the box in the heading row to select all the devices; then click **Delete**.

**Note**

There is no second chance for deleting destination devices. There is no confirm window.

- Step 10** Click **Next**. Proceed to the “[Protocols](#)” section on page 7-41.”

Create from MPLS CPE

When you navigate **Monitoring > SLA > Probes** and select no probe, you have access to the **Create** button. From the **Create** drop-down menu, you can select **From MPLS CPE**, as shown in [Figure 7-24](#), “[SLA Probes > Create > From MPLS CPE](#).”

Figure 7-24 *SLA Probes > Create > From MPLS CPE*

The screenshot shows the 'Probes' configuration interface. At the top, there is a search bar with the text 'Show Probes with Source Device Name matching' followed by a text input field and a dropdown menu for 'of Type'. Below the search bar, it says 'Showing 0 of 0 records'. A table with the following columns is visible: #, ID, Source Device, Source IP, Destination Device, Destination IP, Type, Status, and Traps Enabled. Below the table, there is a 'Rows per page' dropdown set to 'All' and a 'Go to page' section with '1 of 1' and a 'Go' button. At the bottom, there are buttons for 'Details', 'Create', 'Enable', 'Disable', and 'Delete'. The 'Create' button is highlighted, and its dropdown menu is open, showing four options: 'From Any SA Agent Device(s)', 'From MPLS CPE', 'From MPLS PE or MVRP-CE', and 'From IPsec CPE'. The 'From MPLS CPE' option is selected.

You then proceed through the following steps:

- Step 1** The first window to appear is as shown in [Figure 7-25](#), “[SLA Common Parameters](#).”

Figure 7-25 SLA Common Parameters

Accept the defaults or change the information in the fields of the common SLA parameters, as follows, and then click **Next**:

- **SLA Life** (required) is the number of seconds that the probe is active (with the maximum value of a 32-bit integer in seconds). If the value is set to **-1**, the typical and default value, the probe is active forever.
- **Threshold** (required) is an integer that defines the threshold limit in milliseconds. When this threshold is exceeded and traps are enabled, a trap is sent. The maximum value is the maximum value of a 32-bit integer. If the SA Agent operation time exceeds this limit, the threshold violation is recorded by the SA Agent. The value for **Threshold** must not exceed the value for **Timeout**. The default value is **5000**.
- **Timeout** (required) is the duration in milliseconds to wait for an SA Agent operation completion. The value for **Timeout** must be less than or equal to the value for **Frequency** and greater than or equal to the value for **Threshold**. The default value is **5000**.
- **Frequency (0 - 604800)** (required) is the duration in seconds between initiating each SA Agent operation. The value for **Frequency** must be greater than or equal to the value for **Timeout**. The default value is **60**.
- **TOS Category** (default: **Precedence**) If you select the **Precedence** radio button for **TOS Category**, you have one set of type of service (TOS) values. If you select the **DSCP** radio button for **TOS Category**, you have a different set of TOS values.
- **TOS** (required) is an integer. The range and meanings of the values depend on whether the radio button in the **TOS Category** is set to **Precedence** (values: 0 to 7) or **DSCP** (values: 0 to 63).
 - When the **TOS Category** is set to **Precedence**, the valid values are **0** to **7**. These values represent the three most significant bits of the ToS field in an IP header. The default value is **0**. The meanings of the **Precedence** values are specified in [Table 7-2, “Meanings of Precedence Values.”](#)

**Note**

Type of Service does not apply to the **DNS** and **DHCP** types of SLA probes. ISC ignores any ToS value set for these two types of SLA probes. For example, if you first select a ToS value of 5, then select the **DNS**, **DHCP**, and **ICMP Echo** protocols for an SLA probe, ISC applies the selected ToS value to the **ICMP Echo** probe only.

Table 7-2 Meanings of Precedence Values

ToS Value	Binary Value	Meaning
7	111	Network Control
6	110	Internetwork Control
5	101	CRITIC/ECP
4	100	Flash Override
3	011	Flash
2	010	Immediate
1	001	Priority
0	000	Routine

- When the **TOS Category** is set to **DSCP**, the valid values are **0** to **63**. These values represent the six most significant bits of this ToS field in an IP header. The default value is **0**. The interpretation of these **TOS** values is user specified.

**Note**

ISC maps the 0 - 7 PRECEDENCE values to the three most significant ToS bits by left-shifting the value by five positions. Similarly, the 0 - 63 DSCP values are left-shifted by two positions.

- **Keep History** (default: deselected) If you select the **Keep History** box, you indicate to keep the recent History Table on the router. Specifically, it is kept in the SA Agent MIB that keeps the raw round-trip time (RTT) SLA measurement. This selection also enables you to indicate the **Number of Buckets** of raw history data to keep. If you leave the default of a deselected check box for **Keep History**, no raw history data is kept. **Keep History** is not supported for **HTTP** and **Jitter**.
- **Number of Buckets (1 - 60)** (required) The default is **15** when the **Keep History** check box is selected. The range is 1 to 60 and indicates the number of most recent raw data entries to be kept in the raw history data. When the specified **Number of Buckets** is surpassed, removal of buckets starts with the oldest bucket to keep only the number of raw data entries specified.
- **Enable Traps** (default: deselected, which means No) If you select the **Enable Traps** check box, the created SLA is configured to send three types of traps. This selection also enables you to indicate the **Falling Threshold**. If you leave the **Enable Traps** check box deselected, the traps are disabled on the SLAs created in this task.
- **Falling Threshold (1 - Threshold)** (required) The default is **3000** in milliseconds when the **Enable Traps** box is selected. The range is **1** to the **Threshold** value in milliseconds. When traps are enabled and the delay meets the specified number of milliseconds, a trap is sent.

Step 2 The next window to appear is as shown in [Figure 7-26](#), “SLA CPE Parameters.”

Figure 7-26 SLA CPE Parameters

VPN Information	
VPN :	Select
Customer:	
Source Device	
CPE :	
CPE Interface :	
Destination Device(s)	
Type:	☒ Connected PE ☐ CPEs
Connected PE:	
Connected PE Interface:	

- Step 3** Click the **Select** button for **VPN** and a window appears as shown in Figure 7-27, “Select VPN,” which lists all the VPNs in the database.

Figure 7-27 Select VPN

#	Select	VPN Name	Customer Name
1.	☐	Customer1_VPN	Customer1
2.	☐	VPN-1	Customer2

At the top of this window you can select the drop-down menu for **Show VPNs with** and select **VPN Name** or **Customer Name**; then for **matching**, enter the beginning characters of the names you want to match followed by *; and then click **Find**. Click the box next to each row for the VPN you want to select. Then click **Select**.

**Note**

At the bottom of the window, you can change the number of rows shown on this window in **Rows per page**. Click the drop-down menu and you can select **5**, **10**, **20**, **30**, **40**, or **All**.

- Step 4** You return to Figure 7-26 and the newly added VPN and Customer information appear and a **Select** button appears for **CPE**. You can change the VPN by repeating Step 3.

- Step 5** Click the **Select** button for **CPE** and a window appears as shown in Figure 7-28, “Select CPE,” which lists the CPEs associated with the selected VPN. Click the box next to the row for the CPE you want to select. Then click **Select**.

**Note**

At the bottom of the window, you can change the number of rows shown on this window in **Rows per page**. Click the drop-down menu and you can select **5**, **10**, **20**, **30**, **40**, or **All**.

Figure 7-28 Select CPE

Showing 1-2 of 2 records

#	Select	Customer Name	Site Name	Device Name	Management Type
1.	☐	Customer1	Site-ence51	ence51	MANAGED
2.	☐	Customer1	Site-ence61	ence61	MANAGED

Rows per page: 10

Select Cancel

- Step 6** You return to [Figure 7-26](#) and the newly added CPE and its first interface appears. You can change the CPE by repeating [Step 5](#).
- Step 7** If you want to change the default **CPE Interface** information that appears, click **Select** and you receive a window as shown in [Figure 7-29](#), “Interfaces.”

Figure 7-29 Interfaces

Interfaces for device **ence51**

Show Device Interfaces with matching

Showing 1-6 of 6 records

#	Select	Name	IP Address	Interface Logical Name
1.	☐	Ethernet0	192.168.129.137/30	
2.	☐	Ethernet1	10.5.5.1/30	
3.	☐	FastEthernet0		
4.	☐	Loopback0	192.168.115.81/32	
5.	☐	Loopback1	11.11.11.1/32	
6.	☐	Loopback2	12.12.12.1/32	

Rows per page: 10

Select Cancel

At the top of this window you can select the drop-down menu for **Show Device Interfaces with** and select **Interface Name** or **IP Address**; then for **matching**, enter the beginning characters of the names you want to match followed by *; and then click **Find**. Click the box next to the row for the VPN you want to select. Then click **Select**.

**Note**

At the bottom of the window, you can change the number of rows shown on this window in **Rows per page**. Click the drop-down menu and you can select **5**, **10**, **20**, **30**, **40**, or **All**.

- Step 8** You return to [Figure 7-26](#) and the newly added **CPE Interface** appears. You can change the CPE Interface by repeating [Step 7](#).
- Step 9** You can keep the default **Type**, by leaving the radio button for **Connected PE** chosen, which creates an SLA between the CPE and its directly connected PE, or you can select the radio button for **CPEs** in the same VPN. If you keep the default of **Connected PE**, proceed to [Step 10](#). If you click the **CPEs** radio button, proceed to [Step 13](#).

- Step 10** Click **Select** for **Connected PE Interface** and a window appears as shown in [Figure 7-30](#), “**Connected PE Interface**.”

Figure 7-30 Connected PE Interface

Interfaces for device **enpe5**

Show Device Interfaces with matching

Showing 1-9 of 9 records

#	Select	Name	IP Address	Interface Logical Name
1.	☐	FastEthernet1/1		
2.	☐	Loopback0	192.168.115.69/32	
3.	☐	Switch1		
4.	☐	Switch1.1	10.10.10.13/30	
5.	☐	Switch1.100	14.14.14.1/30	
6.	☐	Switch1.120	10.10.10.13/30	
7.	☐	Switch1.152	192.168.12.17/30	
8.	☐	Switch1.400		
9.	☐	Tunnel1	10.10.10.5/30	

Rows per page:

At the top of this window you can select the drop-down menu for **Show Device Interfaces with** and select **Interface Name** or **IP Address**; then for **matching**, enter the beginning characters of the names you want to match followed by *; and then click **Find**. Click the box next to the row for the Name you want to select. Then click **Select**.



Note

At the bottom of the window, you can change the number of rows shown on this window in **Rows per page**. Click the drop-down menu and you can select **5**, **10**, **20**, **30**, **40**, or **All**.

- Step 11** You return to [Figure 7-26](#) and the newly added **Connected PE Interface** appears. You can change the Connected PE Interface by repeating [Step 10](#).
- Step 12** Click **Next** and proceed to the “**Protocols**” section on page 7-41.
- Step 13** When you click **CPEs**, the window is as shown in [Figure 7-31](#), “**CPEs**.”

Figure 7-31 CPEs

SLA Cpe Parameters

IP Solution Center

Service Inventory | Service Design | **Monitoring** | Administration

User: admin

You Are Here: Monitoring > SLA > Probes

SLA Cpe Parameters

Modes: **ADDING**

- ☒ 1. Common Parameters
- ☐ 2. SLA Devices
- ☐ 3. Protocols
- ☐ 4. Summary

VPN Information

VPN: Customer1_VPN [Select](#)

Customer: Customer1

Source Device

CPE: ence51 [Select](#)

CPE Interface: 192.168.129.137 [Select](#)

Destination Device(s)

Type: ☐ Connected PE ☒ CPEs

CPEs: Showing 0 of 0 records [Select](#)

#	Device Name	Interface
Showing 0 of 0 records		

Rows per page: 10

- Step 2 of 4 -

[< Back](#) [Next >](#) [Finish](#) [Cancel](#)

- Step 14** Click the **Select** button for **CPEs** and a window appears as shown in Figure 7-32, “[Select CPE Associated with the Specified VPN](#),” which lists all the CPEs associated with the specified VPN in the database.

Figure 7-32 Select CPE Associated with the Specified VPN

CPEs associated with Customer1_VPN				
Showing 1-2 of 2 records				
#	☐	Customer Name	Site Name	Device Name
1.	☐	Customer1	Site-ence51	ence51
2.	☐	Customer1	Site-ence61	ence61
Rows per page: 10				
Select Cancel				

Select the check box next to the row(s) for the CPE(s) you want to select or the check box in the header row to select all the listed CPEs. Then click **Select**.

**Note**

Do *not* add a device chosen as a **Source Device** to **Destination Device(s)**.

**Note**

At the bottom of the window, you can change the number of rows shown on this window in **Rows per page**. Click the drop-down menu and you can select **5**, **10**, **20**, **30**, **40**, or **All**.

Step 15 You return to [Figure 7-31](#) and the newly added **Device Name** appears.

Step 16 Click **Select** in the **Interface** column and a window appears as in [Figure 7-29](#).

At the top of this window you can select the drop-down menu for **Show Device Interfaces with** and select **Interface Name** or **IP Address**; then for **matching**, enter the beginning characters of the names you want to match followed by *; and then click **Find**. Click the box next to the row for the CPE you want to select. Then click **Select**.



Note

At the bottom of the window, you can change the number of rows shown on this window in **Rows per page**. Click the drop-down menu and you can select **5, 10, 20, 30, 40**, or **All**.

Step 17 You return to [Figure 7-31](#) and the newly added **CPE Interface** appears. You can change the CPE Interface by repeating [Step 16](#).

Step 18 Select the check box next to each row for the Devices you want to remove or select the check box in the heading row to remove all the Devices. Then click the **Remove** button and a window as shown in [Figure 7-31](#) appears without the removed Device(s).

Step 19 When [Figure 7-31](#) reflects what you want, click **Next** and proceed to the “[Protocols](#)” section on [page 7-41](#).

Create From MPLS PE or MVRF-CE

When you navigate **Monitoring > SLA > Probes** and select no probe, you have access to the **Create** button. From the **Create** drop-down menu, you can select **From MPLS PE or MVRF-CE**, as shown in [Figure 7-33](#), “[SLA Probes > Create > From MPLS PE or MVRF-CE](#).”

Figure 7-33 *SLA Probes > Create > From MPLS PE or MVRF-CE*

You then proceed through the following steps:

Step 1 The first window to appear is as shown in [Figure 7-34](#), “[SLA Common Parameters](#).”

Figure 7-34 SLA Common Parameters

SLA Common Parameters

Home | Account | Index | Logout | Help | About

Service Inventory Service Design **Monitoring** Administration

User: admin

Task Manager Ping SLA

You Are Here: Monitoring > SLA > Probes

Mode: ADDING

- ☒ 1. Common Parameters
- ☐ 2. Source Devices
- ☐ 3. Destination Devices
- ☐ 4. Protocols
- ☐ 5. Summary

SLA Common Parameters

SLA Life *	-1	(secs)
Threshold *	5000	(msecs)
Timeout *	5000	(msecs)
Frequency (0 - 604800) *	60	(secs)
TOS Category:	☒ Precedence ☐ DSCP	
TOS (0 - 7) *	0	
Keep History:	☐	
Number of Buckets (1 - 60) *	15	
Enable Traps:	☐	
Falling Threshold (1 - Threshold) *	3000	(msecs)

Note: * - Required Field

- Step 1 of 5 -

< Back Next > Finish Cancel

Accept the defaults or change the information in the fields of the common SLA parameters, as follows, and then click **Next**:

- **SLA Life** (required) is the number of seconds that the probe is active (with the maximum value of a 32-bit integer in seconds). If the value is set to **-1**, the typical and default value, the probe is active forever.
- **Threshold** (required) is an integer that defines the threshold limit in milliseconds. When this threshold is exceeded and traps are enabled, a trap is sent. The maximum value is the maximum value of a 32-bit integer. If the SA Agent operation time exceeds this limit, the threshold violation is recorded by the SA Agent. The value for **Threshold** must not exceed the value for **Timeout**. The default value is **5000**.
- **Timeout** (required) is the duration in milliseconds to wait for an SA Agent operation completion. The value for **Timeout** must be less than or equal to the value for **Frequency** and greater than or equal to the value for **Threshold**. The default value is **5000**.
- **Frequency (0 - 604800)** (required) is the duration in seconds between initiating each SA Agent operation. The value for **Frequency** must be greater than or equal to the value for **Timeout**. The default value is **60**.
- **TOS Category** (default: **Precedence**) If you select the **Precedence** radio button for **TOS Category**, you have one set of type of service (TOS) values. If you select the **DSCP** radio button for **TOS Category**, you have a different set of TOS values.
- **TOS** (required) is an integer. The range and meanings of the values depend on whether the radio button in the **TOS Category** is set to **Precedence** (values: 0 to 7) or **DSCP** (values: 0 to 63).
 - When the **TOS Category** is set to **Precedence**, the valid values are **0** to **7**. These values represent the three most significant bits of the ToS field in an IP header. The default value is **0**. The meanings of the **Precedence** values are specified in [Table 7-3, “Meanings of Precedence Values.”](#)

**Note**

Type of Service does not apply to the **DNS** and **DHCP** types of SLA probes. ISC ignores any ToS value set for these two types of SLA probes. For example, if you first select a ToS value of 5, then select the **DNS**, **DHCP**, and **ICMP Echo** protocols for an SLA probe, ISC applies the selected ToS value to the **ICMP Echo** probe only.

Table 7-3 Meanings of Precedence Values

ToS Value	Binary Value	Meaning
7	111	Network Control
6	110	Internetwork Control
5	101	CRITIC/ECP
4	100	Flash Override
3	011	Flash
2	010	Immediate
1	001	Priority
0	000	Routine

- When the **TOS Category** is set to **DSCP**, the valid values are **0** to **63**. These values represent the six most significant bits of this ToS field in an IP header. The default value is **0**. The interpretation of these **TOS** values is user specified.

**Note**

ISC maps the 0 - 7 PRECEDENCE values to the three most significant ToS bits by left-shifting the value by five positions. Similarly, the 0 - 63 DSCP values are left-shifted by two positions.

- **Keep History** (default: deselected) If you select the **Keep History** check box, you indicate to keep the recent History Table on the router. Specifically, it is kept in the SA Agent MIB that keeps the raw round-trip time (RTT) SLA measurement. This selection also enables you to indicate the **Number of Buckets** of raw history data to keep. If you leave the default of a deselected check box for **Keep History**, no raw history data is kept. **Keep History** is not supported for **HTTP** and **Jitter**.
- **Number of Buckets (1 - 60)** (required) The default is **15** when the **Keep History** check box is selected. The range is 1 to 60 and indicates the number of most recent raw data entries to be kept in the raw history data. When the specified **Number of Buckets** is surpassed, removal of buckets starts with the oldest bucket to keep only the number of raw data entries specified.
- **Enable Traps** (default: deselected, which means No) If you select the **Enable Traps** check box, the created SLA is configured to send three types of traps. This selection also enables you to indicate the **Falling Threshold**. If you leave the **Enable Traps** box deselected, the traps are disabled on the SLAs created in this task.
- **Falling Threshold (1 - Threshold)** (required) The default is **3000** in milliseconds when the **Enable Traps** box is selected. The range is **1** to the **Threshold** value in milliseconds. When traps are enabled and the delay meets the specified number of milliseconds, a trap is sent.

Step 2 The next window to appear is as shown in [Figure 7-35](#), “SLA CPE Parameters.”

Figure 7-35 SLA CPE Parameters

VPN Information

VPN :

Customer:

Source Device

PE :

PE Interface :

Destination Device(s)

Type: ☒ Connected CPE ☐ PEs

Connected CPE:

Connected CPE Interface:

- Step 3** Click the **Select** button for **VPN** and a window appears as shown in Figure 7-36, “Select VPN,” which lists all the VPNs in the database. At the top of this window you can select the drop-down menu for **Show VPNs with** and select **VPN Name** or **Customer Name**; then for **matching**, enter the beginning characters of the names you want to match followed by *; and then click **Find**. Click the box next to the row for the VPN you want to select. Then click **Select**.

**Note**

At the bottom of the window, you can change the number of rows shown on this window in **Rows per page**. Click the drop-down menu and you can select **5**, **10**, **20**, **30**, **40**, or **All**.

Figure 7-36 Select VPN

VPN for SLA Creation

Show VPNs with matching

Showing 1-2 of 2 records

#	Select	VPN Name	Customer Name
1.	☐	Customer1_VPN	Customer1
2.	☐	VPN-1	Customer2

Rows per page: 10

- Step 4** You return to Figure 7-35 and the newly added VPN and Customer information appears. You can change the VPN and Customer by repeating Step 3.
- Step 5** Click the new **Select** button for **PE** and a window appears as shown in Figure 7-37, “Select PE,” which lists all the PEs associated with the selected VPN. Click the box next to the row for the PE you want to select. Then click **Select**.

**Note**

At the bottom of the window, you can change the number of rows shown on this window in **Rows per page**. Click the drop-down menu and you can select **5**, **10**, **20**, **30**, **40**, or **All**.

Figure 7-37 Select PE

#	Select	Provider Name	Region Name	Device Name	Role Type
1.	☐	Provider1	US	enpe5	PE_POP
2.	☐	Provider1	US	enpe6	PE_POP

Showing 1-2 of 2 records

Rows per page: 10

Select Cancel

Step 6 You return to [Figure 7-35](#) and the newly added PE information appears. You can change the PE by repeating [Step 5](#).

Step 7 Click the new **Select** button for **PE Interface** and a window appears as shown in [Figure 7-38](#), “**Select Device Interface**,” which lists all the PE Interfaces in the database. At the top of this window you can select the drop-down menu for **Show Device Interfaces with** and select **Interface Name** or **IP Address**; then for **matching**, enter the beginning characters of the names you want to match followed by *; and then click **Find**. Click the box next to the row for the Device Interface you want to select. Then click **Select**.

**Note**

At the bottom of the window, you can change the number of rows shown on this window in **Rows per page**. Click the drop-down menu and you can select **5**, **10**, **20**, **30**, **40**, or **All**.

Figure 7-38 Select Device Interface

#	Select	Name	IP Address	Interface Logical Name
1.	☐	FastEthernet1/1		
2.	☐	Loopback0	192.168.115.69/32	
3.	☐	Switch1		
4.	☐	Switch1.1	10.10.10.13/30	
5.	☐	Switch1.100	14.14.14.1/30	
6.	☐	Switch1.120	10.10.10.13/30	
7.	☐	Switch1.152	192.168.12.17/30	
8.	☐	Switch1.400		
9.	☐	Tunnel1	10.10.10.5/30	

Showing 1-9 of 9 records

Rows per page: 10

Select Cancel

Step 8 You return to [Figure 7-35](#) and the newly added **PE Interface** information appears. You can change the PE Interface by repeating [Step 7](#).

Step 9 You can keep the default **Type**, by leaving the radio button for **Connected CPE** chosen or you can select the radio button for **PEs**. If you keep the default of **Connected PE**, proceed to [Step 10](#). If you click the **PEs** radio button, proceed to [Step 13](#).

- Step 10** Click **Select** for **Connected PE Interface** and a window appears as shown in [Figure 7-39](#), “**Connected PE Interface**.”

Figure 7-39 Connected PE Interface

Interfaces for device **enpe5**

Show Device Interfaces with matching

Showing 1-9 of 9 records

#	Select	Name	IP Address	Interface Logical Name
1.	☐	FastEthernet1/1		
2.	☐	Loopback0	192.168.115.69/32	
3.	☐	Switch1		
4.	☐	Switch1.1	10.10.10.13/30	
5.	☐	Switch1.100	14.14.14.1/30	
6.	☐	Switch1.120	10.10.10.13/30	
7.	☐	Switch1.152	192.168.12.17/30	
8.	☐	Switch1.400		
9.	☐	Tunnel1	10.10.10.5/30	

Rows per page:

At the top of this window you can select the drop-down menu for **Show Device Interfaces with** and select **Interface Name** or **IP Address**; then for **matching**, enter the beginning characters of the names you want to match followed by *; and then click **Find**. Click the box next to the row for the VPN you want to select. Then click **Select**.



Note

At the bottom of the window, you can change the number of rows shown on this window in **Rows per page**. Click the drop-down menu and you can select **5**, **10**, **20**, **30**, **40**, or **All**.

- Step 11** You return to [Figure 7-35](#) and the newly added **Connected PE Interface** appears. You can change the Connected PE Interface by repeating [Step 10](#).
- Step 12** Click **Next** and proceed to the “**Protocols**” section on page 7-41.
- Step 13** When you click **PEs**, the window is as shown in [Figure 7-40](#), “**PEs**.”

Figure 7-40 PEs

- Step 14** Click the **Select** button for **PE** and a window appears as shown in Figure 7-41, “**Select PE Associated with the Specified VPN**,” which lists all the PEs associated with the specified VPN of the source PE.

Figure 7-41 Select PE Associated with the Specified VPN

PEs associated with Customer1_VPN					
Showing 1-2 of 2 records					
#	☐	Provider Name	Region Name	Device Name	Role Type
1.	☐	Provider1	US	enpe5	PE_POP
2.	☐	Provider1	US	enpe6	PE_POP
Rows per page: 10 v					
					Select Cancel

Select the check box(es) next to the row(s) for the PE you want to select or the check box in the header row to select all the listed PEs. Then click **Select**.

**Note**

Do *not* add a device chosen as a **Source Device** to **Destination Device(s)**.

**Note**

At the bottom of the window, you can change the number of rows shown on this window in **Rows per page**. Click the drop-down menu and you can select **5**, **10**, **20**, **30**, **40**, or **All**.

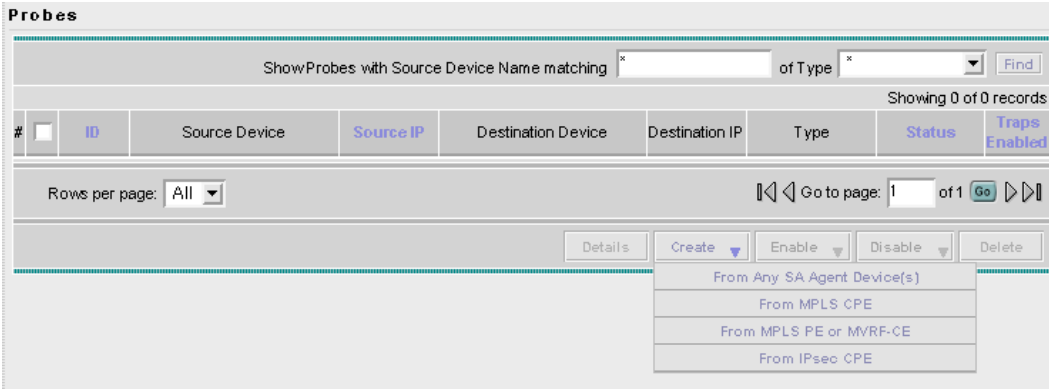
- Step 15** You return to [Figure 7-40](#) and the newly added **Device Name** appears.
- Step 16** Click **Select** in the **Interface** column and a window appears as in [Figure 7-39](#).
At the top of this window you can select the drop-down menu for **Show Device Interfaces with** and select **Interface Name** or **IP Address**; then for **matching**, enter the beginning characters of the names you want to match followed by *; and then click **Find**. Click the box next to the row for the VPN you want to select. Then click **Select**.
-  **Note** At the bottom of the window, you can change the number of rows shown on this window in **Rows per page**. Click the drop-down menu and you can select **5, 10, 20, 30, 40**, or **All**.
- Step 17** You return to [Figure 7-40](#) and the newly added **PE Interface** appears. You can change the PE Interface by repeating [Step 16](#).
- Step 18** Select the check box next to each row for the Devices you want to remove or select the check box in the heading row to select all the Devices you want to remove. Then click the **Remove** button and a window as shown in [Figure 7-40](#) appears without the removed Device(s).
- Step 19** When [Figure 7-40](#) reflects what you want, click **Next** and proceed to the “[Protocols](#)” section on [page 7-41](#).

Create from IPsec CPE

- This feature is NOT SUPPORTED in this release. -

When you navigate **Monitoring > SLA > Probes** and select no probe, you have access to the **Create** button. From the **Create** drop-down menu, you can select **From IPsec CPE**, as shown in [Figure 7-42](#), “[SLA Probes > Create > From IPsec CPE](#).”

Figure 7-42 *SLA Probes > Create > From IPsec CPE*



You then proceed through the following steps:

- Step 1** The first window to appear is as shown in [Figure 7-34](#), “[SLA Common Parameters](#).”

Figure 7-43 SLA Common Parameters

Accept the defaults or change the information in the fields of the common SLA parameters, as follows, and then click **Next**:

- **SLA Life** (required) is the number of seconds that the probe is active (with the maximum value of a 32-bit integer in seconds). If the value is set to **-1**, the typical and default value, the probe is active forever.
- **Threshold** (required) is an integer that defines the threshold limit in milliseconds. When this threshold is exceeded and traps are enabled, a trap is sent. The maximum value is the maximum value of a 32-bit integer. If the SA Agent operation time exceeds this limit, the threshold violation is recorded by the SA Agent. The value for **Threshold** must not exceed the value for **Timeout**. The default value is **5000**.
- **Timeout** (required) is the duration in milliseconds to wait for an SA Agent operation completion. The value for **Timeout** must be less than or equal to the value for **Frequency** and greater than or equal to the value for **Threshold**. The default value is **5000**.
- **Frequency (0 - 604800)** (required) is the duration in seconds between initiating each SA Agent operation. The value for **Frequency** must be greater than or equal to the value for **Timeout**. The default value is **60**.
- **TOS Category** (default: **Precedence**) If you select the **Precedence** radio button for **TOS Category**, you have one set of type of service (TOS) values. If you select the **DSCP** radio button for **TOS Category**, you have a different set of TOS values.
- **TOS** (required) is an integer. The range and meanings of the values depend on whether the radio button in the **TOS Category** is set to **Precedence** (values: 0 to 7) or **DSCP** (values: 0 to 63).
 - When the **TOS Category** is set to **Precedence**, the valid values are **0** to **7**. These values represent the three most significant bits of the ToS field in an IP header. The default value is **0**. The meanings of the **Precedence** values are specified in [Table 7-4, “Meanings of Precedence Values.”](#)

**Note**

Type of Service does not apply to the **DNS** and **DHCP** types of SLA probes. ISC ignores any ToS value set for these two types of SLA probes. For example, if you first select a ToS value of 5, then select the **DNS**, **DHCP**, and **ICMP Echo** protocols for an SLA probe, ISC applies the selected ToS value to the **ICMP Echo** probe only.

Table 7-4 Meanings of Precedence Values

ToS Value	Binary Value	Meaning
7	111	Network Control
6	110	Internetwork Control
5	101	CRITIC/ECP
4	100	Flash Override
3	011	Flash
2	010	Immediate
1	001	Priority
0	000	Routine

- When the **TOS Category** is set to **DSCP**, the valid values are **0** to **63**. These values represent the six most significant bits of this ToS field in an IP header. The default value is **0**. The interpretation of these **TOS** values is user specified.

**Note**

ISC maps the 0 - 7 PRECEDENCE values to the three most significant ToS bits by left-shifting the value by five positions. Similarly, the 0 - 63 DSCP values are left-shifted by two positions.

- **Keep History** (default: deselected) If you select the **Keep History** check box, you indicate to keep the recent History Table on the router. Specifically, it is kept in the SA Agent MIB that keeps the raw round-trip time (RTT) SLA measurement. This selection also enables you to indicate the **Number of Buckets** of raw history data to keep. If you leave the default of a deselected check box for **Keep History**, no raw history data is kept. **Keep History** is not supported for **HTTP** and **Jitter**.
- **Number of Buckets (1 - 60)** (required) The default is **15** when the **Keep History** check box is selected. The range is 1 to 60 and indicates the number of most recent raw data entries to be kept in the raw history data. When the specified **Number of Buckets** is surpassed, removal of buckets starts with the oldest bucket to keep only the number of raw data entries specified.
- **Enable Traps** (default: deselected, which means No) If you select the **Enable Traps** check box, the created SLA is configured to send three types of traps. This selection also enables you to indicate the **Falling Threshold**. If you leave the **Enable Traps** box deselected, the traps are disabled on the SLAs created in this task.
- **Falling Threshold (1 - Threshold)** (required) The default is **3000** in milliseconds when the **Enable Traps** check box is selected. The range is **1** to the **Threshold** value in milliseconds. When traps are enabled and the delay meets the specified number of milliseconds, a trap is sent.

Step 2 The next window to appear is as shown in [Figure 7-44](#), “SLA CPE Parameters.”

Figure 7-44 SLA CPE Parameters

VPN Information

VPN :

Customer:

Source Device

CPE :

CPE Interface :

Destination Device(s)

CPEs: Showing 0 of 0 records

#	Device Name	Interface

Rows per page: 10

- Step 3** Click the **Select** button for **VPN** and a window appears as shown in Figure 7-45, “**Select VPN**,” which lists all the VPNs in the database. At the top of this window you can select the drop-down menu for **Show VPNs with** and select **VPN Name** or **Customer Name**; then for **matching**, enter the beginning characters of the names you want to match followed by *****; and then click **Find**. Click the box next to the row for the VPN you want to select. Then click **Select**.

**Note**

At the bottom of the window, you can change the number of rows shown on this window in **Rows per page**. Click the drop-down menu and you can select **5**, **10**, **20**, **30**, **40**, or **All**.

Figure 7-45 Select VPN

VPN for SLA Creation

Show VPNs with matching

Showing 1-2 of 2 records

#	Select	VPN Name	Customer Name
1.	☐	Customer1_VPN	Customer1
2.	☐	VPN-1	Customer2

Rows per page: 10

- Step 4** You return to Figure 7-44 and the newly added VPN and Customer information appears. You can change the VPN and Customer by repeating Step 3.
- Step 5** Click the new **Select** button for **CPE** and a window appears as shown in Figure 7-46, “**Select CPE**,” which lists all the CPEs associated with the selected VPN. Click the box next to the row for the CPE you want to select. Then click **Select**.

**Note**

At the bottom of the window, you can change the number of rows shown on this window in **Rows per page**. Click the drop-down menu and you can select **5**, **10**, **20**, **30**, **40**, or **All**.

Figure 7-46 Select CPE

#	Select	Provider Name	Region Name	Device Name	Role Type
1.	☐	Provider1	US	enpe5	PE_POP
2.	☐	Provider1	US	enpe6	PE_POP

Showing 1-2 of 2 records

Rows per page: 10

Select Cancel

- Step 6** You return to [Figure 7-44](#) and the newly added CPE and CPE Interface information appears. You can change the CPE by repeating [Step 5](#).
- Step 7** You can change the CPE Interface by clicking the **Select** button for the CPE Interface and reselecting.
- Step 8** Click the **Select** button for **CPEs** and a window appears as shown in [Figure 7-47](#), “[Select CPE Associated with the Specified VPN](#),” which lists all the CPEs associated with the specified VPN of the source CPE.

Figure 7-47 Select CPE Associated with the Specified VPN

#	Customer Name	Site Name	Device Name	Management Type
1.	☐ Customer1	Site-ence51	ence51	MANAGED
2.	☐ Customer1	Site-ence61	ence61	MANAGED

Showing 1-2 of 2 records

Rows per page: 10

Select Cancel

Select the check box(es) next to the row(s) for the CPE you want to select or select the check box in the header row to select all the listed CPEs. Then click **Select**.

**Note**

Do *not* add a device chosen as a **Source Device** to **Destination Device(s)**.

**Note**

At the bottom of the window, you can change the number of rows shown on this window in **Rows per page**. Click the drop-down menu and you can select **5**, **10**, **20**, **30**, **40**, or **All**.

- Step 9** You return to [Figure 7-44](#) and the newly added devices appear. You can change the device by repeating [Step 8](#).
- Step 10** Click **Select** in the **Interface** column and a window appears as in [Figure 7-39](#).

At the top of this window you can select the drop-down menu for **Show Device Interfaces with** and select **Interface Name** or **IP Address**; then for **matching**, enter the beginning characters of the names you want to match followed by *; and then click **Find**. Click the box next to the row for the VPN you want to select. Then click **Select**.

**Note**

At the bottom of the window, you can change the number of rows shown on this window in **Rows per page**. Click the drop-down menu and you can select **5, 10, 20, 30, 40**, or **All**.

- Step 11** You return to [Figure 7-44](#) and the newly added **CPE Interface** appears. You can change the CPE Interface by repeating [Step 10](#).
- Step 12** Select the check box next to each row for the Devices you want to remove or select the check box in the heading row to select all the Devices you want to remove. Then click the **Remove** button and a window as shown in [Figure 7-44](#) appears without the removed Device(s).
- Step 13** When [Figure 7-44](#) reflects what you want, click **Next** and proceed to the “**Protocols**” section on [page 7-41](#).

Protocols

You navigate to this location after you have completed all the steps in one of the **Create** functions: [Create From Any SA Agent Device\(s\)](#), [page 7-16](#); [Create from MPLS CPE](#), [page 7-22](#); [Create From MPLS PE or MVRP-CE](#), [page 7-29](#); or [Create from IPsec CPE](#), [page 7-36](#). Follow these steps:

- Step 1** The next window to appear is as shown in [Figure 7-48](#), “**Protocols**.” At the bottom of the window, you can change the number of rows shown on this window in **Rows per page**. Click the drop-down menu and you can select **5, 10, 20, 30, 40**, or **All**

Figure 7-48 Protocols

The screenshot shows the 'SLA Protocols' configuration window in the Cisco IP Solution Center. The interface includes a top navigation bar with tabs for 'Service Inventory', 'Service Design', 'Monitoring', and 'Administration'. The 'Monitoring' tab is active. Below this, there's a breadcrumb trail: 'You Are Here: Monitoring > SLA > Probes'. On the left, a sidebar shows a tree view with 'Mode: ADDING' and steps 1 through 5. Step 4, 'Protocols', is selected. The main content area features a table titled 'SLA Protocols' with columns: '#', a checkbox, 'Source Device', 'Destination Device', 'Type', and 'Description'. The table is empty, with a message 'Showing 0 of 0 records'. Below the table is a 'Rows per page' dropdown menu set to '10'. At the bottom right of the table area are 'Add' and 'Delete' buttons. At the very bottom of the window are navigation buttons: '< Back', 'Next >', 'Finish', and 'Cancel'. The status bar at the bottom indicates '- Step 4 of 5 -'.

93759

- Step 2** Click the **Add** drop-down menu and select:
- **ICMP Echo** (only available if destination devices are available) Proceed to [Step 3](#).
 - **TCP Connect** (not available for Create from MPLS PE; for all the other Creates, TCP Connect is only available if destination devices are available) Proceed to [Step 4](#).
 - **UDP Echo** (only available if destination devices are available) Proceed to [Step 5](#).
 - **Jitter** (only available if destination devices are available) Proceed to [Step 6](#).
 - **FTP** (not available for Create from MPLS PE) Proceed to [Step 7](#).
 - **DNS** (not available for Create from MPLS PE) Proceed to [Step 8](#).
 - **HTTP** (not available for Create from MPLS PE) Proceed to [Step 9](#).
 - **DHCP** (not available for Create from MPLS PE) Proceed to [Step 10](#).
- Step 3** From [Step 2](#), if you chose **ICMP Echo**, you receive a window as shown in [Figure 7-49](#), “Protocol ICMP Echo.”

Figure 7-49 Protocol ICMP Echo

Protocol ICMP Echo

Request Size (0 - 16384) * : 28 (bytes)

OK Cancel

Note: * - Required Field

Enter the required information as follows, click **OK**, and then proceed to [Step 11](#).

- **Request Size (0 - 16384)** (required) is a number that represents the number of octets (in bytes) to be placed into the data portion of the packet. The default is **28**.
- Step 4** From [Step 2](#), if you chose **TCP Connect**, you receive a window as shown in [Figure 7-50](#), “Protocol TCP Connect.”

Figure 7-50 Protocol TCP Connect

Protocol TCP Connect

Destination Port (1 - 65535) * : 23

Request Size (1 - 16384): 1 (bytes)

OK Cancel

Note: * - Required Field

Enter the required and optional information as follows, click **OK**, and then proceed to [Step 11](#).

- **Destination Port (1 - 65535)** (required) is the port number on the target to where the monitoring packets is sent. If you do not specify a specific port, port **23** is used.
 - **Request Size (1 - 16384)** (optional) is a number that represents the number of octets (in bytes) to be placed into the data portion of the packet. The default is **1**.
- Step 5** From [Step 2](#), if you chose **UDP Echo**, you receive a window as shown in [Figure 7-51](#), “Protocol UDP Echo.”

Figure 7-51 Protocol UDP Echo

Protocol UDP Echo	
Destination Port (1 - 65535) *	7
Request Size (4 - 8192):	16 (bytes)
OK Cancel	
Note: * - Required Field	

Enter the required and optional information as follows, click **OK**, and then proceed to [Step 11](#).

- **Destination Port (1 - 65535)** (required) is the port number on the target to where the monitoring packets are sent. If you do not specify a specific port, port **7** is used.
- **Request Size (4 - 8192)** (optional) is a number that represents the number of octets (in bytes) to be placed into the data portion of the packet. The default is **16**.

Step 6 From [Step 2](#), if you chose **Jitter**, you receive a window as shown in [Figure 7-52](#), “Protocol Jitter.”

Figure 7-52 Protocol Jitter

Protocol Jitter	
Destination Port (1 - 65535) *	8000
Request Size (16 - 1500):	32 (bytes)
Number of Packets (1 - 1000):	10
Interval (1 - 1000):	20 (msecs)
OK Cancel	
Note: * - Required Field	

Enter the required and optional information as follows, click **OK**, and then proceed to [Step 11](#).

- **Destination Port (1 - 65535)** (required) is the port number on the target to where the monitoring packets are sent. If you do not specify a specific port, port **8000** is used.
- **Request Size (16 - 1500)** (optional) is a number that represents the number of octets (in bytes) to be placed into the data portion of the packet. The default is **32**.
- **Number of Packets (1 - 1000)** (optional) is an integer that represents the number of packets that must be transmitted. The default value is **10**.
- **Interval (1 - 1000)** (optional) is an integer, **1** to **1,000**, that represents the inter-packet delay between packets in milliseconds. The default value is **20**.

Step 7 From [Step 2](#), if you chose **FTP**, you receive a window as shown in [Figure 7-53](#), “Protocol FTP.”

Figure 7-53 Protocol FTP

Protocol FTP	
User Name:	admin
Password:	*****
Host IP Address *:	
File Path *:	
OK Cancel	
Note: * - Required Field	

Enter the required and optional information as follows, click **OK**, and then proceed to [Step 11](#).

- **User Name** (optional) If blank, **anonymous** is used.
- **Password** (optional) If blank, **test** is used.
- **Host IP Address** (required) Enter the IP address for File Transfer Protocol (FTP).
- **File Path** (required) Enter the path of the file you want to FTP on the FTP server.

Step 8 From [Step 2](#), if you chose **DNS**, you receive a window as shown in [Figure 7-54](#), “Protocol DNS.”

Figure 7-54 Protocol DNS

Protocol DNS	
Name Server *:	
Name to be Resolved *:	
Request Size (0 - 16384) *:	1 (bytes)
OK Cancel	
Note: * - Required Field	

Enter the required information as follows, click **OK**, and then proceed to [Step 11](#).

- **Name Server** (required) is the string that specifies the IP address of the name server. The address is in dotted IP address format.
- **Name to be Resolved** (required) is a string that is either the name or the IP address that is to be resolved by the DNS server. If the string is a name, the length is 255 characters. If the string is an IP address, it is in dotted IP address format.
- **Request Size (0 - 16384)** (required) is a number that represents the number of octets (in bytes) to be placed into the data portion of the packet. The default is **1**.

Step 9 From [Step 2](#), if you chose **HTTP**, you receive a window as shown in [Figure 7-55](#), “Protocol HTTP.”

Figure 7-55 Protocol HTTP

Protocol HTTP

Version: 1.0

URL * :

Cache: ☒

Proxy Server:

Name Server:

Operation: HTTPGet

RawRequest * :

Request Size 1 - 16384 * : 1 (bytes)

OK Cancel

Note: * - Required Field

93502

Enter the optional and required information as follows, click **OK**, and then proceed to [Step 11](#).

- **Version** (default: 1.0) is a string that specifies the version of the HTTP server. Do not change this. ISC only supports version 1.0.
- **URL** (required) is a string that represents the URL to which an HTTP probe should communicate, *HTTPServerName[/directory]/filename* or *HTTPServerAddress[/directory]/filename* (for example: **http://www.cisco.com/index.html** or **http://209.165.201.22/index.html**). If you specify the *HTTPServerName*, the **Name Server** is required. If you specify the *HTTPServerAddress*, the **Name Server** is not required.
- **Cache** (default: selected, which means Yes) For a deselected check box, the HTTP request should not download cached pages. For a selected check box, the HTTP request downloads cached pages if available, otherwise the request is forwarded to the HTTP server.
- **Proxy Server** (optional) is a string that represents the proxy server information (with a maximum of 255 characters). The default is the null string.
- **Name Server** (optional, dependent on the **URL** setting) is the string that specifies the IP address of the name server. The address is in dotted IP address format.
- **Operation** (default: **HTTPGet**) If you want **HTTPrAw**, which represents the HTTP request with user defined payload, instead of the default **HTTPGet** which represents the HTTP get request, use the drop-down menu and make that choice.
- **Raw Request** (required if the **Operation** is **HTTPrAw**; not available if the **Operation** is **HTTPGet**) is a string that is only needed if the **Operation** is **HTTPrAw**. It allows you to invoke other types of HTTP operations other than the simple GET operation.
- **Request Size (1 - 16384)** (required) is a number that represents the number of octets (in bytes) to be placed into the data portion of the packet. The default is **28**.

Step 10 From [Step 2](#), if you chose **DHCP**, you have no information to add. Proceed to [Step 11](#).

Step 11 You return to [Figure 7-48](#) and additional columns of information now appear based on the Protocol information you provided. Before you click **Next** to proceed, determine if you want to **Add** more protocols, in which case repeat [Step 2](#) to [Step 10](#), or **Delete** any of the currently selected protocols, in which case, click **Delete** and proceed much as in [Step 2](#) to [Step 10](#) to now delete protocols.

**Note**

There is no second chance for deleting destination devices. There is no confirm window.

- Step 12** The next window to appear is a Probe Creation Task Summary window that shows the **Description** (date and time created), **Common Parameters**, **Source Devices**, **Destination Devices**, and **Protocols** that you have defined. If all exists the way you want it, click **Finish**. Otherwise, click **Back** and make corrections.

Details

When you navigate **Monitoring > SLA > Probes**, you can get details by following these steps:

- Step 1** Select an existing probe by selecting the corresponding check box for which you want details. Then you have access to the **Details** button, as shown in [Figure 7-56, “SLA Probes > Details.”](#)

Figure 7-56 SLA Probes > Details

The screenshot shows the Cisco IP Solution Center interface. The breadcrumb trail is **Monitoring > SLA > Probes**. The page title is **Probes**. Below the title, there is a search bar and a table of probes. The table has the following columns: #, ID, Source Device, Source IP, Destination Device, Destination IP, Type, Status, and Traps Enabled. The second row (ID 4) is selected. The 'Details' button is visible at the bottom right of the table.

#	ID	Source Device	Source IP	Destination Device	Destination IP	Type	Status	Traps Enabled
1.	☐ 3	ence51	192.168.129.137	ence61	192.168.129.209	UDP Echo	Created	no
2.	☒ 4	enpe5	192.168.115.69	enpe6	192.168.115.95	Jitter	Created	no
3.	☐ 2	ence11	192.168.129.189	ence132	192.168.129.93	TCP Connect	Created	no
4.	☐ 1	carson.cisco.com	192.168.7.2	barnes.cisco.com	10.128.16.1	ICMP Echo	Created	no

- Step 2** After you click the **Details** button, you receive a window as shown in [Figure 7-57, “SLA Probes Details.”](#) This includes the **Common Attributes** information defined when you first **Create** and the **Protocol Specific Attributes** information defined in the section [Protocols](#).

Figure 7-57 SLA Probes Details

Probe UDP Echo	
Common Attributes	
Source IP Address:	192.168.129.137
Destination IP Address:	192.168.129.209
Status:	Created
SLA Life:	unlimited
Threshold:	5000 msec
Timeout:	5000 msec
Frequency:	60 sec
TOS Category:	PRECEDENCE
TOS:	0
Keep History:	false
Traps Enabled:	false
Protocol Specific Attributes	
Destination Port:	7
Request Size:	16 bytes
OK	

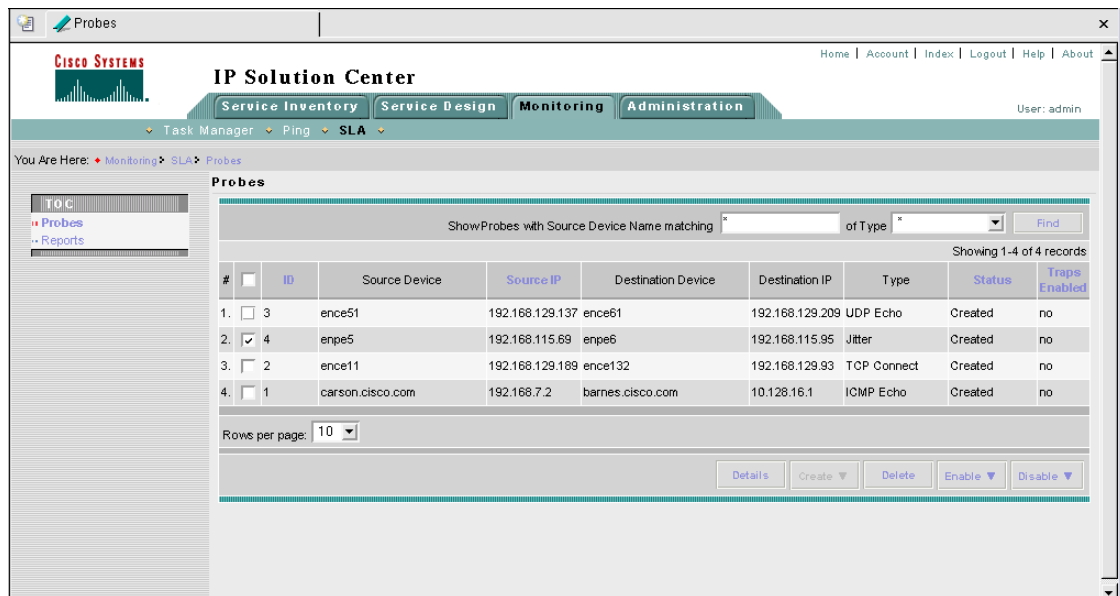
- Step 3** Click **OK** to return to a window as shown in [Figure 7-56](#). You can continue to select more **Details** or complete another function.

Delete

When you navigate **Monitoring > SLA > Probes**, you can delete probes from the list by following these steps:

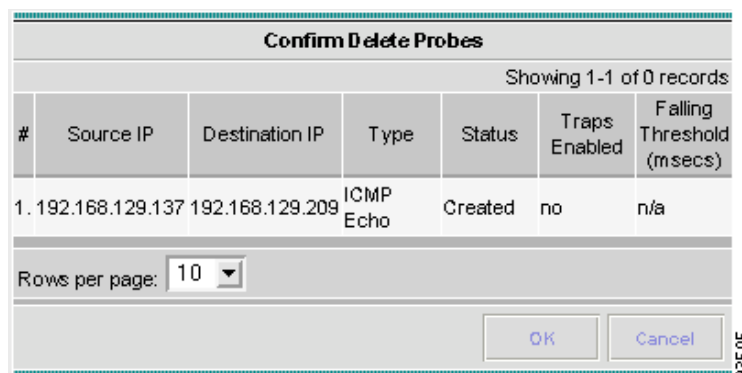
- Step 1** Select one or more existing probes by clicking on the box(es) for the row(s) of existing probe(s) or you can click the box in the header row, to select all the probes. Then you have access to the **Delete** button, as shown in [Figure 7-58](#), “[SLA Probes > Delete](#).”

Figure 7-58 SLA Probes > Delete



Step 2 After you click the **Delete** button, a window as shown in Figure 7-59, “Confirm Delete Probes,” appears.

Figure 7-59 Confirm Delete Probes



Step 3 Click **OK** if Figure 7-59 reflects what you want to delete or click **Cancel** if it does not.

**Note**

After the probe is deleted, it is deleted from the probe list page but still remains in the database.

**Note**

At the bottom of the window, you can change the number of rows shown on this window in **Rows per page**. Click the drop-down menu and you can select **5**, **10**, **20**, **30**, **40**, or **All**.

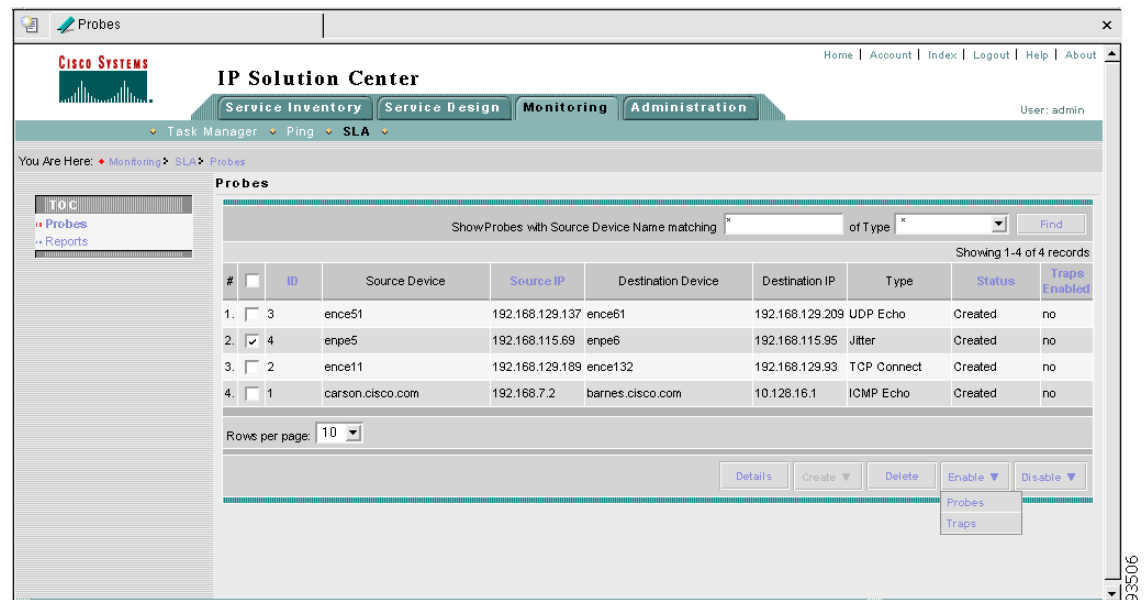
Step 4 You return to Figure 7-58 with updated information.

Enable Probes

When you navigate **Monitoring > SLA > Probes**, you can enable probes by following these steps:

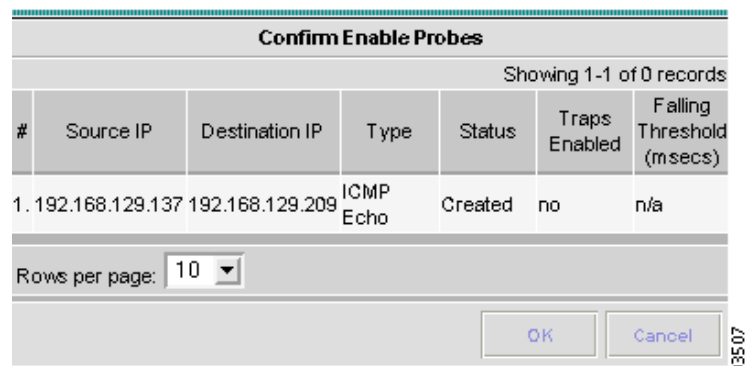
- Step 1** Select one or more existing probes by clicking on the box(es) for the row(s) of existing probe(s) or you can click the box in the header row, to select all the probes. Then you have access to the **Enable** button. From the **Enable** drop-down menu, you have access to **Probes**, as shown in [Figure 7-60](#), “**SLA Probes > Enable > Probes.**”

Figure 7-60 *SLA Probes > Enable > Probes*



- Step 2** After you select **Enable > Probes**, a window as shown in [Figure 7-61](#), “**Confirm Enable Probes.**” appears. All the traps have 3000 ms as the falling threshold set automatically.

Figure 7-61 *Confirm Enable Probes*



- Step 3** Click **OK** if [Figure 7-61](#) reflects the probes you want to enable or click **Cancel** if it does not. In both cases, you return to [Figure 7-60](#).

**Note**

At the bottom of the window, you can change the number of rows shown on this window in **Rows per page**. Click the drop-down menu and you can select **5, 10, 20, 30, 40**, or **All**.

Step 4

If this was successful, you receive a Status window with a green check mark for **Succeeded**. The Status column is set to **Active** when the probe is created successfully on the router.

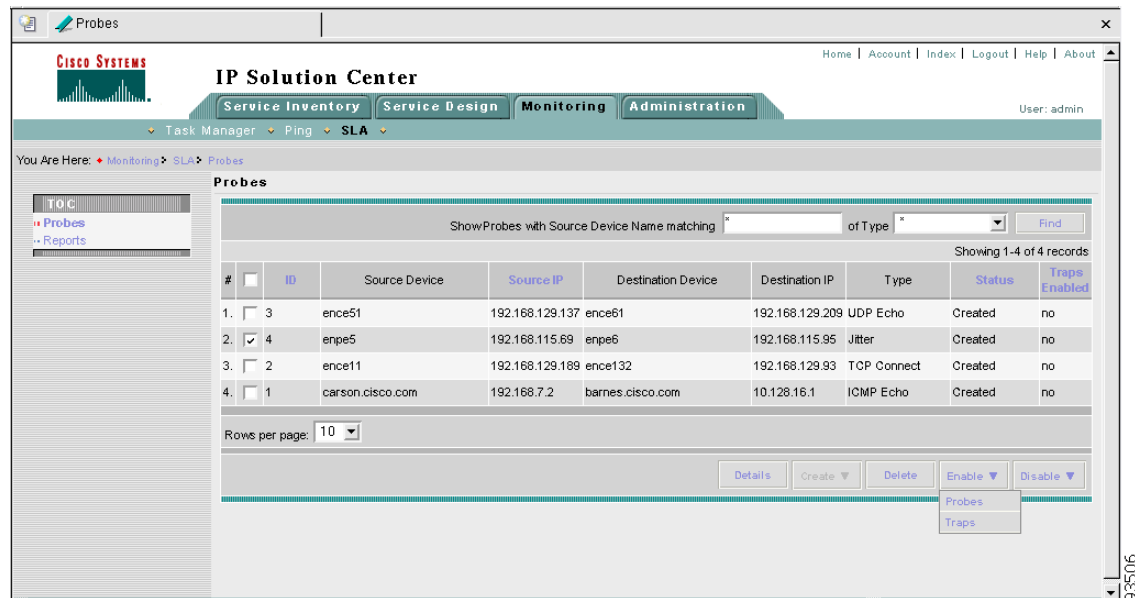
Enable Traps

When you navigate **Monitoring > SLA > Probes**, you can enable traps by following these steps:

Step 1

Select one or more existing probes by clicking on the box(es) for the row(s) of existing probe(s) or you can click the box in the header row, to select all the probes. Then you have access to the **Enable** button. From the **Enable** drop-down menu, you have access to **Traps**, as shown in [Figure 7-62, “SLA Probes > Enable > Traps.”](#)

Figure 7-62 SLA Probes > Enable > Traps

**Step 2**

After you select **Enable > Traps**, a window as shown in [Figure 7-63, “Confirm Enable Traps,”](#) appears.

Figure 7-63 Confirm Enable Traps

Confirm Enable Traps						
Showing 1-1 of 0 records						
#	Source IP	Destination IP	Type	Status	Traps Enabled	Falling Threshold (msecs)
1.	192.168.129.137	192.168.129.209	ICMP Echo	Created	no	n/a

Rows per page: 10

OK Cancel

Step 3 Click **OK** if [Figure 7-63](#) reflects the traps you want to enable or click **Cancel** if it does not. In both cases you return to [Figure 7-62](#).

**Note**

At the bottom of the window, you can change the number of rows shown on this window in **Rows per page**. Click the drop-down menu and you can select **5, 10, 20, 30, 40**, or **All**.

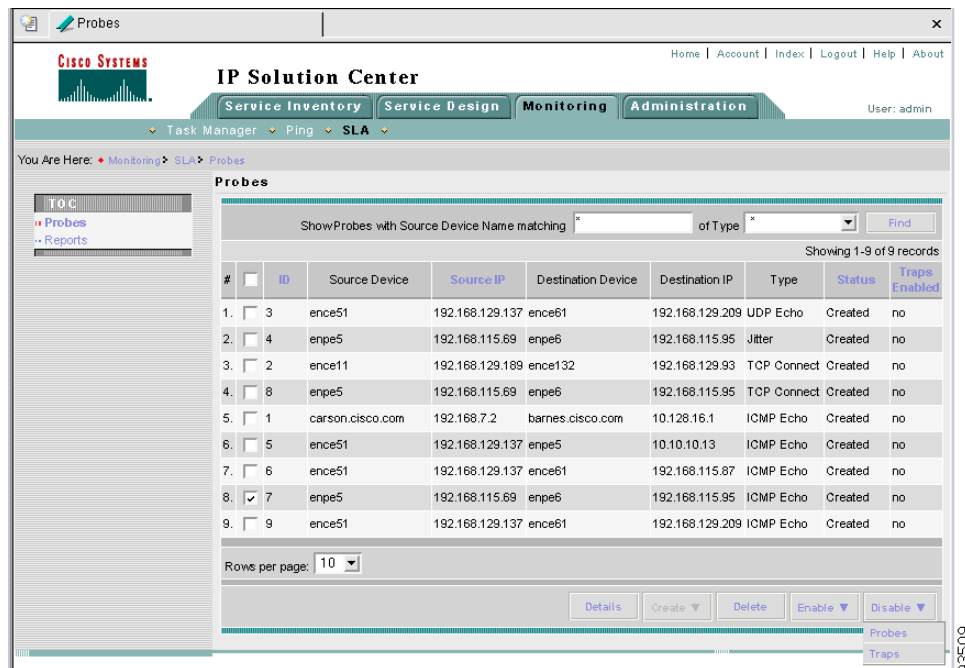
Step 4 If this was successful, you receive a Status window with a green check mark for **Succeeded**. The Traps Enabled column is set to **yes** when the probes on the router are successfully changed.

Disable Probes

When you navigate **Monitoring > SLA > Probes**, you can use **Disable Probes** to delete probes on the devices. Follow these steps:

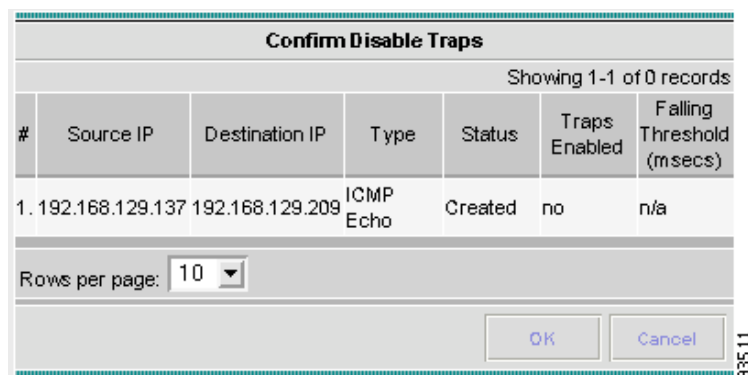
Step 1 Select one or more enabled probes by clicking on the box(es) for the row(s) of existing probe(s) or you can click the box in the header row, to select all the probes. Then you have access to the **Disable** button. From the **Disable** drop-down menu, you have access to **Probes**, as shown in [Figure 7-64](#), “**SLA Probes > Disable > Probes**.”

Figure 7-64 SLA Probes > Disable > Probes



Step 2 After you select **Disable > Probes**, a window as shown in Figure 7-65, “Confirm Disable Probes,” appears.

Figure 7-65 Confirm Disable Probes



Step 3 Click **OK** if Figure 7-65 reflects the probes you want to disable or click **Cancel** if it does not. In both cases you return to Figure 7-64.

**Note**

At the bottom of the window, you can change the number of rows shown on this window in **Rows per page**. Click the drop-down menu and you can select **5, 10, 20, 30, 40**, or **All**.

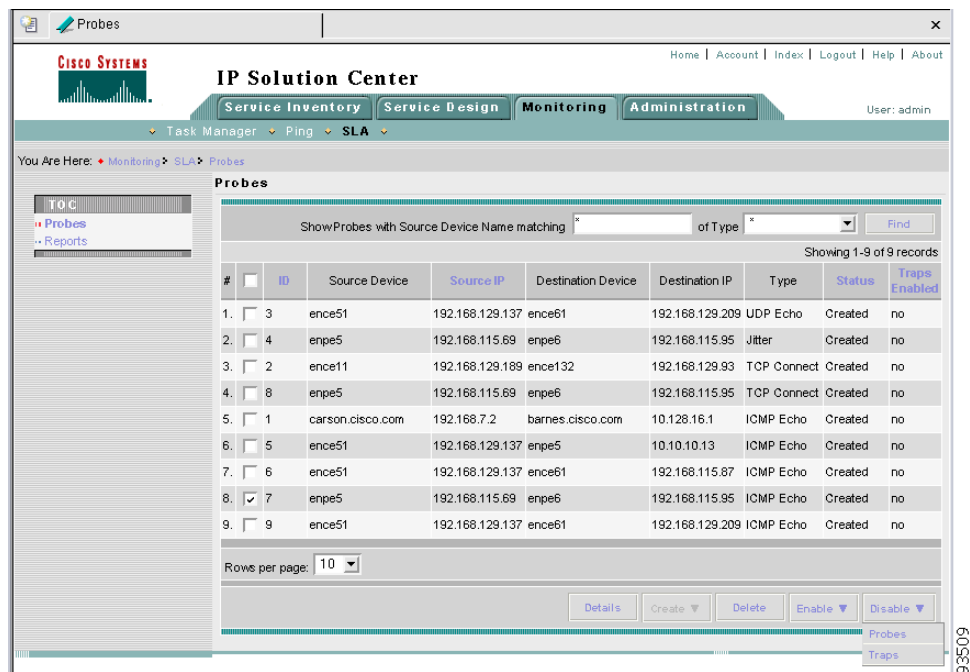
Step 4 If this was successful, you receive a Status window with a green check mark for **Succeeded**, and the probe’s status becomes Disabled when the probe on the router is successfully removed.

Disable Traps

When you navigate **Monitoring > SLA > Probes**, you can disable traps by following these steps:

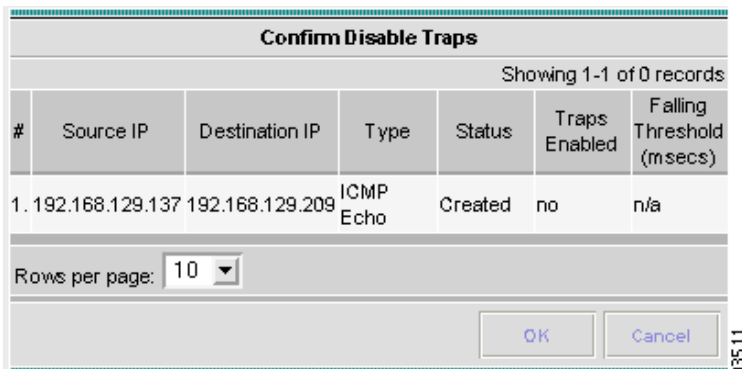
- Step 1** Select one or more existing probes by clicking on the box(es) for the row(s) of existing probe(s) or you can click the box in the header row, to select all the probes. Then you have access to the **Disable** button. From the **Disable** drop-down menu, you have access to **Traps**, as shown in [Figure 7-66](#), “**SLA Probes > Disable > Traps**.”

Figure 7-66 SLA Probes > Disable > Traps



- Step 2** After you select **Disable > Traps**, a window as shown in [Figure 7-67](#), “**Confirm Disable Traps**,” appears.

Figure 7-67 Confirm Disable Traps



- Step 3** Click **OK** if [Figure 7-67](#) reflects the traps you want to disable or click **Cancel** if it does not. In both cases you return to [Figure 7-66](#).

**Note**

At the bottom of the window, you can change the number of rows shown on this window in **Rows per page**. Click the drop-down menu and you can select **5, 10, 20, 30, 40**, or **All**.

Step 4

If this was successful, you receive a Status window with a green check mark for **Succeeded**. The traps are disabled when the probes on the router are successfully changed.

Reports

When you navigate **Monitoring > SLA > Reports**, you receive a window as shown in [Figure 7-68](#), “SLA Reports.”

Figure 7-68 SLA Reports



You can then click on any of the following choices and receive that report

- [Summary Report, page 7-55](#) This report summarizes all the information other than for HTTP and Jitter (ICMP Echo, TCP Connect, UDP Echo, FTP, DNS, and DHCP).
- [HTTP Report, page 7-57](#) This is a summary report for HTTP information.
- [Jitter Report, page 7-58](#) This is a summary report for Jitter information.
- [Summary CoS Report, page 7-58](#) This report a summary report for Class of Service (CoS) other than for HTTP and Jitter (ICMP Echo, TCP Connect, UDP Echo, FTP, DNS, and DHCP).
- [HTTP CoS Report, page 7-59](#) This report is for HTTP CoS information.
- [Jitter CoS Report, page 7-59](#) This report is for Jitter CoS information.

Summary Report

From [Figure 7-68](#), select **Summary Report** and proceed as follows:

- Step 1** The resulting window is shown in [Figure 7-69](#), “Parameters of Summary Report.”

Figure 7-69 Parameters of Summary Report

Parameters of Summary Report

Layout

Value Displayed *: All

Aggregate By *: ☒ All ☐ Customer ☐ Provider ☐ VPN ☐ Source Router ☐ Probe

Timeline *: ☐ All ☐ Yearly ☐ Monthly ☒ Weekly ☐ Daily ☐ Hourly

2003 JUN 5 00:00

Filtering

Customer: Select

Provider: Select

VPN: Select

Source Routers: Select

Destination Routers: Select

Probes: Select

Precedence: All

DSCP: All

Probe Type: All

OK Cancel

Note: * - Required Field

93838

- Step 2** For [Figure 7-69](#), fill in the **Layout** fields, as follows:

- **Value Displayed** (required) (default: **All**) Click the drop-down menu and select one of the following:
 - **All** to display all the values
 - **Connections (#)** to display the number of connections
 - **Timeouts (#)** to display the number of timeouts
 - **Connectivity (%)** to display connectivity as a percentage
 - **Threshold Violations (%)** to display threshold violations as a percentage
 - **Max Delay (ms)** to display the maximum delay in milliseconds
 - **Min Delay (ms)** to display the minimum delay in milliseconds
 - **Avg Delay (ms)** to display the average delay in milliseconds.

- **Aggregate By** (required) (default: All) Click the radio button for how you want to aggregate the data, by **All**, **Customer**, **Provider**, **VPN**, **Source Router**, or **Probe**.
- **Timeline** (required) (default: **Weekly**; starting with midnight of the first day of the selected week) Click the radio button for the report data that you want to display, **All** data; **Yearly** data; **Monthly** data; **Weekly** data; **Daily** data; or **Hourly** data. Also click the drop-down menus for the year, month, day of the month, and time of day for which to start the report.

Step 3 For [Figure 7-69](#), fill in the **Filtering** fields, as follows:



Note

The report contains only the data that fulfills all the conditions in the filtering fields (all the conditions are ANDed together).

- **Customer** (optional) Click the **Select** button and from the resulting list of Customers, filter the list if you choose. From the listed Customers, click the radio button for the Customer for which you want this SLA report. Then click **Select**. The result is that you return to [Figure 7-69](#) and the selected customer is listed for **Customer**. You can repeat this process if you want to change your selection.
- **Provider** (optional) Click the **Select** button and from the resulting list of Providers, filter the list if you choose. From the listed Providers, click the radio button for the Provider for which you want this SLA report. Then click **Select**. The result is that you return to [Figure 7-69](#) and the selected provider is listed for **Provider**. You can repeat this process if you want to change your selection.
- **VPN** (optional) Click the **Select** button and from the resulting list of VPNs, filter the list if you choose. From the listed VPNs, click the radio button for the VPN for which you want this SLA report. Then click **Select**. The result is that you return to [Figure 7-69](#) and the selected VPN is listed for **VPN**. You can repeat this process if you want to change your selection.
- **Source Routers** (optional) Click the **Select** button and from the resulting list of devices, filter the list if you choose. From the listed devices, select the check box(es) for device(s) or the check box in the header row to select all the devices for which you want this SLA report. Then click **Select**. The result is that you return to [Figure 7-69](#) and **Source Routers** contains the selected device(s). You can repeat this process if you want to change your selection.
- **Destination Routers** (optional) Click the **Select** button and from the resulting list of devices, filter the list if you choose. From the listed devices, select the check box(es) for device(s) or the check box in the header row to select all the devices for which you want this SLA report. Then click **Select**. The result is that you return to [Figure 7-69](#) and **Destination Routers** contains the selected device(s). You can repeat this process if you want to change your selection.
- **Probes** (optional) Click the **Select** button and from the resulting list of source probes, filter the list if you choose. From the listed source probes, select the check box(es) for source probe(s) or the check box in the header row to select all the source probes for which you want this SLA report. Then click **Select**. The result is that you return to [Figure 7-69](#) and **Probes** contains the selected source probe(s). You can repeat this process if you want to change your selection.
- **Precedence** (default: **All**) Click the drop-down menu to select the other **Precedence** TOS choices, **0** to **7**. These values represent the three most significant bits of the ToS field in an IP header. The meanings of the **Precedence** values are specified in [Table 7-1](#), “[Meanings of Precedence Values](#).”



Note

ISC maps the 0 - 7 PRECEDENCE values to the three most significant ToS bits by left-shifting the value by five positions.

**Note**

Type of Service does not apply to the **DNS** and **DHCP** types of SLA probes. ISC ignores any ToS value set for these two types of SLA probes. For example, if you first select a ToS value of 5, then select the **DNS**, **DHCP**, and **ICMP Echo** protocols for an SLA probe, ISC applies the selected ToS value to the **ICMP Echo** probe only.

- **DSCP** (default: **All**) Click the drop-down menu to select the other **DSCP** TOS choices, **0** to **63**. These values represent the six most significant bits of this ToS field in an IP header. The interpretation of these **TOS** values is user specified.

**Note**

ISC maps the 0 - 63 DSCP values to the six most significant ToS bits by left-shifting the values by two positions.

**Note**

Type of Service does not apply to the **DNS** and **DHCP** types of SLA probes. ISC ignores any TOS value set for these two types of SLA probes. For example, if you first select a TOS value of 5, then select the **DNS**, **DHCP**, and **ICMP Echo** protocols for an SLA probe, ISC applies the selected ToS value to the **ICMP Echo** probe only.

- **Probe Type** (default: **All**) Click the drop-down menu to select from the following types of probes: ICMP Echo; UDP Echo; TCP Connect; HTTP; DNS; Jitter; DHCP; FTP.

**Note**

These probe types are explained in detail in the [“Protocols” section on page 7-41](#).

Step 4 Click **OK** in [Figure 7-69](#) after you have the information you want.

Step 5 The result is a Summary Report with the selections you made listed. You can **Modify**, **Refresh**, **Print**, or **Close** this report with the appropriate button.

**Note**

If you choose **Modify**, you receive a window such as [Figure 7-69](#) in which you can modify your selections as explained in the previous steps.

HTTP Report

From [Figure 7-68](#), select **HTTP Report** and proceed similarly to the [“Summary Report” section on page 7-55](#), with the following exceptions:

- Value Displayed
- There is no **Destination Routers** selection
- There is no **Probe Type** drop-down menu in the equivalent of [Figure 7-69](#), because the probe type is automatically **HTTP**. The result is an HTTP Report.

Jitter Report

From [Figure 7-68](#), select **Jitter Report** and proceed exactly as in the “[Summary Report](#)” section on [page 7-55](#), with only two exceptions. There is no **Destination Routers** selection and there is no **Probe Type** drop-down menu in the equivalent of [Figure 7-69](#), because the probe type is automatically **Jitter**. The result is a Jitter Report.

Summary CoS Report

From [Figure 7-68](#), select **Summary CoS Report** for a summary of the Class of Service (CoS) reports, which are based on the TOS values of the SLA probes, and proceed as follows:

- Step 1** The resulting window is shown in [Figure 7-70](#), “Parameters of CoS Summary Report.”

Figure 7-70 Parameters of CoS Summary Report

Parameters of CoS Summary Report

Layout

Value Displayed :

TOS Type : ☒ Precedence ☐ DSCP

Aggregate By : ☒ All ☐ Customer ☐ Provider ☐ VPN ☐ Source Router ☐ Probe

Timeline : ☐ All ☐ Yearly ☐ Monthly ☒ Weekly ☐ Daily ☐ Hourly

2003 JUN 5 00:00

Filtering

Customer:

Provider:

VPN:

Source Routers:

Destination Routers:

Probes:

Probe Type:

Note: * - Required Field

- Step 2** For [Figure 7-70](#), fill in the **Layout** fields, as shown in [Step 2](#) of the “[Summary Report](#)” section on [page 7-55](#), with the following exception. After **Value Displayed** and before **Aggregate By**, select the radio button **Precedence** (default) or **DSCP** for the new **TOS Type**. The explanations are given in the Filtering section, [Step 3](#) of the “[Summary Report](#)” section on [page 7-55](#).
- Step 3** For [Figure 7-70](#), fill in the **Filtering** fields, as shown in [Step 3](#) of the “[Summary Report](#)” section on [page 7-55](#), with the exception that there are no **Precedence** or **DSCP** drop-down menus, they are now in the **Layout** fields, as explained in [Step 2](#) in this section.
- Step 4** Click **OK** in [Figure 7-70](#) after you have the information you want.

Step 5 The result is a CoS Summary Report with the selections you made listed. You can **Modify**, **Refresh**, **Print**, or **Close** this report with the appropriate button.

**Note**

If you choose **Modify**, you receive a window such as [Figure 7-70](#) in which you can modify your selections as explained in the previous steps.

HTTP CoS Report

From [Figure 7-68](#), select **HTTP Report** and proceed exactly as in the “[Summary CoS Report](#)” section on [page 7-58](#), with only two exceptions. There is no **Destination Routers** selection and there is no **Probe Type** drop-down menu in the equivalent of [Figure 7-70](#), because the probe type is automatically **HTTP**. The result is an HTTP CoS Report. This CoS report is based on the TOS values of the SLA probes.

Jitter CoS Report

From [Figure 7-68](#), select **Jitter Report** and proceed exactly as in the “[Summary CoS Report](#)” section on [page 7-58](#), with only two exceptions. There is no **Destination Routers** selection and there is no **Probe Type** drop-down menu in the equivalent of [Figure 7-70](#), because the probe type is automatically **Jitter**. The result is a Jitter CoS Report. This CoS report is based on the TOS values of the SLA probes.

TEM Performance Report

TEM Performance Report for Traffic Engineering Management is explained in detail in [Cisco IP Solution Center Traffic Engineering Management User Guide, 4.0](#).



Administration

From the Home window of Cisco IP Solution Center (ISC), you receive upon logging in, click the **Administration** tab and you receive a window as shown in [Figure 8-1](#), “Administration Selections.”

Figure 8-1 Administration Selections



Then you can navigate to the following selections:

- **Security, page 8-2** Create and manage Users, User Groups, User Roles, and Object Groups
- **Control Center, page 8-25** Manage ISC configuration, servers, remote installation, and licensing
- **Active Users, page 8-37** View users currently connected to ISC. Disconnect users.
- **User Access Log, page 8-37** View the user access log.
- **Manage TIBCO Rendezvous, page 8-39** Specify attributes for proper messaging among all Java™ Web Start distributed applications.

Security

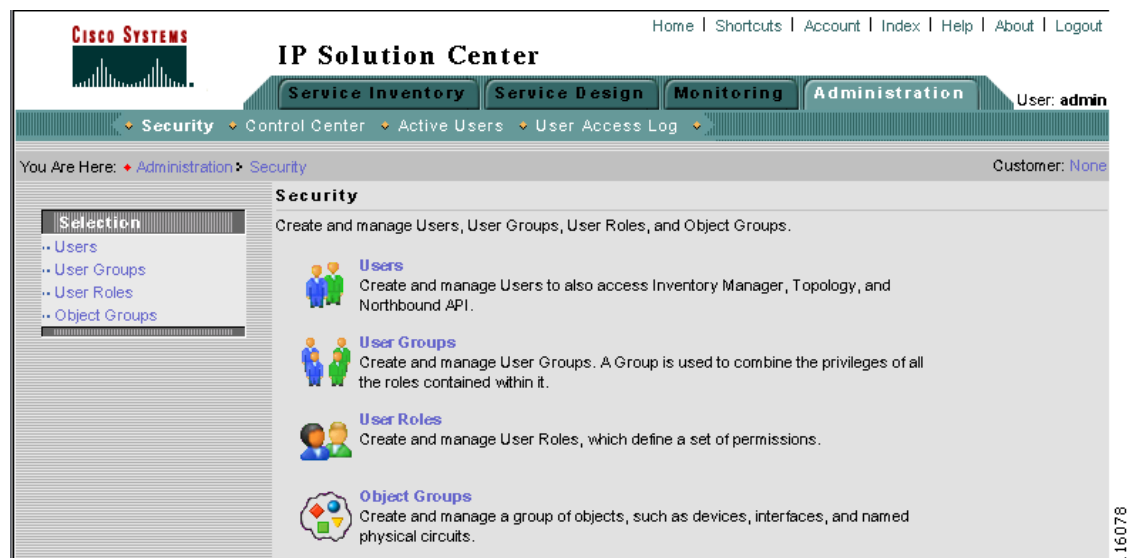
This section describes how system administrators create, edit, and delete users, user groups, and user roles and how privileges are assigned to these entities.

The security features are only accessible to the user **admin** or users with the following roles:

- **SysAdminRole** gives access to all the ISC tools. This is similar to “root” in a UNIX system.
- **UserAdminRole** gives access to only the user management tools in **Administration > Security**.

Navigate **Administration > Security** to access the user management tools. The window shown in [Figure 8-2](#), “Security Window,” appears.

Figure 8-2 Security Window



From the Security window, navigate to the following:

- [Users](#), [page 8-2](#) to manage users
- [User Groups](#), [page 8-8](#) to manage user groups
- [User Roles](#), [page 8-11](#) to manage user roles
- [Object Groups](#), [page 8-18](#) to manage object groups.

For an example of how to use the Users, User Groups, User Roles, and Object Groups, see the “[User Roles Design Example](#)” section on [page 8-22](#).

Users

Navigate **Administration > Security > Users** and follow these steps:

-
- Step 1** The window in [Figure 8-3](#), “Users Window,” appears.

Figure 8-3 Users Window

IP Solution Center

Service Inventory | Service Design | Monitoring | Administration

Security > Control Center > Active Users > User Access Log

You Are Here: Administration > Security > Users

Customer: None

Users

Show users with: User ID Matching * Find

Showing 1 - 21 of 21 records

#	User ID	First Name	Last Name	Work Phone	Mobile Phone
1.	admin	admin	admin		
2.	user-collection	Joe	Collection	(123) 456-7890	(123) 456-7890
3.	user-firewall	Joe	Firewall	(123) 456-7890	(123) 456-7890
4.	user-firewallserviceop	Joe	FirewallServiceOp	(123) 456-7890	(123) 456-7890
5.	user-import	Joe	Import	(123) 456-7890	(123) 456-7890
6.	user-ipsec	Joe	IPSec	(123) 456-7890	(123) 456-7890
7.	user-ipsecserviceop	Joe	IPSecServiceOp	(123) 456-7890	(123) 456-7890
8.	user-l2vpn	Joe	L2VPN	(123) 456-7890	(123) 456-7890
9.	user-l2vpnserviceop	Joe	L2VPNServiceOp	(123) 456-7890	(123) 456-7890
10.	user-mpls	Joe	MPLS	(123) 456-7890	(123) 456-7890
11.	user-mplsserviceop	Joe	MPLSServiceOp	(123) 456-7890	(123) 456-7890
12.	user-nat	Joe	NAT	(123) 456-7890	(123) 456-7890
13.	user-nat-serviceop	Joe	NATServiceOp	(123) 456-7890	(123) 456-7890
14.	user-qos	Joe	QoS	(123) 456-7890	(123) 456-7890
15.	user-qos-serviceop	Joe	QOSServiceOp	(123) 456-7890	(123) 456-7890
16.	user-sysadmin	Joe	SysAdmin	(123) 456-7890	(123) 456-7890
17.	user-te	Joe	TE	(123) 456-7890	(123) 456-7890
18.	user-teserviceop	Joe	TEServiceOp	(123) 456-7890	(123) 456-7890
19.	user-useradmin	Joe	UserAdmin	(123) 456-7890	(123) 456-7890
20.	user-vpls	Joe	VPLS	(123) 456-7890	(123) 456-7890
21.	user-vplsserviceop	Joe	VPLSServiceOp	(123) 456-7890	(123) 456-7890

Rows per page: All Go to page: 1 of 1 Go

Details Create Copy Edit Delete

Step 2 In Figure 8-3, you can filter the list of users (corresponding to the column headings) in which to search, using the drop-down menu for **Show users with**:

- **User ID** user ID used for logging into ISC
- **First Name** user's first name
- **Last Name** user's last name
- **Work Phone** user's work phone number
- **Mobile Phone** user's cell phone or mobile phone number.

Enter the search criteria, using * if you want, and click **Find**.



Note

The search tool is case-sensitive.

- Step 3** At the bottom of the window, you can change the number of rows shown on this window in **Rows per page**.
- Step 4** The explanations of the remainder of the buttons are given as follows:
- [Details, page 8-4](#) View a User Detail Report
 - [Create, page 8-4](#) Create a new user
 - [Copy, page 8-7](#) Make a copy of an existing user and make changes to create a new user
 - [Edit, page 8-7](#) Edit selected user
 - [Delete, page 8-7](#) Delete selected user(s).
-

Details

The **Details** button, located at the bottom of [Figure 8-3](#), has the following columns of information: **User ID**; **User Group** that a user belongs to; **Role** that a user occupies; **Resource Privilege** permissions that a user has for each role occupied; **Object Group** that a user role is associated with; **Customer View** that a user's role is limited to; **Provider View** that a user's role is limited to. Navigate **Administration > Security > Users** and click the **Details** button.

Create

The **Create** button, located at the bottom of [Figure 8-3](#), allows a user with the required privileges to create a new user. Follow these steps:

-
- Step 1** Navigate **Administration > Security > Users**.
- Step 2** Click the **Create** button and the window shown in [Figure 8-4](#), “[Create/Edit Users Window](#),” appears.

Figure 8-4 Create/Edit Users Window

Security	
User ID :	
Password :	
Verify Password :	
Permissions for Others:	☒ View ☒ Edit ☐ Delete
User Groups:	Edit
Assigned Roles:	Edit
Personal Information	
Full Name :	
Work Phone:	
Mobile Phone:	
Pager:	
Email:	
Location:	
Supervisor Information:	
User Preferences	
Language:	English
Rows per page:	10
Logging Level:	Warning
Initial Screen:	Home
Save Cancel	

116.080

Step 3 Enter information in the **Security** section, as follows:

- **User ID** (required) Enter a User ID for this new user.
- **Password** (required) New password to replace any existing password
- **Verify Password** (required) Confirm by re-entering the selected password
- **Permission for Others** Select each of the associated check boxes for the permission that the user (to be created) wants to give to other users. The user who creates the object is the owner of the objects. The creator can allow or disallow other users to **View**, **Edit**, and/or **Delete** the objects owned by the creator by defining permissions. This is the last line of defense. For UserA to delete an object X that UserB created, UserA must first have Delete permission for object X, then UserB's settings for permissions for others will be checked, to finally decide whether UserA can delete object X. Permission for others can be enabled or disabled by setting the property: repository.rbac.checkCreatorPermissionEnabled. After you make a change, you must restart the WatchDog by entering **stopwd** followed by **startwd**. For more WatchDog details, see [Chapter 2, "WatchDog Commands"](#).

- **User Groups** Click **Edit** and you receive a list of the groups. Add this user to a user group(s). The user inherits all the roles assigned to the group(s). You can filter this list. From the selected groups, select the check box next to each group to which you want to add this user or select the check box in the header row to add the user to all the groups shown. Then click **OK**. You can repeat this procedure if you want to change your selection.

A user's group membership can also be changed in the group editor (see the [“Edit” section on page 10](#)).

- **Assigned Roles** Click **Edit** and you receive a list of the roles. You can filter this list. From the selected roles, select the check box next to each role to which you want to assign this user or select the check box in the header row to assign all the shown roles to the user. Then click **OK**. You can repeat this procedure if you want to change your selection.

The user inherits all the privileges from the groups in which it participates and from the roles assigned to it. That is, the permissions received by the user is an OR result of the permissions in each role.

Step 4 Enter information in the **Personal Information** section, as follows:

- **Full Name** (required) Click the drop-down menu and select a title; enter the first name; and then enter the last name.
- **Work Phone** (optional) Enter the work phone number.
- **Mobile Phone** (optional) Enter the user's cell phone or mobile phone number.
- **Pager** (optional) Enter the user's pager number.
- **E-mail** (optional) Enter the user's e-mail address.
- **Location** (optional) Enter the user's location.
- **Supervisor Information** (optional) Enter information about the supervisor.

Step 5 Enter information in the User Preferences section, as follows:

- **Language** (optional) Click the drop-down menu to select a language (at this time only English is supported).
- **Rows per page** (optional) This defines the number of rows per page for object listing. The default is **10**. The choices are: **5, 10, 20, 30, 40, 50**, and **All**.
- **Logging Level** (optional) The default is **Warning**. The choices are: **Off, Severe, Warning, Config, Info, Fine, Finer, Finest**, and **All** (see all levels of logs). This defines the logging level for viewing logging events. The list progresses from the least number of messages to the most number of messages.
- **Initial Screen** (optional) The default is **Home**. The choices are: **Home, Service Inventory, Service Design, Monitoring, Administration, Site Index**. This is a way to specify the first screen you will see after logging in.

Step 6 Click **Save**. [Figure 8-3](#) reappears with the new user listed.

Copy

The **Copy** button, located at the bottom of [Figure 8-3](#), provides a convenient way to create a new User by copying the information for an existing User including User Groups, Assigned Roles, and User Preferences. Follow these steps:

-
- Step 1** Navigate **Administration > Security > Users**.
 - Step 2** Select one check box for the existing User you want to copy and edit to create a new User.
 - Step 3** Click the **Copy** button and the window shown in [Figure 8-4](#), “**Create/Edit Users Window**,” appears.
 - Step 4** Required entries are a **User ID**, **Password**, **Verify Password**, and **Full Name**.
 - Step 5** Make all the other changes you want by following the instructions in the “**Create**” section on [page 8-4](#).
 - Step 6** Click **Save** and you will return to [Figure 8-3](#). The newly created **User** is added to the list and a Status Succeeded message appears in green.
-

Edit

The **Edit** button, located at the bottom of [Figure 8-3](#), allows a user with the required privileges to edit user-specific information. Follow these steps:

-
- Step 1** Navigate **Administration > Security > Users**.
 - Step 2** Select the check box for the row of the user you want to edit.
 - Step 3** Click the **Edit** button and a window as shown in [Figure 8-4](#), “**Create/Edit Users Window**,” appears.

**Note**

To change your password without the SysAdmin or UserAdmin privileges, click the **Account** tab on the top of the Home page. This allows the user to edit the user profile, including changing the password.

-
- Step 4** Enter the desired information for the user profile, as specified in [Step 3](#) of the “**Create**” section on [page 8-4](#).
 - Step 5** Click **Save**. [Figure 8-3](#) reappears with the edited user listed.
-

Delete

The **Delete** button, located at the bottom of [Figure 8-3](#), allows a user with the required privileges to delete user-specific information. Follow these steps:

-
- Step 1** Navigate **Administration > Security > Users**.
 - Step 2** Select the check box(es) for the row(s) of the user(s) you want to delete or select the check box in the header row to select all the users for deletion.
 - Step 3** Click the **Delete** button and a window as shown in [Figure 8-5](#), “**Users Confirm Delete**” appears.

Figure 8-5 Users Confirm Delete

#	User ID	Name
1. new1		newfirstname1 newname1

Rows per page: 10

Delete Cancel

- Step 4** Click **Delete** to continue with the process of deleting information for the specified user(s). Otherwise click **Cancel**.
- Step 5** [Figure 8-3, “Users Window,”](#) reappears. If this was successful, the newly updated information appears and a **Status** box appears in the lower left corner of the window with a green check mark for **Succeeded**.

User Groups

A user group is a logical grouping of users with common privileges. The **User Groups** feature is used to create, edit, or delete user groups.

To access the User Groups window, navigate **Administration > Security > User Groups** and follow these steps:

- Step 1** The window in [Figure 8-6, “User Groups Window”](#) appears.

Figure 8-6 User Groups Window

Selection

- .. Users
- .. **User Groups**
- .. User Roles
- .. Object Groups

IP Solution Center

Service Inventory Service Design Monitoring Administration

Security Control Center Active Users User Access Log

You Are Here: Administration > Security > User Groups

Customer: None

User Groups

Show groups with Name Matching * Find

Showing 0 of 0 records

Name Description

Rows per page: All

Go to page: 1 of 1 Go

Create Edit Delete

Step 2 In [Figure 8-6](#), you can filter the list of user groups (corresponding to the column headings) in which to search, using the drop-down menu for **Show groups with:**

- **Name**
- **Description**

Enter the search criteria, using * if you want, and click **Find**.



Note

The search tool is case-sensitive.

Step 3 At the bottom of the window, you can change the number of rows shown on this window in **Rows per page**.

Step 4 The explanations of the remainder of the buttons is given as follows:

- [Create, page 8-9](#) Create a new user group
- [Edit, page 8-10](#) Edit selected user group
- [Delete, page 8-10](#) Delete selected user group(s)

Create

The **Create** button, located at the bottom of [Figure 8-6](#), allows a user with the required privileges to create a user group. Follow these steps:

Step 1 Navigate **Administration > Security > User Groups**.

Step 2 Click the **Create** button and the window shown in [Figure 8-7](#), “Create/Edit User Groups Window,” appears.

Figure 8-7 Create/Edit User Groups Window

Step 3 Enter information for the user group profile, as follows:

- **Name** (required) Enter a name for the new user group.
- **Description** (optional) Enter a description of this new user group.

- **Roles** This allows you to assign roles to this user group. Click **Edit** and you receive a list of the roles. You can filter this list. From the selected roles, select the check box next to each role you want to attach to this user group or select the check box in the header row to assign all the shown roles to this user group. Then click **OK**. You can repeat this procedure if you want to change your selection.
- **Users** This allows you to add users to this user group. Click **Edit** and you receive a list of the users. You can filter this list. From the selected users, select the check box next to each user you want to attach to this user group or select the check box in the header row to assign all the shown users to this user group. Then click **OK**. You can repeat this procedure if you want to change your selection.

Step 4 Click **Save**. [Figure 8-6](#) reappears with the new user group listed.

Edit

The **Edit** button, located at the bottom of [Figure 8-6](#), allows a user with the required privileges to edit user group-specific information. Follow these steps:

-
- Step 1** Navigate **Administration > Security > User Groups**.
- Step 2** Select the check box for the row of the user group you want to edit.
- Step 3** Click the **Edit** button and a window as shown in [Figure 8-7](#), “[Create/Edit User Groups Window](#),” appears.
- Step 4** Enter the desired information for the user group profile, as specified in [Step 3](#) of the “[Create](#)” section on [page 8-9](#).
- Step 5** Click **Save**. [Figure 8-6](#) reappears with the edited user group list.
-

Delete

The **Delete** button, located at the bottom of [Figure 8-6](#), allows a user with the required privileges to delete user group-specific information. Follow these steps:

-
- Step 1** Navigate **Administration > Security > User Groups**.
- Step 2** Select the check box(es) for the row(s) of the user group(s) you want to delete or select the check box in the header row to select all the user groups for deletion.
- Step 3** Click the **Delete** button and a window as shown in [Figure 8-8](#), “[User Groups Confirm Delete](#),” appears.

Figure 8-8 User Groups Confirm Delete

Confirm Delete		
Showing 1-1 of 1 records		
#	Name	Description
1.	newgroup1	description for newgroup1

Rows per page: 10

Delete Cancel

937 48

- Step 4** Click **Delete** to continue the process of deleting information for the specified user group(s). Otherwise click **Cancel**.
- Step 5** [Figure 8-6, “User Groups Window,”](#) reappears. If this was successful, the newly updated information appears and a **Status** box appears in the lower left corner of the window with a green check mark for **Succeeded**.

User Roles

A user role is a predefined or a user-specified role defining a set of permissions. The **User Roles** feature is used to create, edit, or delete user roles.

To better understand the way roles are managed, certain specific characteristics of roles are defined as follows:

- **Parent Role** All permission of the parent roles are inherited by the role that is being created or edited (child role). A child role always has the same or more privileges than its parent role.
- **Customer** If a role is associated with a customer, a user of this role does not have access to the objects associated with other customers. Object types that are constrained by customer view are: Persistent Task, Customer Site, VPN, CPE, SR, Policy, Service Order, and resource pools that are associated with a Customer, Customer Site, or VPN.
- **Provider** If a role is associated with a provider, a user of this role does not have access to the objects associated with other providers. Object types that are constrained by provider view are: Persistent Task, Access Domain, Region, PE, Policy, and some resource pools that are associated with a provider, Access Domain, Region, or PE.

Customer view and provider view within a role have no affect on those objects that do not belong to either a customer or a provider. Those object types are: task, probe, workflow, device, ISC host, and template.

Permission operation types in a Role editor, namely View, Create, Edit, and Delete mean View, Create, Modify, and Delete on database object. For example, SR modification (or subsumption) is viewed as Role Based Access Control (RBAC) Creation. SR purge is viewed as RBAC Delete.

A Role can be enabled to be associated with Object Group(s). When Object Group association is enabled, a Role can no longer be associated with a Customer or a Provider, and it cannot have a Parent Role. Resources are limited to PE, CPE, and Named Physical Circuit only. PE and CPE permission implies Device Permission.

**Note**

A global policy, the one that is not associated with any customer or provider, is accessible by both customer-view roles and provider-view roles.

Separate provider-view from customer-view roles when defining a role. When a role is associated with a provider, choose only the resources for which an access scope can be constrained by a provider view. Do the same for a customer-view role.

To access the User Roles window, navigate **Administration > Security > User Roles** and follow these steps:

Step 1 The window in [Figure 8-9](#), “[User Roles Window](#),” appears.

Figure 8-9 User Roles Window

The screenshot shows the Cisco IP Solution Center User Roles window. The navigation pane on the left includes 'Users', 'User Groups', 'User Roles' (selected), and 'Object Groups'. The main content area is titled 'User Roles' and contains a table of predefined roles. The table has columns for '#', 'Name', and 'Description'. There are 20 roles listed, each with a checkbox in the first column. The roles are: CollectionRole, DeviceImportRole, FirewallRole, FirewallServiceOpRole, IPsecRole, IPsecServiceOpRole, L2VPNRole, L2VPNServiceOpRole, MPLSRole, MPLSServiceOpRole, NATRole, NATServiceOpRole, QoSRole, QoSServiceOpRole, SysAdminRole, TERole, TESServiceOpRole, UserAdminRole, VPLSRole, and VPLSServiceOpRole. Each role's description states it is an 'ISC predefined role' with specific permissions. At the top of the table, there are search filters: 'Viewroles with' (Name), 'Matching' (*), and a 'Find' button. Below the table, there are pagination controls: 'Showing 1 - 20 of 20 records', 'Rows per page: All', and 'Go to page: 1 of 1' with a 'Go' button. At the bottom right, there are buttons for 'Create', 'Copy', 'Edit', and 'Delete'.

#	Name	Description
1.	CollectionRole	ISC predefined role. It has the permission to run collection on devices.
2.	DeviceImportRole	ISC predefined role. It has the permission to import devices.
3.	FirewallRole	ISC predefined role. It has the permission to manage Inventory and deploy Firewall Service Request.
4.	FirewallServiceOpRole	ISC predefined role. It has the permission to deploy Firewall Service Request.
5.	IPsecRole	ISC predefined role. It has the permission to manage Inventory and deploy IPsec Service Request.
6.	IPsecServiceOpRole	ISC predefined role. It has the permission to deploy IPsec Service Request.
7.	L2VPNRole	ISC predefined role. It has the permission to manage Inventory and deploy L2VPN Service Request.
8.	L2VPNServiceOpRole	ISC predefined role. It has the permission to deploy L2VPN Service Request.
9.	MPLSRole	ISC predefined role. It has the permission to manage Inventory and deploy MPLS Service Request.
10.	MPLSServiceOpRole	ISC predefined role. It has the permission to deploy MPLS Service Request.
11.	NATRole	ISC predefined role. It has the permission to manage Inventory and deploy NAT Service Request.
12.	NATServiceOpRole	ISC predefined role. It has the permission to deploy NAT Service Request.
13.	QoSRole	ISC predefined role. It has the permission to manage Inventory and deploy QoS Service Request.
14.	QoSServiceOpRole	ISC predefined role. It has the permission to deploy QoS Service Request.
15.	SysAdminRole	ISC predefined role. It has full permission.
16.	TERole	ISC predefined role. It has the permission to manage Inventory and deploy TE Service Request.
17.	TESServiceOpRole	ISC predefined role. It has the permission to deploy TE Admission Service Request.
18.	UserAdminRole	ISC predefined role. It has full permission to manage User, Group and Role.
19.	VPLSRole	ISC predefined role. It has the permission to manage Inventory and deploy VPLS Service Request.
20.	VPLSServiceOpRole	ISC predefined role. It has the permission to deploy VPLS Service Request.

The predefined roles shown in Figure 8-9 are provided with associated permissions that cannot be edited or deleted. They are intended to cover most of the needed use cases to facilitate a rapid assignment of roles to users and groups with minimum manual configuration. They can also be used as examples to create new roles.

Step 2 In Figure 8-9, you can filter the list of user roles (corresponding to the column headings) in which to search, using the drop-down menu for **Show roles with**:

- Name
- Description

Enter the search criteria, using * if you want, and click **Find**.

**Note**

The search tool is case-sensitive.

- Step 3** At the bottom of the window, you can change the number of rows shown on this window in **Rows per page**.
- Step 4** The explanations of the remainder of the buttons is given as follows:
- [Create, page 8-14](#) Create a new user role
 - [Copy, page 8-17](#)
 - [Edit, page 8-17](#) Edit selected user role
 - [Delete, page 8-18](#) Delete selected user role(s)

Create

The **Create** button, located at the bottom of [Figure 8-9](#), allows a user with the required privileges to create a new user role. Follow these steps:

- Step 1** Navigate **Administration > Security > User Roles**.
- Step 2** Click the **Create** button and a window comprised of [Figure 8-10](#), “Create/Edit User Roles Window (Top),” and [Figure 8-11](#), “Create/Edit User Roles Window (Bottom),” appears.

Figure 8-10 Create/Edit User Roles Window (Top)

Name *	
Enable Object Group Association:	☐
Parent Role:	Edit
Customer:	Edit
Provider:	Edit
Object Groups:	Edit
Description:	
Users:	Edit
User Groups:	Edit

118070

Figure 8-11 Create/Edit User Roles Window (Bottom)

Resource	All	Create	View	Edit	Delete
Persistent Task	☐	☐	☐	☐	☐
SAA Probe	☐	☐	☐	☐	☐
Work flow	☐	☐	☐	☐	☐
Device	☐	☐	☐	☐	☐
ISC Host	☐	☐	☐	☐	☐
Customer	☐	☐	☐	☐	☐
Provider	☐	☐	☐	☐	☐
PE	☐	☐	☐	☐	☐
CPE	☐	☐	☐	☐	☐
QoS Policy	☐	☐	☐	☐	☐
QoS Service Request	☐	☐	☐	☐	☐
MPLS Policy	☐	☐	☐	☐	☐
MPLS Service Request	☐	☐	☐	☐	☐
L2VPN Policy	☐	☐	☐	☐	☐
L2VPN Service Request	☐	☐	☐	☐	☐
Firewall Policy	☐	☐	☐	☐	☐
Firewall Service Request	☐	☐	☐	☐	☐
NAT Service Request	☐	☐	☐	☐	☐
IPsec Policy	☐	☐	☐	☐	☐
IPsec Service Request	☐	☐	☐	☐	☐
Deployment Flow	☐	☐	☐	☐	☐
Template	☐	☐	☐	☐	☐
TE Provider	☐	☐	☐	☐	☐
TE Router	☐	☐	☐	☐	☐
TE Tunnel Policy	☐	☐	☐	☐	☐
TE Tunnel & Resource Service Request	☐	☐	☐	☐	☐
TE Traffic Admission Service Request	☐	☐	☐	☐	☐
VPLS Policy	☐	☐	☐	☐	☐
VPLS Service Request	☐	☐	☐	☐	☐
Service Order	☐	☐	☐	☐	☐
Object Group	☐	☐	☐	☐	☐
Named Physical Circuit	☐	☐	☐	☐	☐

Note: * - Required Field

116071

Step 3 Enter the following information in Figure 8-10:

- **Name** (required) Enter the name of this new user role.
- **Enable Object Group** The default is that this check box is deselected. In this case, **Parent Role**, **Customer**, and **Provider** are enabled and **Object Groups** is not enabled. Figure 8-11 is complete as shown. If you select this check box, **Parent Role**, **Customer**, and **Provider** are not enabled and **Object Groups** is enabled. Figure 8-11 is reduced to just **PE**, **CPE**, and **Named Physical Circuit**.

- **Parent Role** (optional) Click **Edit** and a list of the existing roles appears, similar to [Figure 8-9](#), from which you can click the radio button for the parent role you choose. Then click **Select**. You can repeat this procedure if you want to change your selection. Click the **Clear** button if you want no parent selection.
- **Customer** (optional) Click **Edit** and a list of the existing customers appears. You can filter this list. From the selected customers, click the radio button for the customer you want to select to own this role. Then click **Select**. You can repeat this procedure if you want to change your selection. Click the **Clear** button if you want no customer selection.

**Note**

A customer can only be associated with a logical device, such as **CPE** and **PE**. This is not possible with a physical device, such as **device**.

- **Provider** (optional) Click **Edit** and a list of the existing providers appears. You can filter this list. From the selected providers, click the radio button for the provider you want to select to own this role. Then click **Select**. You can repeat this procedure if you want to change your selection. Click the **Clear** button if you want no provider selection.
- **Object Groups** (optional) Click **Edit** and a list of the existing object groups appears. You can filter this list. From the selected object groups, click the radio button for the object group(s) you want to select to associate with this User Role. Then click **OK**. You can repeat this procedure if you want to change your selection. Deselect the **Enable Object Group Association** button if you want no object group selection.
- **Description** (optional) Enter the descriptive information about permissions in this field, as shown in the Description column of [Figure 8-9](#).
- **Users** (optional) Click **Edit** and a list of the existing users appears. You can filter this list. From the selected users, select the check box(es) for the user(s) you want assigned to this role or select the check box in the header row to assign all the users to this role. Then click **OK**. You can repeat this procedure if you want to change your selection.

**Note**

A user who is associated with a specific role cannot see objects associated with other customers or with other providers.

- **User Groups** (optional) Click **Edit** and a list of the existing user groups appears. You can filter this list. From the selected user groups, select the check box(es) for the user group(s) you want assigned to this role or select the check box in the header row to assign all the user groups to this role. Then click **OK**. You can repeat this procedure if you want to change your selection.

Step 4

In [Figure 8-11](#), click any combination of the following permissions: **Create**; **View**; **Modify**; **Delete**. If you want all the permissions, click **All**.

**Note**

ISC Host refers to **Administration > Control Center**. Here, you can view host details, perform configuration tasks, start and stop servers, activate a watchdog, and so on.

**Note**

SAA Probe is intended for management of SLA under **Monitoring > SLA**. Any user who wants to generate SLA reports *must* have **View** permission on **ISC Host** in addition to **View** permission on **SAA Probe**.

**Note**

The **Workflow** object is currently not used.

Step 5 Click **Save**. [Figure 8-9](#) reappears with the new user role listed.

Copy

The **Copy** button, located at the bottom of [Figure 8-9](#), provides a convenient way to copy the information from an existing User Role and edit it to create a new User Role. Follow these steps:

**Note**

All fields in the existing role are copied to the new role, even including Users and User Groups. You should edit the new role *carefully* to reflect your intention.

- Step 1** Navigate **Administration > Security > User Roles**.
- Step 2** Select one check box for the existing User Role you want to copy and edit to create a new User Role.
- Step 3** Click the **Copy** button and the window comprised of [Figure 8-10](#), “**Create/Edit User Roles Window (Top)**,” and [Figure 8-11](#), “**Create/Edit User Roles Window (Bottom)**” appears.
- Step 4** Required entries are a **Name**. A default name is given, **Copy of** and the name of the original User Role. You cannot duplicate a **Name**.
- Step 5** Make all the other changes you want by following the instructions in the “**Create**” [section on page 8-14](#).
- Step 6** Click **Save** and you will return to [Figure 8-9](#). The newly created **User** is added to the list and a Status Succeeded message appears in green.

Edit

The **Edit** button, located at the bottom of [Figure 8-9](#), allows a user with the required privileges to edit user role-specific information. Follow these steps:

- Step 1** Navigate **Administration > Security > User Roles**.
- Step 2** Select the check box for the row of the user role you want to edit.
- Step 3** Click the **Edit** button and a window appears combining [Figure 8-10](#) and [Figure 8-11](#) for this user role.
- Step 4** Enter the desired information for the user role profile, as specified in [Step 3](#) and [Step 4](#) of the “**Create**” [section on page 8-14](#).
- Step 5** Click **Save**. [Figure 8-9](#) reappears with the edited user roles listed.

Delete

The **Delete** button, located at the bottom of [Figure 8-9](#), allows a user with the required privileges to delete user role-specific information. Follow these steps:

-
- Step 1** Navigate **Administration > Security > User Roles**.
 - Step 2** Select the check box(es) for the row(s) of the user role(s) you want to delete or select the check box in the header row to select all the users for deletion.
 - Step 3** Click the **Delete** button and a window as shown in [Figure 8-12](#), “**User Roles Confirm Delete**,” appears.

Figure 8-12 User Roles Confirm Delete

Confirm Delete		
Showing 1-1 of 1 records		
#	Name	Description
1.	newrole1	

Rows per page: 20

Delete Cancel

- Step 4** Click **Delete** to continue with the process of deleting information for the specified user role(s). Otherwise click **Cancel**.
 - Step 5** [Figure 8-9](#), “**User Roles Window**,” reappears. If this was successful, the newly updated information appears and a Status box appears in the lower left corner of the window with a green check mark for **Succeeded**.
-

Object Groups

An Object Group is a named aggregate entity comprised of a set of objects. The object types can be PE, CE, Named Physical Circuit (NPC), and interfaces of PEs or CEs. An Object Group provides instance level of access granularity for users.

An Object Group can be associated with different roles. A role can be associated with multiple Object Groups. A role can be associated with either Object Group(s), or a Customer, a Provider, but not both. When a role is associated with Object Group(s), you can only define permissions for PE, CE, and NPC. Permissions on interfaces implies PEs or CEs, that is, PE Create or CE Create implies Interface Create. PE or CE Edit implies Interface Create, Edit, or Delete. CE or PE Delete implies Interface Delete.

When instance level of access is desired for PE, CE, NPC, or interface of PEs and CEs, you can usually define a role associated with Object Group(s) that contains a collection of PEs and CEs that you are limited to operate. Then define other roles to include permissions on other types of objects. See the “[User Roles Design Example](#)” section on page 8-22.

If an Object Group contains PEs (or CEs) only, with no explicit interface as a group member, you can access all interfaces of grouped PEs or CEs. If an Object Group contains any explicit interface as group members, every single interface that you want to access you must manually choose to include as group members.

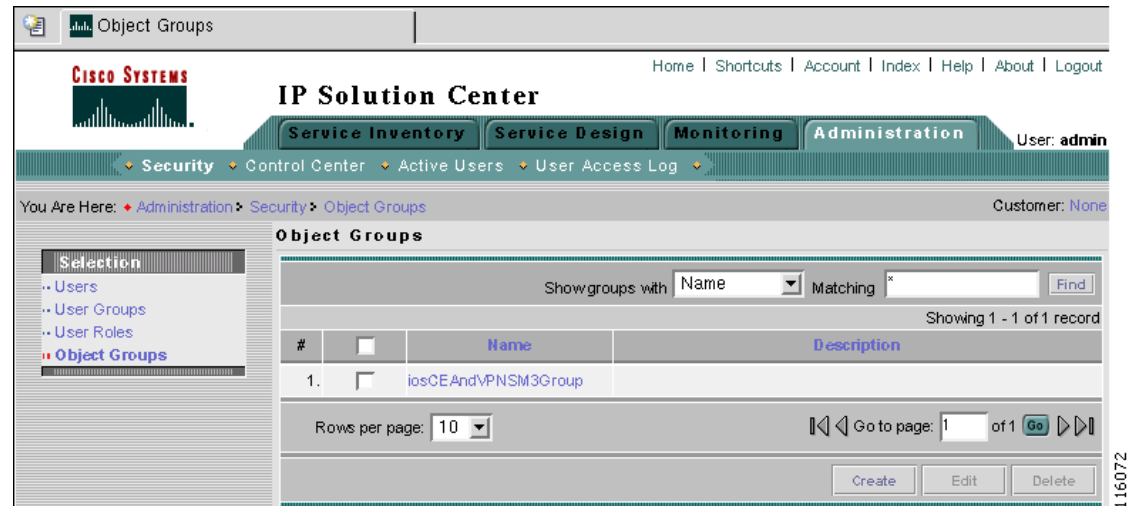
**Note**

Permissions are the union of all roles that you occupy. If your intention is to limit access to a scope of devices or NPCs, define a role to be associated with Object Group(s), Device, CE, PE, and NPC.

To access the Object Groups window, navigate **Administration > Security > Object Groups** and follow these steps:

Step 1 The window in [Figure 8-13](#), “Object Groups Window,” appears.

Figure 8-13 Object Groups Window



Step 2 In [Figure 8-13](#), you can filter the list of object groups (corresponding to the column headings) in which to search, using the drop-down menu for **Show groups with**:

- **Name**
- **Description**

Enter the search criteria in **Matching**, using * if you want, and click **Find**.

**Note**

The search tool is case-sensitive.

Step 3 At the bottom of the window, you can change the number of rows shown on this window in **Rows per page**.

Step 4 The explanations of the remainder of the buttons is given as follows:

- [Create, page 8-14](#) Create a new object group
- [Edit, page 8-17](#) Edit a selected object group
- [Delete, page 8-18](#) Delete selected object group(s)

Create

The **Create** button, located at the bottom of [Figure 8-13](#), allows a user with the required privileges to create a new object group. Follow these steps:

- Step 1** Navigate **Administration > Security > Object Groups**.
- Step 2** Click the **Create** button and the window [Figure 8-14](#), “Create/Edit Object Group Window,” appears.

Figure 8-14 Create/Edit Object Group Window

The screenshot shows a web-based configuration window titled "Create/Edit Object Group Window". It contains the following sections:

- Name:** A text input field with a small 'x' icon for clearing the field.
- Description:** A large text area for entering a description.
- PE Group Members:** A table with columns: #, Name, Interface Members, and an Edit button.

#	Name	Interface Members
1.	ios-pe102	
2.	ios-pe101	

 Below the table are pagination controls: "Rows per page: 10", "Go to page: 1 of 1", and a "Go" button.
- CE Group Members:** A table with columns: #, Name, Interface Members, and an Edit button.

#	Name	Interface Members
1.	sec4-cat6k_VPNM_3	FastEthernet2/1, FastEthernet2/10

 Below the table are pagination controls: "Rows per page: 10", "Go to page: 1 of 1", and a "Go" button.
- NPC Group Members:** A table with columns: #, Name, and an Edit button.

#	Name

 Below the table are pagination controls: "Rows per page: 10", "Go to page: 1 of 1", and a "Go" button.

At the bottom right of the window are "Save" and "Cancel" buttons. A small vertical text "116073" is visible on the right edge of the window.

- Step 3** Enter the following information in [Figure 8-14](#):
- **Name** (required) Enter the name of this new object group.
 - **Description** (optional) Enter a description of this new object group.
 - **PE Group Members** (optional) Click **Edit** and a list of the existing PEs appears. You can filter this list. From the selected PEs, click the radio button for the PE(s) you want to include in this group. Then click **OK**. You can repeat this procedure if you want to change your selection(s). The **Interface Members** column will be empty. All existing interfaces for each of the PE Groups in the **Name** column will default to be members of the group unless you select only a subset. To limit the interfaces and select a subset of interfaces, click a PE Group in the **Name** column. You receive a list of all the interfaces for that PE from which you can individually select only the interfaces you want to associate with that PE Group. Then click **OK**. You return to [Figure 8-14](#), “Create/Edit Object Group Window,” and the **Name** and selected **Interface Members** for each PE Group Member appear. If no entries exist in the **Interface Members** column for both **PE Group Members** and **CE Group Members**, the default is all existing interfaces for both (if any exist).

- **CE Group Members** (optional) Click **Edit** and a list of the existing CEs appears. You can filter this list. From the selected CEs, click the radio button for the CE(s) you want to include in this group. Then click **OK**. You can repeat this procedure if you want to change your selection(s). The **Interface Members** column will be empty. All existing interfaces for each of the CE Groups in the **Name** column will default to be members of the group unless you select only a subset. To limit the interfaces and select a subset of interfaces, click a CE Group in the **Name** column. You receive a list of all the interfaces for that CE from which you can individually select only the interfaces you want to associate with that CE Group. Then click **OK**. You return to [Figure 8-14, “Create/Edit Object Group Window,”](#) and the **Name**, and selected **Interface Members** for each CE Group Member appear. If no entries exist in the **Interface Members** column for both **CE Group Members** and **PE Group Members**, the default is all existing interfaces for both (if any exist).
- **NPC Group Members** (optional) Click **Edit** and a list of the existing Named Physical Circuits (NPCs) appears. You can filter this list. From the selected NPCs, click the radio button for the NPC(s) you want to select to own this role. Then click **OK**. You can repeat this procedure if you want to change your selection(s). You will return to [Figure 8-14, “Create/Edit Object Group Window,”](#) and the **Name** for each NPC Group Member appears.

Step 4 Click **Save**. [Figure 8-14](#) reappears with the new object group listed.

Edit

The **Edit** button, located at the bottom of [Figure 8-14](#), allows a user with the required privileges to edit object group-specific information. Follow these steps:

-
- Step 1** Navigate **Administration > Security > Object Groups**.
- Step 2** Select the check box for the row of the object group you want to edit.
- Step 3** Click the **Edit** button and a window appears as shown in [Figure 8-14](#), with the object group chosen specified in the **Name** field.
- Step 4** Enter the desired information for the object group, as specified in [Step 3](#) of the “Create” section on [page 8-20](#).
- Step 5** Click **Save**. [Figure 8-14](#) reappears with the edited object groups listed.
-

Delete

The **Delete** button, located at the bottom of [Figure 8-14](#), allows a user with the required privileges to delete object group-specific information. Follow these steps:

-
- Step 1** Navigate **Administration > Security > Object Groups**.
- Step 2** Select the check box(es) for the row(s) of the object group(s) you want to delete or select the check box in the header row to select all the object groups for deletion.
- Step 3** Click the **Delete** button and a window as shown in [Figure 8-15, “Delete Object Groups Confirm Delete,”](#) appears.

Figure 8-15 Delete Object Groups Confirm Delete

#	Name	Description
1.	objgp2	
2.	objgp3	

Rows per page: All Go to page: 1 of 1 Go

Delete Cancel

- Step 4** Click **Delete** to continue with the process of deleting information for the specified object group(s). Otherwise click **Cancel**.
- Step 5** [Figure 8-14, “Create/Edit Object Group Window,”](#) reappears. If this was successful, the newly updated information appears and a Status box appears in the lower left corner of the window with a green check mark for **Succeeded**.

User Roles Design Example

This section gives an example situation, an illustration that shows this setup, and steps on how to setup this design:

- [Example, page 8-22](#)
- [Illustration of Setup, page 8-23](#)
- [Steps to Set Up Example, page 8-24](#)

Example

This section explains an example data center for which the following sections, [“Illustration of Setup” section on page 8-23](#) and [“Steps to Set Up Example” section on page 8-24](#) give an illustration setup and steps, respectively.

Finance Customer XYZ built an MPLS network to connect its branch offices to its data center. Subsidiaries of XYZ are running different parts of the MPLS network. Each subsidiary uses a different BGP AS domain, which results in different Provider Administrative Domains (PADs) inside ISC.

Each subsidiary acts as a Provider and owns therefore its own Devices, like PE and CE devices and should also own logical attributes inside ISC, like Regions, Sites, Customers, and VPNs. Therefore, the view of the devices for each subsidiary must be separated into PAD views. Thus, Provider A cannot manipulate or view the configuration files for devices of Provider B. Devices are not shared between PADs.

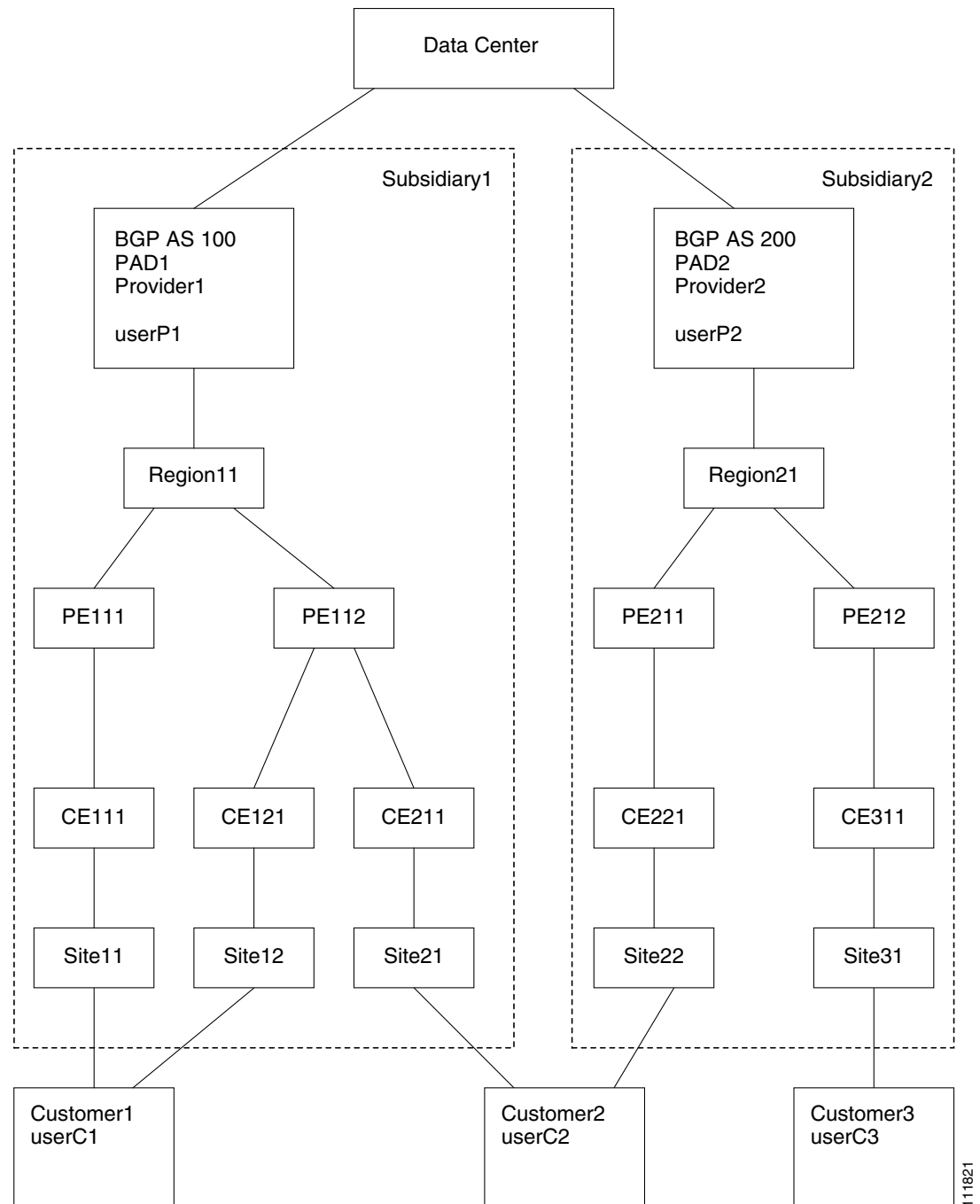
Inside a PAD, there are Customers with sites and VPNs with only local significance. Also, the IP addressing should be defined per PAD.

But there are also Customers that have sites in different PADs. This means that there is a need for Inter-AS VPNs. The Provider who owns the Customer should also have the right to share this Customer with other Providers. In this case, the VPNs and CERCs should be shared between the providers.

Illustration of Setup

Figure 8-16, “Contents in Example,” shows the setup described in the “Example” section on page 8-22.

Figure 8-16 Contents in Example



Steps to Set Up Example

This section explains the steps to create the example explained in the [“Example” section on page 8-22](#) and shown in the [“Illustration of Setup” section on page 8-23](#).

-
- Step 1** Create the following Object Groups (see the [“Create” section on page 8-20](#), which is for the section [Object Groups](#)):
- P1PEGroup that has members PE111 and PE112
 - P2PEGroup that has members PE211 and PE212
 - C1CEGroup that has members CE111 and CE121
 - C2CEGroup that has members CE211 and CE221
 - C3CEGroup that has the member CE311
 - C2DeviceGroup that has members PE112, CE211, PE211, and CE221
 - C3DeviceGroup that has members PE212 and CE311.
- Step 2** Create the following User Roles that are associated with one or more groups created in [Step 1](#) (see the [“Create” section on page 8-14](#), which is for the section [User Roles](#)).
- P1DeviceGroupRole, associated with groups P1PEGroup, C1CEGroup, and C2CEGroup, and have the Modify and Delete permissions on for PE and Cpe.
 - P2DeviceGroupRole, associated with groups P2PEGroup, C2CEGroup, and C3CEGroup, and have the Modify and Delete permissions on for PE and Cpe.
 - C1DeviceGroupRole, associated with groups P1PEGroup, C1CEGroup, and have the Modify permission on for PE and the Modify and Delete permissions on for Cpe.
 - C2DeviceGroupRole, associated with group C2DeviceGroup, and have the Modify permission on for PE and the Modify and Delete permissions on for Cpe.
 - C3DeviceGroupRole, associated with group C3DeviceGroup, and have the Modify permission on for PE and the Modify and Delete permissions on for Cpe.
- Step 3** Create the following User Roles that have Customer View or Provider View, as explained in the [“User Roles” section on page 8-11](#).
- P1MplsRole, associated with Provider P1, and have permissions on Provider, Task, ISC Host, Mpls SR, Mpls Policy, NPC, and Probe. (Add Service, Template, and ServiceOrder if needed.)
 - P2MplsRole, associated with Provider P2, and have permissions on Provider, Task, ISC Host, Mpls SR, Mpls Policy, NPC, and Probe. (Add Service, Template, and ServiceOrder if needed.)
 - C1MplsRole, associated with Customer C1, and have permissions on Customer, Task, ISC Host, Mpls SR, Mpls Policy, NPC, and Probe. (Add Service, Template, and ServiceOrder if needed.)
 - C2MplsRole, associated with Customer C2, and have permissions on Customer, Task, ISC Host, Mpls SR, Mpls Policy, NPC, and Probe. (Add Service, Template, and ServiceOrder if needed.)
 - C3MplsRole, associated with Customer C3, and have permissions on Customer, Task, ISC Host, Mpls SR, Mpls Policy, NPC, and Probe. (Add Service, Template, and ServiceOrder if needed.)
- Step 4** Assign the User Roles defined in [Step 2](#) and [Step 3](#) to Users, as explained in the [“Users” section on page 8-2](#).
- User P1 has User Roles: P1DeviceGroupRole, P1MplsRole, C1MplsRole, and C2MplsRole.
 - User P2 has User Roles: P2DeviceGroupRole, P2MplsRole, C2MplsRole, and C3MplsRole.
 - User C1 has User Roles: C1DeviceGroupRole and C1MplsRole.

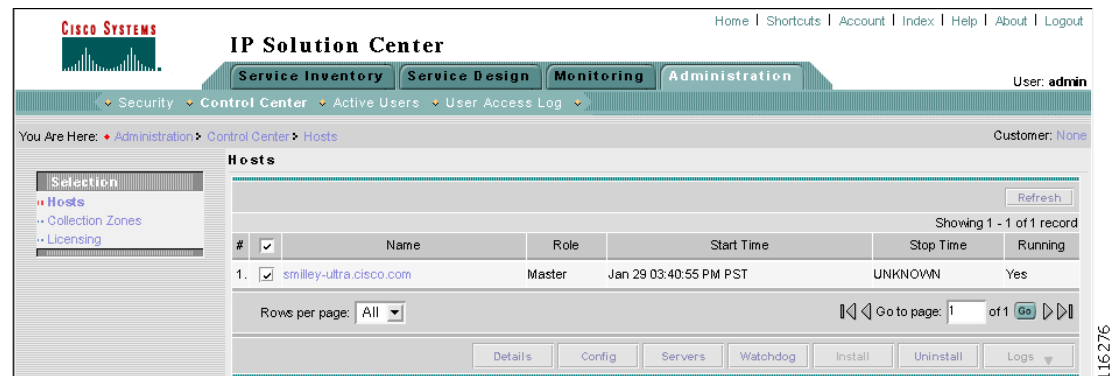
- User C2 has User Roles: C2DeviceGroupRole and C2MplsRole.
- User C3 has User Roles: C3DeviceGroupRole and C3MplsRole.

Control Center

This section explains how to view and change the properties in the Dynamic Component Properties Library (DCPL); how to view status information about a host, servers, the WatchDog, and logs; how to remotely install and uninstall a Processing server, Collection server, or Interface server; how to define collection zones; and how to install license keys.

Navigate **Administration > Control Center** and you go to the default page of **Hosts** in the TOC, as shown in [Figure 8-17](#), “Control Center > Hosts.”

Figure 8-17 Control Center > Hosts



From **Administration > Control Center**, you have the following three choices in the TOC:

- [Hosts, page 8-25](#) **Hosts** allows you to manage the various servers.
- [Collection Zones, page 8-32](#) **Collection Zones** are the means of associating collection servers with network devices.
- [Licensing, page 8-34](#) **Licensing** is where you install license keys, which is the only way to access services and APIs.

Hosts

Navigate **Administration > Control Center > Hosts**.

A window as shown in [Figure 8-17](#) appears.



Note

Only the **Install** and **Logs** buttons are enabled by default when there is no host selected. When one or more hosts are selected by selecting the check boxes, the Install and Logs buttons are disabled and the other buttons are enabled.

Click any of the buttons and proceed as follows:

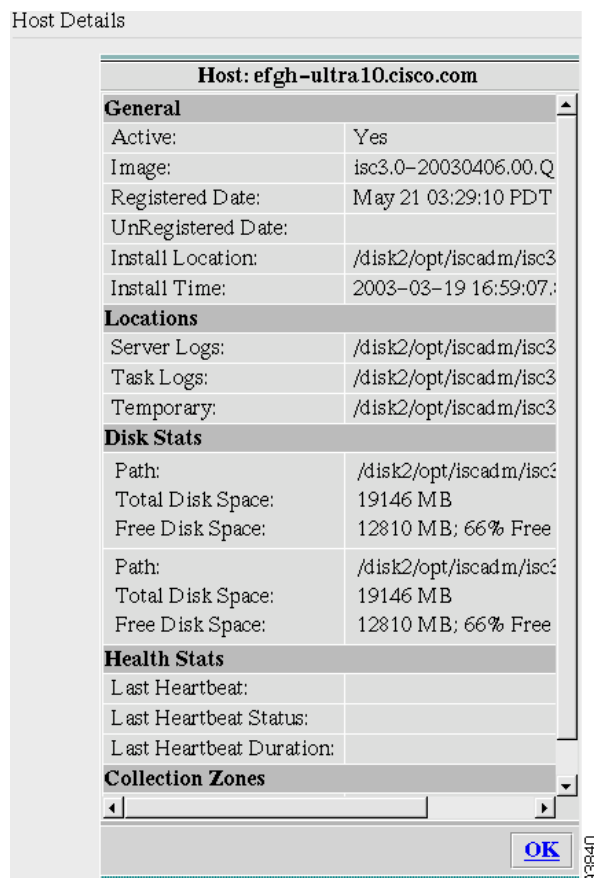
- [Details, page 8-26](#) Available only when one host system is chosen.
- [Config, page 8-27](#) Available only when one or more host systems are chosen.
- [Servers, page 8-28](#) Available only when one or more host systems are chosen.
- [Watchdog, page 8-29](#) Available only when one or more host systems are chosen.
- [Install, page 8-30](#) Available only when no host system selections are made.
- [Uninstall, page 8-31](#) Available only when one host system is chosen.
- [Logs, page 8-31](#) Available only when no host system selections are made.

Details

For details about a chosen host, do the following:

- Step 1** Choose a host by selecting the check box to the left of the host name and then click the **Details** button.
- Step 2** You receive a window as shown in [Figure 8-18, “Host Details.”](#) This shows the details about the chosen host.

Figure 8-18 Host Details



- Step 3** Click **OK** and you return to [Figure 8-17](#).

Config

To view or change the Dynamic Component Properties Library (DCPL) properties, which replaces the csm.properties file for VPNSC, do the following:

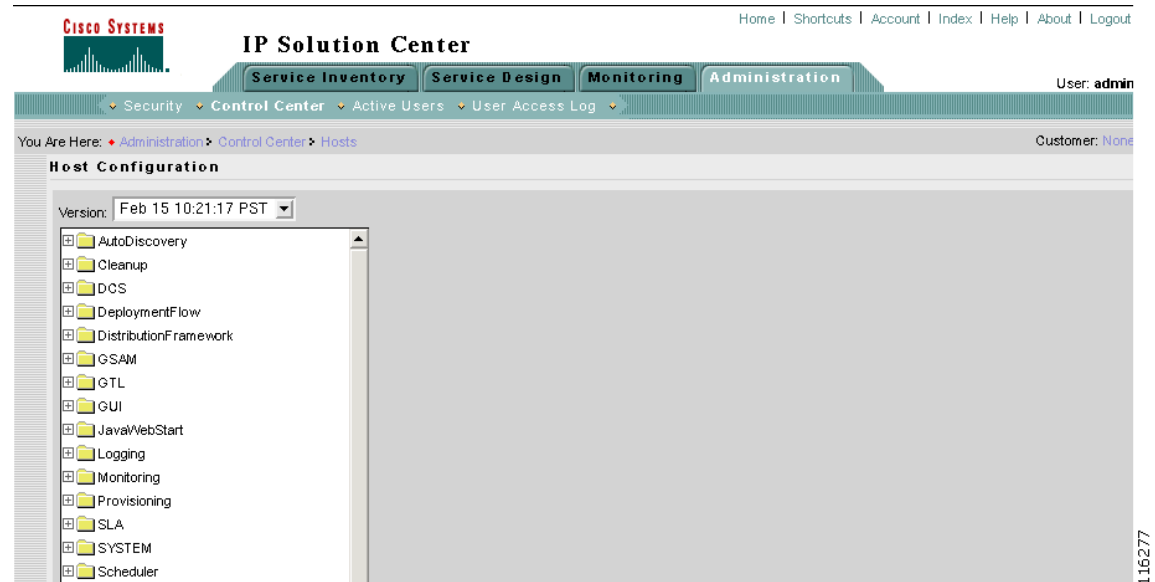


Note

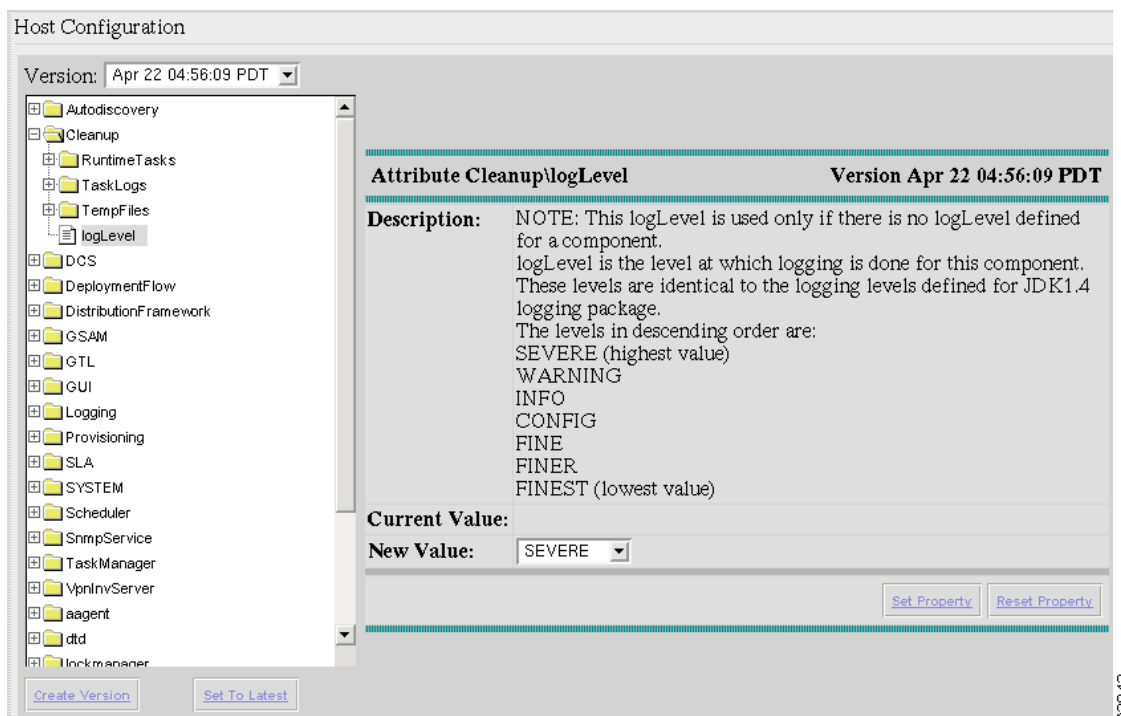
csm.properties in VPNSC cannot be migrated to DCPL settings in ISC.

- Step 1** From [Figure 8-17 on page 8-25](#), select a check box next to a host name for which you want to know the existing properties and then click the **Config** button.
- Step 2** A window as shown in [Figure 8-19, “Properties,”](#) appears. It is a list of all the folders with all the properties. See [Appendix B, “Property Settings”](#) for a list of all the properties with explanations, defaults, and ranges/rules. If you don’t know the property name, you can use a key word and do a Find on the pdf version of this appendix.

Figure 8-19 Properties



- Step 3** Click the + sign to expand each folder. The result could be more subfolders and the final level is the property name.
- Step 4** Position the mouse over the folder or property name and you see a description.
- Step 5** Click on an entry to get details and instructions on how to change the value, as shown in the example in [Figure 8-20, “Properties Detail Example.”](#)

Figure 8-20 Properties Detail Example

- Step 6** For each property that can be modified, you can modify the value and click **Set Property**. If when making your modifications, you want to return to the previous settings, click **Reset Property**.
- Step 7** After making all the changes you choose in each of the specific properties, you can click **Create Version** to create a new version of these properties. This feature gives you the option of saving multiple property sets for future use.
- Step 8** To view the values of previous versions of property sets, click the drop-down menu in **Version** and select any version you choose.
- Step 9** When you click **Set to Latest** after selecting a version in [Step 8](#), this version is dated as the most current.
- Step 10** To return, click to the navigation path you want to use next.

Servers

To view the status information about the servers, do the following:

- Step 1** From [Figure 8-17 on page 8-25](#), select a check box next to a host name for which you want to know the server statistics and then click the **Servers** button.
- Step 2** A window as shown in [Figure 8-21](#), “Servers,” appears.

Figure 8-21 Servers

#	☐	Name	State	Generation	Start Time	PID	Successful Heartbeats	Missed Heartbeats
1.	☐	cornerstonebridge	started	1	Jan 29 03:41:03 PM PST	527 22703	0	
2.	☐	worker	started	1	Jan 29 03:41:03 PM PST	530 22566	0	
3.	☐	dispatcher	started	1	Jan 29 03:41:03 PM PST	528 22661	0	
4.	☐	lockmanager	started	1	Jan 29 03:41:03 PM PST	529 22549	0	
5.	☐	nspoller	started	1	Jan 29 03:40:57 PM PST	0 22709	0	
6.	☐	scheduler	started	1	Jan 29 03:43:46 PM PST	550 22565	0	
7.	☐	httpd	started	2	Jan 29 03:45:19 PM PST	556 22716	0	
8.	☐	dbpoller	started	1	Jan 29 03:40:57 PM PST	0 22637	0	
9.	☐	cnsserver	started	1	Jan 29 03:41:03 PM PST	526 22522	0	

Showing 1 - 9 of 9 records

Rows per page: All Go to page: 1 of 1 Go

Start Stop Restart Logs OK

- Step 3** Select any one check box next to the server you want to address and you have access to **Start**, **Stop**, **Restart**, and **Logs**. When you click on a specific server name or the Logs button, you get a list of server logs. If you then click on the log name for which you want details, the log viewer appears. You can filter this information in the log viewer. After you complete the task of your choice, you return to [Figure 8-21](#).
- Step 4** You can click a different server and click the button for the process of your choice. Or you can unclick the server choice and click **OK**.
- Step 5** After you click **OK** in [Figure 8-21](#), you return to [Figure 8-17 on page 8-25](#).

Watchdog

To view the log information about WatchDog, do the following:

- Step 1** From [Figure 8-17 on page 8-25](#), select a check box next to a host name for which you want to know the WatchDog logs and then click the **Watchdog** button.
- Step 2** A window as shown in [Figure 8-22](#), “**WatchDog Logs**,” appears.

Figure 8-22 WatchDog Logs

Name	Size	Last Modified
watchdog.0	255110	Thursday, January 29, 2004 3:45:35 PM PST
watchdog.1	193363	Thursday, January 29, 2004 1:28:30 PM PST

OK

- Step 3** Click on a specific WatchDog log name in the **Name** column to get the contents of that log. You can filter the information in this log. Click **OK** to return to [Figure 8-22](#).
- Step 4** You can repeat the process in [Step 3](#) or click **OK** to return to [Figure 8-17 on page 8-25](#).

Install

You can remotely install the **Processing Server**, **Collection Server**, or **Interface Server**, as follows:



Note

Telnet and ftp *must* be available on both the Master and remote server.



Note

In this remote install, you *must* accept the default values, similar to the **express** install. If you want to do a **custom** install, it is only available through the installation procedure explained in the “Installing ISC” section of Chapter 2 of *Cisco IP Solution Center Installation Guide, 4.0*

- Step 1** From [Figure 8-17 on page 8-25](#), be sure that no check boxes are selected and then click the **Install** button.
- Step 2** A window as shown in [Figure 8-23](#), “Remote Install,” appears.

Figure 8-23 Remote Install

- Step 3** Provide the following information in [Figure 8-23](#).
- **Host Name** (required)
 - **ISC User** (required) This same user *must* be created on the remote server.



Note

Be sure you have 1 GB of disk space available in the ISC User’s home directory.

- **ISC User Password** (required)
- **Role** Accept the default of **Process Server** or click the drop-down menu and choose the **Collection Server** or **Interface Server** option.
- **Install Location** (required)
- **Root Password** (optional) To auto start ISC on a remote server, the root password is required.

- Step 4** Click the **Install** button.
- Step 5** The result is an Install Log.

Uninstall

You can remotely uninstall the **Processing Server**, **Collection Server**, or **Interface Server**, as follows:

- Step 1** From [Figure 8-17 on page 8-25](#), select a check box next to a host name for which you want to uninstall and then click the **Uninstall** button.
- Step 2** A window as shown in [Figure 8-24](#), “**Remote Uninstall**,” appears.

Figure 8-24 Remote Uninstall

- Step 3** Provide the following information in [Figure 8-24](#).
- **ISC User** (required)
 - **ISC User Password** (required)
- Step 4** Click the **Uninstall** button.
- Step 5** The result is an Uninstall Log.

Logs

You can view install and uninstall logs for the Master and remotely installed server, as follows:

- Step 1** From [Figure 8-17 on page 8-25](#), be sure that no check boxes are selected.
- Step 2** Click the **Logs** drop-down menu and select **Install** or **Uninstall**.
- Step 3** The window that appears is the log of installations or uninstallations, dependent on your selection in [Step 2](#).
- Step 4** Click the link in the **Name** column to view the detailed log information.
- Step 5** Click **OK** to return to the window in [Step 3](#).
- Step 6** Click **OK** again to return to [Figure 8-17 on page 8-25](#).

Collection Zones

Navigate **Administration > Control Center**.

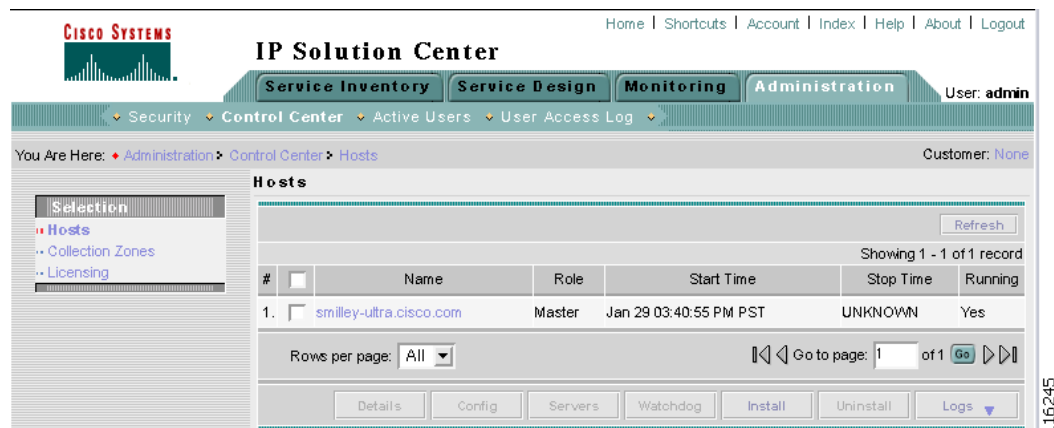
A collection zone is a geographical grouping of devices. Each collection zone is associated with exactly one Collection server that collects data from its devices. However, a Collection server can service multiple collection zones. For example, if you initially create several collection zones and have them all serviced by the Master server, then as the number of devices in each zone grows, you can install additional Collection servers and assign some of the zones to them.

When you install a new Collection server or Processing server, the system creates a new collection zone with the same name as the server. This functionality is for your convenience. You can delete this collection zone if this does not fit your distribution environment setup.

To define collection zones, do the following:

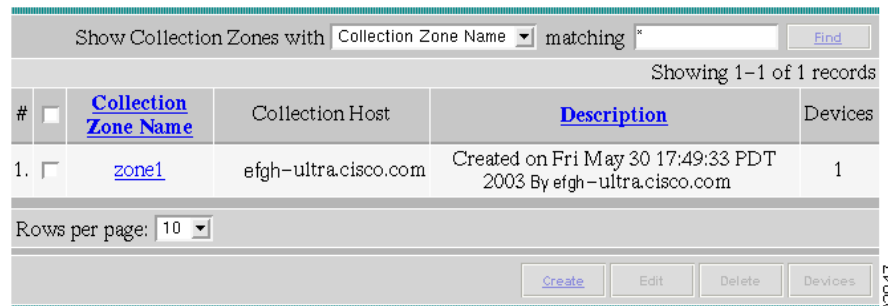
- Step 1** From the Control Center, choose **Collection Zones** from the TOC in the left column, as shown in [Figure 8-25](#), “Choose Control Center > Collection Zones.”

Figure 8-25 Choose Control Center > Collection Zones



- Step 2** A window as shown in [Figure 8-26](#), “Collection Zones,” appears.

Figure 8-26 Collection Zones



- Step 3** To **Create** a collection zone, proceed to [Step 4](#). To **Edit** a collection zone, proceed to [Step 7](#). To **Delete** a collection zone, proceed to [Step 9](#). To display the **Devices**, proceed to [Step 12](#).
- Step 4** From [Figure 8-26](#), without selecting any check boxes, click the **Create** button.

Step 5 A window as shown in [Figure 8-27](#), “Create Collection Zone,” appears.

Figure 8-27 Create Collection Zone

Create Collection Zone

Name *

Description:

Created on Mon Jun 09 01:12:38 PDT 2003
By efigh-ultra.cisco.com

Collection Host:

Note: * - Required Field

Fill in the following information:

- **Name** (required)
- **Description** (optional) This is automatically filled in with the creation statistics: date, time, and creator. You can overwrite this information, add to it, or delete it altogether.
- **Collection Host** (default host appears) Click the drop-down menu if you want to select a different collection host.

- Step 6** Click **Save**. [Figure 8-26](#) reappears, the newly created collection zone is added and a Status appears with a green check in **Succeeded**. You can repeat [Step 4](#) to [Step 6](#) to create another collection zone. For **Edit**, proceed to [Step 7](#). For **Delete**, proceed to [Step 9](#). For **Devices**, proceed to [Step 12](#).
- Step 7** To edit a collection zone, in [Figure 8-26](#), select the check box for the collection zone you want to edit and then click the **Edit** button.
- Step 8** A window as shown in [Figure 8-27](#) appears. Follow the instructions in [Step 5](#) and [Step 6](#).
- Step 9** To delete a collection zone, in [Figure 8-26](#), select one or more check boxes for the collection zone(s) you want to delete. You can select all the collections zones by selecting the check box in the header row. Then click the **Delete** button.
- Step 10** A Confirm Delete window appears to give you a chance to click **Cancel** and not delete or to click **OK** and delete.
- Step 11** [Figure 8-26](#) reappears and the collection zone is removed. You can repeat [Step 9](#) and [Step 10](#) to delete more collection zones, you can proceed to [Step 3](#) to create a collection zone, you can proceed to [Step 7](#) to edit a collection zone, or you can proceed to [Step 12](#) to display and assign devices.
- Step 12** To display, add, or delete devices, in [Figure 8-26](#), select a check box for the desired collection zone. Then click the **Devices** button.
- Step 13** A window appears as shown in [Figure 8-28](#), “Collection Zone Devices.” This window shows the current devices assigned to the selected collection zone.

Figure 8-28 Collection Zone Devices

Collection Zone Devices

Show Devices with Any matching * Find

Showing 1-1 of 1 records

#	☐	Device Name	Collection Zone Name	IP Address	Role	Type
1.	☐	newdevice1	null		CE	IE2100

Rows per page: 10

Add Delete OK Cancel

- Step 14** You can filter the list of devices shown by selecting from the **Show Devices with** drop-down menu, entering what you want to match in **matching**, and then clicking **Find**. To add a device, click **Add**; to delete devices, select the devices you want to delete from those shown and click **Delete** (this happens automatically with no chance to reconsider, but you can add it back in with another **Add** process); to accept what is listed, click **OK**; or to cancel, click **Cancel**.
- Step 15** If you click **Add**, you get a window with all the devices in the database. You can filter the list and from the listed choices you can select one or more devices to add to the selected collection zone. Then click **Select**.
- Step 16** [Figure 8-28](#) reappears with the updated device information for the selected collection zone.
- Step 17** When [Figure 8-28](#) has all the devices you want, click **OK** and [Figure 8-26](#) reappears with the updated information.

Licensing

Navigate **Administration > Control Center**.



Note

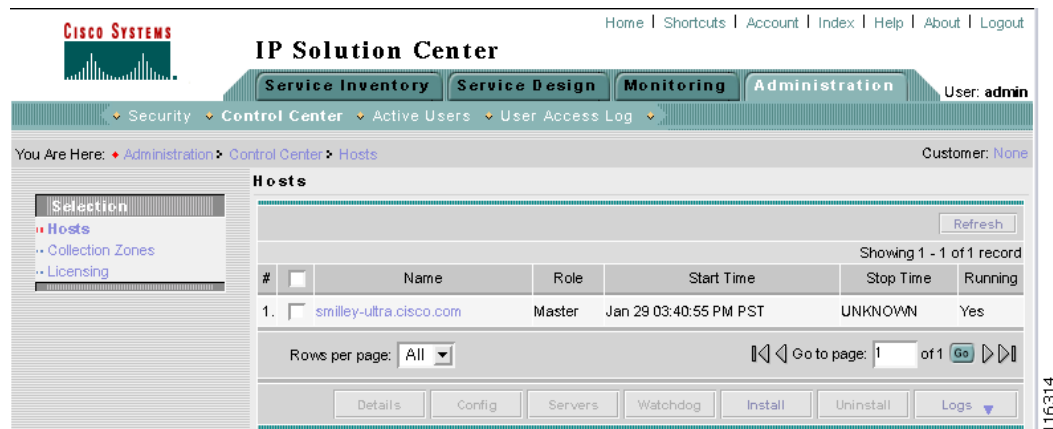
To enable Traffic Engineering Management (TEM), you need to install a permanent license file. You need to replace the `<install_directory>/thirdparty/parc/installed/data/system.properties` file with the `<distribution_directory>/permLic_system.properties` file. For example:

```
cp permLic_system.properties <install_directory>/thirdparty/parc/installed/data/system.properties
```

To install license keys, do the following:

- Step 1** From **Control Center**, choose **Licensing** from the TOC in the left column, as shown in [Figure 8-29](#), “[Choose Control Center > Licensing](#).”

Figure 8-29 Choose Control Center > Licensing



- Step 2** From the **Installed Licenses** table, click the **Install** button, as shown in Figure 8-30, “Install Button.” The Installed Licenses table explains the current statistics. The columns of information tell the **Type** of license keys that you have installed (API-L2VPN, API-L3MPLS, API-SEC (**This feature is NOT SUPPORTED in this release.**), IPSEC (**This feature is NOT SUPPORTED in this release.**), FIREWALL (**This feature is NOT SUPPORTED in this release.**), L2VPN, L3MPLS/VPN, NAT (**This feature is NOT SUPPORTED in this release.**), QOS, TE, TE/BRG, TE/RG, VPLS); the **Size**, which is valid for the **ACTIVATION** (licensed maximum global count of services) or the **VPN** (Maximum number of VPNs licensed); the **Usage**, which gives the number currently used for the rows; and the **Date Updated**, which reflects the refresh of the license usage (on an hourly basis, by default).

**Note**

When you purchase Traffic Engineering Management (TEM), you automatically receive **TE**, **TE/BRG**, and **TE/RG** licenses and an unlimited VPN license. All of these licenses *must* be installed to use the TEM function. The **TE** license serves as an activation license for the maximum number of TE-enabled nodes to be managed by TEM; the **TE/RG** license enables primary tunnel placement; and the **TE/BRG** license enables the Fast ReRoute (FRR) protection function.

**Note**

Click **Refresh** to give the most current status.

Figure 8-30 Install Button

Installed Licenses			
Type	Size	Usage	Date Updated
ACTIVATION	25	4	2004-12-20 16:06
API-L3MPLS			2004-12-20 16:06
FIREWALL			2004-12-20 16:06
IPSEC			2004-12-20 16:06
L2VPN		4	2004-12-20 16:06
L3MPLS/VPN			2004-12-20 16:06
NAT			2004-12-20 16:06
QOS			2004-12-20 16:06
TE	25		2004-12-20 16:06
TE/BRG			2004-12-20 16:06
TE/R/G			2004-12-20 16:06
VPLS			2004-12-20 16:06
VPN	50	1	2004-12-20 16:06

Refresh Install

129 024

- Step 3** In the resulting window, as shown in [Figure 8-31](#), “Enter License Key,” enter a **License Key** that you received on your *Right to Use* paperwork with your product.

Figure 8-31 Enter License Key

The screenshot shows the Cisco IP Solution Center Administration interface. The top navigation bar includes links for Home, Shortcuts, Account, Index, Help, About, and Logout. The user is logged in as 'admin'. The main menu has tabs for Service Inventory, Service Design, Monitoring, and Administration. The left sidebar shows a tree view with Security, Control Center, Active Users, and User Access Log. The 'Control Center' tab is selected, and the 'Licensing' sub-tab is active. The main content area is titled 'Install a License Key' and contains a form with a 'License Key' field and 'Save' and 'Cancel' buttons. A note at the bottom states: 'Note: * - Required Field'.

116 281

- Step 4** Click **Save**. Your newly installed license appears in an updated version of the Installed License table, as shown in [Figure 8-30](#), “Install Button.”
- Step 5** Repeat [Step 2](#), [Step 3](#), and [Step 4](#) for each of the *Right to Use* documents shipped with your product.

**Note**

When you receive multiple *Right to Use* documents to upgrade either the ACTIVATION License, which activates and sets the maximum global count of the services, or VPN licenses, which activates and set the maximum number of VPNs, be sure to enter the licenses in the correct order. For example, if you are upgrading from 500 to 3000 global count of the services and there are two steps to get there, enter the license to upgrade from 500 to 1500 and then the license key to upgrade from 1500 to 3000.

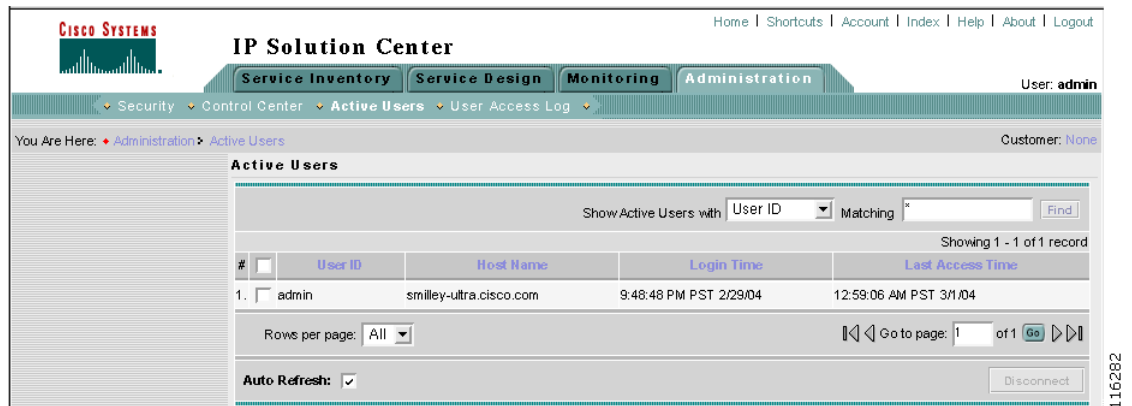
Active Users

This section explains how to communicate with active users.

Navigate **Administration > Active Users** and follow these steps:

- Step 1** After you navigate **Administration > Active Users**, a window that shows the currently logged users appears, as shown in [Figure 8-32](#), “Active Users.”

Figure 8-32 Active Users



- Step 2** In [Figure 8-32](#), if you have the privileges of **SysAdmin** or **UserAdmin**, you can disconnect one or more users. Select the check box next to each user you want to disconnect or select the check box in the header row, to select all the users. Then click the **Disconnect** button at the bottom of the window.



Caution

The current login sessions for the disconnected users are terminated and their work is lost.

- Step 3** To exit this list of all active users, choose another feature from the main product tabs.

User Access Log

This section shows a detailed report of every activity by every user.

Navigate **Administration > User Access Log** and follow these steps:

- Step 1** After you navigate **Administration > User Access Log**, a window appears as shown in [Figure 8-32](#), “Active Users.”

Figure 8-33 User Access Log Viewer with Simple Filter

The screenshot shows the IP Solution Center interface with the 'User Access Log Viewer' tab selected. The 'Simple Filter' radio button is selected. The 'Filter By' dropdown is set to 'Date'. The 'Matches' field is empty. The 'Find' button is visible. The table displays 5 records of user access logs.

#	Date	Time	User Name	Origin Host	Action	Object	Severity	Activity	Message
1.	2004/03/01	01:54:15	admin	smiley-ultra.cisco.com	Logon	User	INFO	SecurityActivity	Login successfully.
2.	2004/03/01	01:52:28	admin		SessionTimeout	User	INFO	SecurityActivity	Session timed out.
3.	2004/03/01	01:35:23	admin		SessionTimeout	User	INFO	SecurityActivity	Session timed out.
4.	2004/03/01	01:21:01	admin	smiley-ultra.cisco.com	Logon	User	INFO	SecurityActivity	Login successfully.
5.	2004/03/01	00:44:11	backendadm		Logon	User	ERROR	SecurityActivity	Login failed.

Showing 1 - 5 of 4,043 records

Rows per page: 5

Go to page: 1 of 809

All the log information about user actions appears.



Note

The types of activities or objects to be logged can be configured. This can be done directly through SQL. By default, security-related activities and activities on objects listed in the Role editor are logged.

- Step 2** The default **Simple Filter** radio button is selected. To filter using the **Simple Filter**, continue with [Step 3](#). To filter using **Advanced Filter**, proceed to [Step 5](#).
- Step 3** To filter the information with **Simple Filter**, keep the **Simple Filter** radio button selected and from **Filter By**, choose: **Date**, **User Name**, **Origin Host**, **Action**, **Severity**, or **Activity** (also column names). For **Matches**, enter the beginning characters of what you want to match followed by *. Then click **Find**. The result is that only the log information matching the entered filter appears.
- Step 4** To exit this log report, choose another feature from the main product tabs.
- Step 5** To filter the information with **Advanced Filter**, click the **Advanced Filter** radio button. A window as shown in [Figure 8-34](#), “**User Access Log Viewer with Advanced Filter**,” appears.

Figure 8-34 User Access Log Viewer with Advanced Filter

The screenshot shows the IP Solution Center interface with the 'User Access Log Viewer' tab selected. The 'Advanced Filter' radio button is selected. The 'Find' button is visible. The table displays 5 records of user access logs.

#	Date	Time	User Name	Origin Host	Action	Object	Severity	Activity	Message
1.	2004/03/01	01:54:15	admin	smiley-ultra.cisco.com	Logon	User	INFO	SecurityActivity	Login successfully.
2.	2004/03/01	01:52:28	admin		SessionTimeout	User	INFO	SecurityActivity	Session timed out.
3.	2004/03/01	01:35:23	admin		SessionTimeout	User	INFO	SecurityActivity	Session timed out.
4.	2004/03/01	01:21:01	admin	smiley-ultra.cisco.com	Logon	User	INFO	SecurityActivity	Login successfully.
5.	2004/03/01	00:44:11	backendadm		Logon	User	ERROR	SecurityActivity	Login failed.

Showing 1 - 5 of 4,043 records

Rows per page: 5

Go to page: 1 of 809

All the log information about user actions appears.

- Step 6** Enter filter information you want to match in one or more of the following categories and then click **Find**.

**Note**

When you choose multiple filters, the log results that appear are only the ones that match all the specified filter information.

- **Date** Enter the beginning characters of the date you want to view followed by a *, in the format given in the **Date** column.
- **User Name** Enter the beginning characters of the specific **User Name** you want to view followed by a *.
- **Host Name** Enter the beginning characters of the specific **Host Name** you want to view followed by a *.
- **Action** Click the drop-down button and choose from: **UNKNOWN; View; Create; Modify; Delete; Logon; Logoff; Session Timeout**. If you decide not to use this filter, just keep *.
- **Severity** Click the drop-down button and choose from: **UNKNOWN; INFO; WARNING; ERROR**. If you decide not to use this filter, just keep *.
- **Activity** Click the drop-down button and choose from: **UNKNOWN; SecurityActivity; or UserActivity**. The result is that only the log information matching the entered filter appears.

Step 7

To exit this log report, choose another feature from the main product tabs.

Manage TIBCO Rendezvous

The only reason you would ever use this functionality is if you change the TIBCO ports for TIBCO Rendezvous Agent (rva) or TIBCO Rendezvous Daemon (rvd) after installation. The changes being made here only affect Java WebStart applications, such as Inventory Manager and the topology tool.

Navigate **Administration > Manage TIBCO Rendezvous** and follow these steps:

- Step 1** After you navigate **Administration > Manage TIBCO Rendezvous**, a window appears as shown in [Figure 8-35](#), “**TIBCO Rendezvous**.”

Figure 8-35 TIBCO Rendezvous

TIB/Rendezvous [efgh-ultra]
Agent for Java - 7.1.3
2003-06-18 22:50:06

State: **Component Information**

[information](#)
Configuration:
[change state](#)
[security](#)
[connection](#)
[subjects](#)
[http tunnel](#)
[certificates](#)
Miscellaneous:
[copyright](#)
[web home](#)

component:	rva
version:	7.1.3
license ticket:	65599
host name:	efgh-ultra
IP address:	128.107.128.130
client port:	7600
http tunnel:	enabled on main port
state:	running
total clients:	0
direct clients:	0
tunnel clients:	0

95362

- Step 2** From [Figure 8-35](#), click **connection**, as described in [Step 3](#); and click **change state**, as described in [Step 4](#). These are choices in the left column of [Figure 8-35](#).
- Step 3** In [Figure 8-35](#), when you click **connection**, a window such as [Figure 8-36](#), “**Connection Configuration**,” appears.

Figure 8-36 Connection Configuration

Connection Configuration

Accept Client Connections on Listen Port: 7600

TIB/Rendezvous Daemon Connection:

service:	7530
network:	
daemon:	

Submit Reset

95361

If you must change the **rva** port number from the existing value, change the **Accept Client Connections on Listen Port:** field to your new rva port number for ISC. If you must change the **rvd** port number from the existing value, change the **service** field to your new rvd port number for ISC. Then click **Submit**. Then [Figure 8-36](#) returns with the new value and a note that says “Configuration change will take effect after RVA is re-activated. To re-activate RVA set it into idle state and then back to active state.”

- Step 4** In [Figure 8-35](#), click **change state**, follow the instructions, and you complete this functionality.
- Step 5** From a terminal window, change to the **bin** directory of your ISC installation, such as **/opt/isc-3.2/bin**

Step 6 Source the ISC environment:

- C Shell - use the command **source ./vpnenv.csh**
- K Shell or Bash - use the command **./vpnenv.sh**

Step 7 To start the script, at the command line type **updateWebStartJars**.

Step 8 The next time you start a Java WebStart, such as Inventory Manager or the topology tool, these changes are in effect.



Cisco CNS IE2100 Appliances

Cisco IP Solution Center (ISC) supports the Cisco CNS IE2100 Device Access Protocol for communication with any Cisco IOS device, such as uploading a configuration file from a device, downloading a configlet to a device, or executing a command on a device and obtaining a result. ISC also supports CNS Plug-and-Play.

To use the Cisco CNS IE2100 functionality on ISC, you must first set up the Cisco CNS IE2100 appliance and the ISC workstation as explained in an appendix in [Cisco IP Solution Center Installation Guide, 4.0](#).

This appendix includes the following sections. Implement these sections in sequence:



Note

The “[Using Plug-and-Play](#)” section on page A-6 is optional.

1. [Creating a Cisco CNS IE2100 Appliance](#), page A-1
2. [Creating a Cisco IOS Device Using the Cisco CNS Device Access Protocol](#), page A-3
3. [Using Plug-and-Play](#), page A-6

Creating a Cisco CNS IE2100 Appliance

ISC supports multiple Cisco CNS IE2100 appliances. To create a Cisco CNS IE2100 appliance, follow these steps:

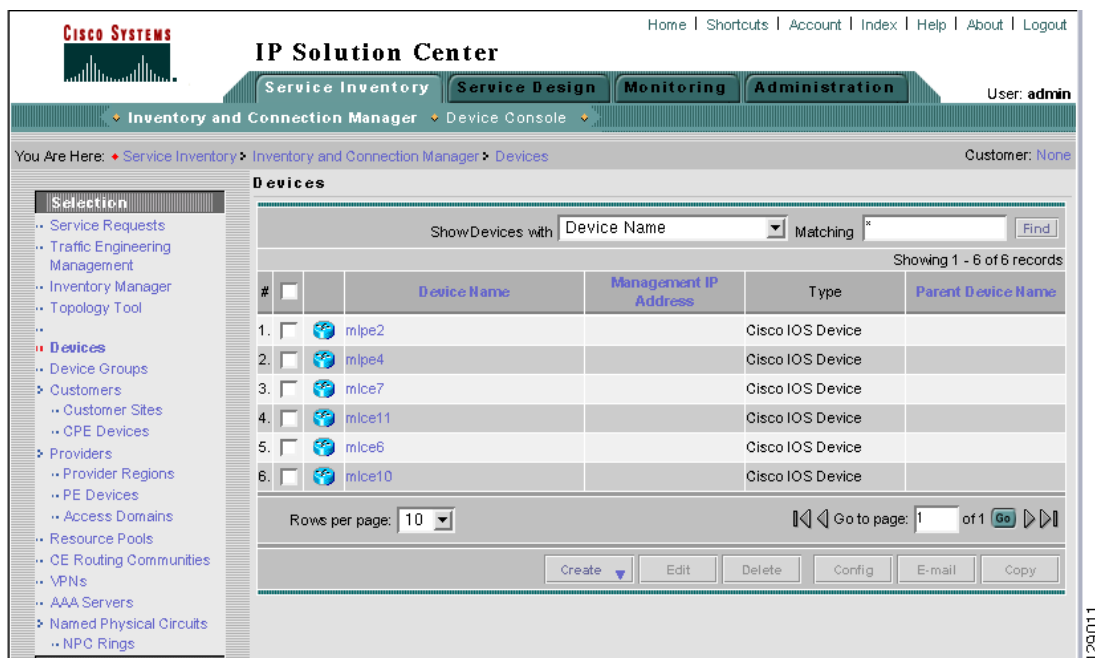


Note

For more information, see the [Devices](#) section of [Chapter 3, “Service Inventory > Inventory and Connection Manager”](#).

- Step 1** Navigate **Service Inventory > Inventory and Connection Manager > Devices**.
- Step 2** A window appears as shown in [Figure A-1, “Devices Window.”](#)

Figure A-1 Devices Window



Step 3 Click the **Create** button.

Step 4 From the **Create** menu, click **IE2100**.

A window appears as shown in Figure A-2, “Create IE2100 Device Window”.

Figure A-2 Create IE2100 Device Window

The screenshot shows the 'Create IE2100 Device Window' form. It has a 'General' tab with the following fields: Device Host Name (required), Device Domain Name, Description, and IP Address. Below the fields are 'Save' and 'Cancel' buttons. A note at the bottom states: 'Note: * - Required Field'.

Step 5 Enter the **Device Host Name** and if applicable, the **IE2100 Device Domain Name**. If the Cisco CNS IE2100 appliance is not registered with DNS, then you must enter the **IP Address** of the Cisco CNS IE2100 appliance. Click **Save**.

Figure A-1 reappears with the IE2100 listed as a device.

Creating a Cisco IOS Device Using the Cisco CNS Device Access Protocol

Each Cisco CNS IE2100 appliance can serve multiple Cisco IOS devices. A Cisco IOS device can only be served by one Cisco CNS IE2100 appliance. To create a Cisco IOS device using the Cisco CNS Device Access Protocol, follow these steps:

**Note**

For more information, see the [Devices](#) section of [Chapter 3, “Service Inventory > Inventory and Connection Manager”](#).

Step 1 Navigate **Service Inventory > Inventory and Connection Manager > Devices**.

Step 2 A window appears as shown in [Figure A-1, “Devices Window.”](#)

Step 3 Click the **Create** button.

Step 4 From the **Create** menu, click **Cisco IOS Device**.

A window appears as shown in [Figure A-3, “Create Cisco IOS Device Window.”](#)

Figure A-3 Create Cisco IOS Device Window

General

Device Host Name^{*}:

Device Domain Name:

Description:

Collection Zone:

Management IP Address:

Interfaces:

Associated Groups:

Login and Password Information

Login User:

Login Password:

Verify Login Password:

Enable User:

Enable Password:

Verify Enable Password:

Device and Configuration Access Information

Terminal Session Protocol:

Config Access Protocol:

SNMP Version:

SNMP v1/v2c

Community String RO:

Community String RW:

Additional Properties:

Note: * - Required Field

96323

Step 5 In the **General** section, enter the **Device Host Name** and **Device Domain Name**.

For **CNS Device Access Protocol**, you do not need to define the parameters in the **Login User** and **Login Password** sections.

For the **Device and Configuration Access Information** section, you must select **CNS** for the **Terminal Session Protocol**. Defining Cisco IOS Device Properties

Step 6 Click the **Edit** button for **Additional Properties** at the bottom of the window. A window as shown in [Figure A-4](#), “Cisco IOS Device Additional Properties,” appears.

Figure A-4 Cisco IOS Device Additional Properties

Cisco IOS Device Properties	
Device:	
SNMP v3	
SNMP Security Level:	Default (No Authentication/No Encryption) ▼
Authentication User Name:	
Authentication Password:	
Verify Authentication Password:	
Authentication Algorithm:	None ▼
Encryption Password:	
Verify Encryption Password:	
Encryption Algorithm:	None ▼
Terminal Server and CNS Options	
Terminal Server:	None ▼
Port:	0
Fully Managed:	☐
Device State:	ACTIVE ▼
CNS Identification:	
Device Event Identification:	CNS_ID ▼
Most recent CNS event:	None ▼
IE2100:	None ▼
CNS Software Version:	1.3.2 ▼
CNS Device Transport:	HTTP ▼
Device Platform Information	
Platform:	
Software Version:	
Image Name:	
Serial Number:	
Device Owner's Email Address:	
OK Cancel	

111006

Step 7 The following steps pertain to the **Terminal Server** and **CNS Options** section.

Step 8 Select the **Fully Managed** check box if you want the device to become a fully managed device. For fully managed devices, ISC sends e-mail notifications upon receipt of device configuration changes originated outside ISC and schedules enforcement audit tasks upon detection of possible intrusion.

**Note**

Be sure to set the DCPL parameters for e-mail and Fully Managed, as explained in the [“Config” section on page 8-27](#). Navigate **Administration > Control Center**. Select a Host and then click **Config**. Then in the TOC in the left column, be sure to enter appropriate information in the following four fields: **SYSTEM > email > from**; **SYSTEM > email > smtpHost**; **SYSTEM > fullyManaged > enforcementAuditScript**; and **SYSTEM > fullyManaged > externalEventsEmailRecipients**.

**Note**

Verify that the **cns config notify** command is configured for the IOS device.

Step 9 Specify the **Device State**, as follows:

- Select **ACTIVE** (the default) if the router is physically present on the network.
- Select **INACTIVE** if the router is not yet physically present on the network.

Step 10 Specify the **Device Event Identification**, as follows:

- Select **HOST_NAME** if the **Device Host Name** as defined in [Step 5](#) is to be used as the **CNS Identification** for this device.
- Select **CNS_ID** if the device CNS Identification string is other than the **Device Host Name**.
- If you have selected **CNS_ID** as the **Device Event Identification**, you must enter the **CNS Identification** parameter in the field labeled **CNS Identification**. This must be a unique argument. It is used to create the device in the corresponding Cisco CNS IE2100 repository and to listen to events pertaining to this device.

**Note**

Verify that the **cns id string {CNS_ID} event** command is configured for the IOS device.

Step 11 Select the Cisco CNS **IE2100** appliance that serves this Cisco IOS device. Select one entry from the drop-down menu of IE2100 devices already defined in the repository.

Step 12 Use the drop-down menu for **CNS Software Version** to choose the version of Cisco CNS Configuration Engine that manages the IOS device (1.3, 1.3.1, 1.3.2, or 1.4).

Step 13 Use the drop-down menu for **CNS Device Transport** to choose HTTP or HTTPS as the transport mechanism used by ISC to create, delete, or edit devices in the IE2100 repository. If HTTPS is used, the Cisco CNS Configuration Engine must be running in secure mode.

Step 14 Click **OK**. [Figure A-1](#) reappears with the Cisco IOS device listed.

Using Plug-and-Play

ISC supports the Plug-and-Play device configuration through a Cisco CNS IE2100 appliance. ISC supports devices not physically present on the network.

The procedures for using Plug-and-Play when the Cisco IOS device is not physically present on the network vary depending on whether there is an initial configuration file for the device.

Follow these steps if the Cisco IOS device *does not* have an initial configuration file:

-
- Step 1** Create a Cisco IOS Device as described in the “[Creating a Cisco IOS Device Using the Cisco CNS Device Access Protocol](#)” section.
- Step 2** Define the Cisco IOS device properties as shown in [Figure A-4](#).
Be sure to specify the **Device State** as **INACTIVE** because the device is not physically present on the network
- Step 3** Click **Save**.
A Cisco IOS Device entry is created in the ISC repository and in the corresponding Cisco CNS IE2100 appliance repository.
-

Follow this step if the Cisco IOS device *does* have an initial configuration file:

-
- Step 1** Import the initial configuration file into ISC using the Inventory Manager functionality, explained in [Chapter 4, “Service Inventory > Inventory and Connection Manager > Inventory Manager”](#) in this manual.
Be sure to specify the **Device State** as **INACTIVE** because the device is not physically present on the network.
The Inventory Manager create a Cisco IOS Device entry in the ISC repository. Also, it creates an entry in the corresponding Cisco CNS IE2100 repository, and associates the specified initial configuration file with this new device in the Cisco CNS IE2100 repository.
-

You can provision the newly created inactive Cisco IOS Device for different services. Because the device is not physically present on the network, ISC saves the configlets associated with these services in its repository and tries to download them to the device only after the device has come up. Until the device is physically present on the network, the service request goes into the **WAIT_DEPLOY** state. The service requests are explained in the user guides for each of the services.

After the device comes up and connects to its corresponding Cisco CNS IE2100 appliance, the device retrieves and applies its initial configuration if there is one waiting for it in the Cisco CNS IE2100 repository.

ISC detects that the device has come onto the network and performs the following actions:

- Changes the Cisco IOS Device state from **INACTIVE** to **ACTIVE**.
ISC performs a collect config of the IOS device and stores it in the ISC repository.
- Verifies whether any ISC service has been waiting for this device to come up and tries to download the corresponding configlets to the device to complete the service request.



Property Settings

To navigate to the properties, known as Dynamic Component Properties Library (DCPL), navigate to the tab **Administration > Control Center > Hosts**. Then select a check box for a specific host and click the **Config** button.



Note

More details about this are explained in the [“Config” section on page 8-27](#).

When you click on the folder or subfolder, it expands to more subfolders or eventually to the property itself. Then you receive an explanation, default values, and in some cases range and rules. This table can help you understand all the properties available at a glance. The properties are listed alphabetically. When a / ends an entry, this means it can be expanded further. Also, if you are searching for a property and do not know the name, you can use some key words and do a Find on the pdf version.

Table B-1 DCPL Properties

Property	Default Value	Range/Rules	Explanation
AutoDiscovery Property:			Controls the operation of Autodiscovery.
/DiscoveryTemplateFolder	/Discovery	string	Template folder under which the templates to be discovered for MPLS VPN Discovery will reside.
/performTemplateDiscovery	false	The valid values are true and false .	With this flag, the user can control the template discovery. For performance reasons, if the template discovery is not desired this should be set to false.
Cleanup Properties:			Cleans up various system resources such as log files and temporary files.
/Cleanup/RuntimeTasks/			This component cleans up old runtime task logs.
maxAgeInHours	168	integer	Maximum age for a runtime task in hours. Runtime tasks older than this age will be deleted during the next cleanup cycle. Set to 0 to disable this feature.
sleepIntervalInHours	24	integer, 1-1000 hours	Time in hours for runtime task cleanup service to sleep between clean up cycles.

Table B-1 DCPL Properties (continued)

/Cleanup/TaskLogs/			This component cleans up old TaskLogs.
maxAgeInHours	168	integer	Maximum age of the TaskLogs in hours. TaskLogs older than this age will be deleted during the next cleanup cycle. Set to 0 to disable this feature.
sleepIntervalInHours	24	integer, 1-1000 hours	Time in hours for taskLog cleanup service to sleep between clean up cycles.
/Cleanup/TempFiles/			This component cleans up old temporary files.
maxAgeInHours	168	integer	Maximum age of the temporary files in hours. Temporary files older than this age will be deleted during the next cleanup cycle. Set to 0 to disable this feature.
sleepIntervalInHours	24	integer, 1-1000 hours	Time in hours for tempFile cleanup service to sleep between clean up cycles.
/Cleanup/logLevel	CONFIG	selection	This log Level is used only if there is no log Level defined for a component. The log Level is the level at which logging is done for this component. These levels are identical to the logging levels defined for JDK1.4 logging package. The levels in descending order are: SEVERE (highest value) WARNING INFO CONFIG FINE FINER FINEST (lowest value).
DCS Properties:			Device Configuration Service. This component corresponds to a library that is used by ISC to communicate with network devices using protocols such as telnet, ssh, tftp, and so forth.

/DCS/CATWarningExpressions		string	CatOS (Catalyst switch) warning expressions that can be safely ignored; case insensitive; . matches any char except newline, * means zero or more, + means one or more, ? means zero or one. All regular expressions except the last one should have a \$ at the end of the regular expression. ^.??.??.??.?-[5-7]- \$ Access Rules Download Complete\$ also defined on firewall module (Firewall is NOT SUPPORTED in this release.)\$ Adding vlans .* to allowed list.\$ already allowed on the trunk\$ CDP disabled on port.*\$ Dot1q tunnel feature disabled.*\$ Dot1q tunnel feature set to.*\$ Jumbo frames enabled on port .*\$ Jumbo frames disabled.*\$ Layer 2 protocol tunneling enabled.*\$ Layer 2 protocol tunneling disabled.*\$ Packets on native vlan will be tagged on .*\$ Port .* enabled\$ Removing Vlan.*\$ Secured .* cleared from\$.?security level for .* changed to\$.*successful\$ This command will deactivate.*\$ Vlan .* also defined on firewall module (Firewall is NOT SUPPORTED in this release.)\$ Vlans .* declared secure for firewall module (Firewall is NOT SUPPORTED in this release.)\$ VLAN Mod/Ports.*\$ VTP advertisements transmitting temporarily stopped.*\$ VLAN .* modified*\$ VLAN .*Mod/Ports .*\$
/DCS/FTP/			FTP Settings.
ftpPassword		string	Password for FTP server login, used by DCS and GTL.
ftpRootDirectory		string	FTP root directory, used by DCS and GTL.
ftpServer		string	FTP Server host name or IP address, used by DCS and GTL.

Table B-1 DCPL Properties (continued)

ftpSubDirectory		string	FTP sub directory, used by DCS and GTL.
ftpUsername		string	Username for FTP server login, used by DCS and GTL.
DCS/IOSUsePrimaryWarningExprOnly	true	The valid values are true and false .	If true , DCS uses only the primary warning expression list, specified in DCS/IOSWarningExpressions. If false , DCS uses the primary list specified in DCS/IOSWarningExpressions for add and modify operations and uses the list specified in DCS/IOSWarningExpressionsRemoveCfg during delete (decommissioning) operations.

Table B-1 DCPL Properties (continued)

/DCS/IOSWarningExpressions		string	IOS warning expressions that can be safely ignored; case insensitive; . matches any char except newline, * means zero or more, + means one or more, ? means zero or one. All regular expressions except the last one should have a \$ at the end of the regular expression. %Aborting Save. Compress the config\$. *Access Rules Download Complete\$ % Access VLAN does not exist.\$ Address aliases with.*\$ % All RSA Keys will be removed.\$ % All router certs issued using these keys will also be removed.*\$ % Already found same .* statement in this profile\$. *also defined on firewall module\$ (Firewall is NOT SUPPORTED in this release.) % A profile is deemed incomplete until it has match identity statements\$. *certificate accepted\$ Certificate request sent\$.?Changes to the System MTU will not take effect until the next reload.*\$ CNS config partial agent is running already\$ % Configuration buffer full, can't add command.*\$. *Crypto EzVPN does not exist.*\$ % declared secure for firewall module\$ (Firewall is NOT SUPPORTED in this release.) Enter configuration commands, one per line\$ Explicit Path name .*\$ % Generating .* bit RSA keys\$ Global .* will be Port Address Translated.*\$ Global Ethernet MTU is set to.*\$ If the interface doesn't support baby giant frames.*\$ Increasing .* burst size to\$ % Interface .* IP address .* removed due to enabling VRF\$ % Interface .* IP address .* removed due to disabling VRF\$ % IP addresses from all interfaces in VRF .*have been removed\$

Table B-1 DCPL Properties (continued)

/DCS/IOSWarningExpressions (Continued)		string	% IP routing table V.* does not exist. Create first\$ % IP routing table g.*does not exist. Create first\$ % No CEF interface information\$ %No matching route to delete\$ %Translation not found\$.*Not all config may be removed and may reappear after reactivating\$ ^%.*NOTE:\$ OSPF: Unrecognized virtual interface .* Treat it as loopback stub route\$ outside interface address added\$ % Profile already contains this keyring\$ %PVC is already defined\$ Restarting RADIUS authentication service on port .*\$ \$ Restarting RADIUS accounting service on port .*\$ Redundant .* statement\$ security level for .* changed to\$.*Service policy .* is already attached\$ % Signature RSA Keys not found in configuration.\$.*success\$ The .*command will also show the fingerprint\$ %The static routes in .* with outgoing interface .* will be removed\$ Unable to disable parser cache\$ % Unknown VPN\$.* Unknown VRF specified\$ Vlan .* also defined on firewall module\$ (Firewall is NOT SUPPORTED in this release.) Vlans .* declared secure for firewall module\$ (Firewall is NOT SUPPORTED in this release.) % VRF .* does not exist or does not have a RD\$.*warning.*
DCS/IOSWarningExpressionsRemoveCfg		string	IOS warning expressions that can be safely ignored during decommissioning; case insensitive; . matches any char except newline, * means zero or more, + means one or more, ? means zero or one.

Table B-1 DCPL Properties (continued)

/DCS/PIXWarningExpressions (NOT SUPPORTED in this release.)		string	PIX warning expressions that can be safely ignored; case insensitive; . matches any char except newline, * means zero or more, + means one or more, ? means zero or one. All regular expressions except the last one should have a \$ at the end of the regular expression. Access Rules Download Complete\$ Added .*to the bridge table\$.*also defined on firewall module\$ arp inspection disabled on \$ arp inspection enabled on \$ bytes copied in \$ Cannot overwrite an already existing static entry\$ Configurations are no longer synchronized\$ Creating context\$ Disabling learning on\$ Enabling learning on\$ Please wait\$ MAC address.* has been deleted from the bridge table\$ Disabling failover\$ Global .* will be Port Address Translated\$ outside interface address added\$ %PIX-7-\$ %PIX-6-\$ %PIX-5-\$ Restarting .* service\$ Secured .* cleared from\$ security level for .* changed to\$ Vlan .* also defined on firewall module\$ Vlans .* declared secure for firewall module\$ VLAN Mod/Ports.*
/DCS/RCP/			RCP Settings.
rcpDirectory	/tmp	string	Directory to use for uploaded/downloaded config files.

Table B-1 DCPL Properties (continued)

/DCS/SSH/			SSH Client Settings.
overWriteSSHKeys	true	The valid values are true and false .	Overwrite SSH Keys: If true , will allow new keys to overwrite existing keys in the key file for a given host. If false , an error will be displayed if host sent key does not match the server sent key.
sshEncryptionCipher	3DES->DES	selection	Cipher to use for SSH Encryption/Decryption; requires restart on change. Values: 3DES->DES first tries 3DES then if not available falls back to DES; 3DES, only tries 3DES; DES, only tries DES.
/DCS/TFTP/			TFTP Settings.
tftpCreateFileOnServerBeforeUpload	true	The valid values are true and false .	Some TFTP servers require a file to exist on the server with write access before a TFTP client can upload it. This is sometimes called write-replace or overwrite mode. Other TFTP servers require a that a file NOT exist, this is sometimes called write-create or no overwrite mode. When true , DCS will create the file on the TFTP server before uploading device configuration.
tftpRootDirectory	/tftpboot	string	TFTP Root Directory used by DCS and GTL.
tftpServerIPAddress		string	TFTP Server host name or IP Address used by DCS and GTL.
tftpSubDirectory		string	TFTP Sub Directory used by DCS and GTL.
/DCS/allowCommandDownloadOnError	false	The valid values are true and false .	Continue command download on error.
/DCS/cnsEventTimeout	120	integer, 0-120 seconds	CNS event wait time in seconds
/DCS/customPasswordPrompt	Password:	string	Device Custom password prompt.
/DCS/customUsernamePrompt	Username:	string	Device Custom User name prompt.
/DCS/logLevel	CONFIG	selection	The log Level is the level at which logging is done for this component. These levels are identical to the logging levels defined for JDK1.4 logging package. The levels in descending order are: SEVERE (highest value) WARNING INFO CONFIG FINE FINER FINEST (lowest value).

Table B-1 DCPL Properties (continued)

/DCS/maxDeviceConnectCompleteTime	60	integer, 15-600 seconds	Maximum time in seconds to wait for a terminal session connection to a device.
/DCS/maxDeviceConnectRetryCount	3	integer, 0-5	Maximum number of times to retry connecting to a device when the maxDeviceConnectCompleteTime expires. 0= no retries.
/DCS/maxOperationTimeout	30	integer, 5-300 minutes	Maximum time in minutes to wait for a device operation to complete.
/DCS/maxPromptTimeout	60	integer, 15-300 seconds	Maximum time in seconds to wait for a prompt during a terminal session with a device.
/DCS/maxSocketReadTimeout	30	integer, 10-300 seconds	Maximum time in seconds to wait for data on a socket connection read operation.
DeploymentFlow Property:			
/DeploymentFlow/logLevel	CONFIG	selection	Deployment flow Component: Used to create a flow of different types of steps such as mpls, ipsec (IPsec is NOT SUPPORTED in this release.), qos and nat (NAT is NOT SUPPORTED in this release.).
DistributionFramework Properties:			
/DistributionFramework/Dispatcher/			The log Level is the level at which logging is done for this component. These levels are identical to the logging levels defined for JDK1.4 logging package. The levels in descending order are: SEVERE (highest value) WARNING INFO CONFIG FINE FINER FINEST (lowest value).
DefaultUnitDuration	1000	integer	Distribution Framework. This component handles the distribution of work (jobs) between different servers in a ISC distributed installation.
PingInterval	1000	integer	Service that dispatches jobs to workers.
ProcessorEpsilon	10	integer	The unit duration (in ms) used to estimate jobs without a profile.
ProfileUpdateThreshold	10	integer	The interval (in ms) dispatcher pings the workers to get the load.
			If two processors differ in usage by an amount less than this, they are considered identical from the point of view of the load balancer.
			The percent change of a profile that triggers an update of the dispatcher.

Table B-1 DCPL Properties (continued)

logLevel	CONFIG	selection	The log Level is the level at which logging is done for this component. These levels are identical to the logging levels defined for JDK1.4 logging package. The levels in descending order are: SEVERE (highest value) WARNING INFO CONFIG FINE FINER FINEST (lowest value).
/DistributionFramework/NamingHost	<master_server>	string	The hostname or ip address of the name server.
/DistributionFramework/NamingPort	<naming_port>	string	The port of the name server.
/DistributionFramework/RemoteUtil/			Layer abstracting the remote call functionality.
logLevel	CONFIG	selection	The log Level is the level at which logging is done for this component. These levels are identical to the logging levels defined for JDK1.4 logging package. The levels in descending order are: SEVERE (highest value) WARNING INFO CONFIG FINE FINER FINEST (lowest value).
/DistributionFramework/ServiceLauncher/			Manages the execution of multiple services in the same VM.
logLevel	CONFIG	selection	The log Level is the level at which logging is done for this component. These levels are identical to the logging levels defined for JDK1.4 logging package. The levels in descending order are: SEVERE (highest value) WARNING INFO CONFIG FINE FINER FINEST (lowest value).
/DistributionFramework/ThreadPool/			Thread pool component used by the worker to execute jobs.
logLevel	CONFIG	selection	The log Level is the level at which logging is done for this component. These levels are identical to the logging levels defined for JDK1.4 logging package. The levels in descending order are: SEVERE (highest value) WARNING INFO CONFIG FINE FINER FINEST (lowest value).
/DistributionFramework/Worker/			Worker.
Groups		string	The groups this worker belongs to. This property is deprecated because groups are stored in the database rather than being provided by the worker.

Table B-1 DCPL Properties (continued)

ThreadPoolSize	100	integer	The maximum number of threads. Set it to 0 to allow the pool to use as many thread as necessary.
logLevel	CONFIG	selection	The log Level is the level at which logging is done for this component. These levels are identical to the logging levels defined for JDK1.4 logging package. The levels in descending order are: SEVERE (highest value) WARNING INFO CONFIG FINE FINER FINEST (lowest value).
GSAM Property:			Generic Service Access Model to get an XML dump from the repository for the provisioning driver.
/GSAM/logLevel	CONFIG	selection	The log Level is the level at which logging is done for this component. These levels are identical to the logging levels defined for JDK1.4 logging package. The levels in descending order are: SEVERE (highest value) WARNING INFO CONFIG FINE FINER FINEST (lowest value).
GTL Properties:			Generic Transport Layer. This library provides an API to different jobs (such as provisioning, collection etc.) to access Device Configuration Service (DCS). The jobs do not interface with DCS directly (to access the devices), but work with the API provided by GTL.
/GTL/CSL/			Configuration Services Layer
ios/			IOS related properties.
cmdsRequiringDelay		string	List of the IOS commands that execute asynchronously and require time to be processed before they are reflected in the running configuration. Matching rules: case insensitive, . matches any char except newline, * means zero or more, + means one or more, ? means zero or one.

Table B-1 DCPL Properties (continued)

delayAfterDownloadingCmd		command name:integer, 0-1800 seconds	List of the IOS commands that require a delay after they are downloaded using a terminal session protocol, such as Telnet. The character ; delimits the list elements. The IOS command in each list element must be followed by the character : followed by a maximum integer of 1800, which indicates the number of seconds to delay, thus indicating 0-1800 seconds (0-30 minutes). The command matching rules: case insensitive, . matches any char except newline, * means zero or more, + means one or more, ? means zero or one. The default is a blank field.
delayBeforeDownloadingCmd			List of the IOS commands that require a delay before they are downloaded using a terminal session protocol, such as Telnet. The character ; delimits the list elements. The IOS command in each list element must be followed by the character : followed by a maximum integer of 1800, which indicates the number of seconds to delay, thus indicating 0-1800 seconds (0-30 minutes). The command matching rules: case insensitive, . matches any char except newline, * means zero or more, + means one or more, ? means zero or one.
delayBeforeUpload		integer, 0-30 seconds	The delay in seconds to wait after downloading a configlet that contains async. commands before uploading the new configuration.
delayBeforeWriteMem	0	integer, 0-300 seconds	The delay in seconds to wait after downloading a configlet before performing a write memory command.
/GTL/device-config-access-protocol	1	integer, 1-3	Protocol to use for device configuration uploads and downloads. 1= TERMINAL (Use the device-terminal-session-protocol for config access) 2= TFTP 3= FTP.
/GTL/device-terminal-session-protocol	1	integer, 1-2	Protocol to use for device terminal sessions. 1= TELNET 2= SSH.
/GTL/echo-mode	false	The valid values are true and false .	Flag indicating whether to run GTL in ECHO mode or DCS mode.
/GTL/ios/			IOS related GTL properties.
copy-running-to-startup	true	The valid values are true and false .	Flag indicating whether to copy running config to startup config when downloading configlets. Write Mem flag.

Table B-1 DCPL Properties (continued)

/GTL/logLevel	CONFIG	selection	The log Level is the level at which logging is done for this component. These levels are identical to the logging levels defined for JDK1.4 logging package. The levels in descending order are: SEVERE (highest value) WARNING INFO CONFIG FINE FINER FINEST (lowest value).
/GTL/pix/			PIX related properties.
copy-running-to-startup	true	The valid values are true and false .	Flag indicating whether to copy running config to startup config when downloading configlets. Write Mem flag.
GUI Properties:			The component for GUI-based properties.
/GUI/Common/			Generic GUI component. Use it if you do not have any specific component requirements, such as security or L2VPN.
logLevel	FINE	selection	The log Level is the level at which logging is done for this component. These levels are identical to the logging levels defined for JDK1.4 logging package. The levels in descending order are: SEVERE (highest value) WARNING INFO CONFIG FINE FINER FINEST (lowest value).
/GUI/L2VPN/			L2VPN related GUI component. Use it with L2VPN related operations only.
logLevel	SEVERE	selection	The log Level is the level at which logging is done for this component. These levels are identical to the logging levels defined for JDK1.4 logging package. The levels in descending order are: SEVERE (highest value) WARNING INFO CONFIG FINE FINER FINEST (lowest value).
/GUI/MplsVPN/			MPLS VPN related GUI component. Use it with MPLS VPN related operations only.
logLevel	SEVERE	selection	The log Level is the level at which logging is done for this component. These levels are identical to the logging levels defined for JDK1.4 logging package. The levels in descending order are: SEVERE (highest value) WARNING INFO CONFIG FINE FINER FINEST (lowest value).

Table B-1 DCPL Properties (continued)

/GUI/Performance/			For monitoring GUI performance.
logLevel	INFO	selection	The log Level is the level at which logging is done for this component. These levels are identical to the logging levels defined for JDK1.4 logging package. The levels in descending order are: SEVERE (highest value) WARNING INFO CONFIG FINE FINER FINEST (lowest value).
GUI/Ping			Ping related GUI component. Use it with Ping related operations only.
logLevel	CONFIG	selection	The log Level is the level at which logging is done for this component. These levels are identical to the logging levels defined for JDK1.4 logging package. The levels in descending order are: SEVERE (highest value) WARNING INFO CONFIG FINE FINER FINEST (lowest value).
/GUI/QoS/			QoS related GUI component. Use it with QoS related operations only.
logLevel	SEVERE	selection	The log Level is the level at which logging is done for this component. These levels are identical to the logging levels defined for JDK1.4 logging package. The levels in descending order are: SEVERE (highest value) WARNING INFO CONFIG FINE FINER FINEST (lowest value).
sendAuditEvent	true	The valid values are true and false .	Set true to enable sending audit event for this service.
/GUI/Security/			Security related component. This is to be used for security purposes only.
logLevel	CONFIG	selection	The log Level is the level at which logging is done for this component. These levels are identical to the logging levels defined for JDK1.4 logging package. The levels in descending order are: SEVERE (highest value) WARNING INFO CONFIG FINE FINER FINEST (lowest value).
/GUI/Topology/			Component related to the web start topology application.

Table B-1 DCPL Properties (continued)

logLevel	CONFIG	selection	The log Level is the level at which logging is done for this component. These levels are identical to the logging levels defined for JDK1.4 logging package. The levels in descending order are: SEVERE (highest value) WARNING INFO CONFIG FINE FINER FINEST (lowest value).
/GUI/VPLS/			VPLS related GUI component. Use it with VPLS related operations only.
logLevel	SEVERE	selection	The log Level is the level at which logging is done for this component. These levels are identical to the logging levels defined for JDK1.4 logging package. The levels in descending order are: SEVERE (highest value) WARNING INFO CONFIG FINE FINER FINEST (lowest value).
/GUI/srRefreshRate	30000	integer	The refresh rate (in milliseconds) for the SR List screen.
/GUI/workflowSteps	<vpnsc_home>/etc/workflowSteps.csv	string	The pre-defined workflow steps.
/GUI/workflows	<vpnsc_home>/etc/workflows.csv	string	The pre-defined workflows.
JavaWebStart Properties			Java Web Start components.
/JavaWebStart/InventoryManager/			Component to create and manage Devices.
MaxDevicesPerSaveTransaction		integer, 1-500	Specifies the maximum number of devices per transaction when performing save operation.
/JavaWebStart/TaskManager/			Component to create and monitor scheduled tasks.
MaxDevicesPerCollectionTask		integer, 1-500	Specifies the maximum number of devices per Collect Config task. More devices can be specified for a single task and they will be managed as such from a user perspective. However, there may be more than one Collect Config task created and executed in the repository.
Logging Properties:			This contains different properties needed by the logging framework. There are a set of default values for logging parameters. These values can be overridden for a specific server.

Table B-1 DCPL Properties (continued)

/Logging/Defaults/			This contains the default values for the logging framework.
logFileNumber	2	integer, 1-10	Maximum number of log files for a process. Each of these files can be of size logFileSize . When the maximum number for log files is reached for a process, the log files are rotated by deleting the oldest log file for that process.
logFileSize	2000000	integer, 1000000-10000000 bytes	Size in bytes of a single log file for a process. Each process will have a number of log files (see logFileNumber property), where each of these files can grow to this size.
logFormatter	java.util.logging.XMLFormatter	string	Class name for the default formatter of log records.
logLevel	CONFIG	selection	NOTE: This log Level is used only if there is no log Level defined for a component. The log Level is the level at which logging is done for this component. These levels are identical to the logging levels defined for JDK1.4 logging package. The levels in descending order are: SEVERE (highest value) WARNING INFO CONFIG FINE FINER FINEST (lowest value).
logLocation	<vpnsc_tmp>	string	The directory name where log files are kept.
/Logging/TaskLogs/			This contains logging properties for task logs.
logLocation	<vpnsc_tmp>/TaskLogs	string	The directory name where all the task logs are kept.
Provisioning Properties:			Contains properties and components for service provisioning like MPLS and IPsec (IPsec is NOT SUPPORTED in this release.) VPNs.
/Provisioning/Engine/			Contains properties for the XML driven provisioning engine.
logLevel	CONFIG	selection	The log Level is the level at which logging is done for this component. These levels are identical to the logging levels defined for JDK1.4 logging package. The levels in descending order are: SEVERE (highest value) WARNING INFO CONFIG FINE FINER FINEST (lowest value).
serviceSchema	service.xsd	string	Specifies the XML schema definition file for defining new services.

Table B-1 DCPL Properties (continued)

/Provisioning/NOM/			Network Object Model for parsing and delta generation of configs.
DocumentBuilderFactory/			This contains the properties for the DOM builder factory.
ignoreComments	true	The valid values are true and false .	Flag.
ignoreWhiteSpace	false	The valid values are true and false .	Flag for DOM builder factory.
validation	false	The valid values are true and false .	Flag for validation of xml files.
catSyntaxFile	catSyntax.xml	string	Contains the XML for Catalyst command syntax.
iosSyntaxFile	iosSyntax.xml	string	Contains the xml syntax for IOS command.
logLevel	CONFIG	selection	The log Level is the level at which logging is done for this component. These levels are identical to the logging levels defined for JDK1.4 logging package. The levels in descending order are: SEVERE (highest value) WARNING INFO CONFIG FINE FINER FINEST (lowest value).
/Provisioning/PasswordManagement/			User generated Password generation
PasswordFormula/			User generated Password formula generation class
class		string	User generated class file
/Provisioning/ProvDrv/			Contains properties for the XML driven provisioning ProvDrv.
AuditJITUpload	true	The valid values are true and false .	If the value of this property is set to false , the provisioning server does NOT upload a copy of the configuration file from the routers when it processes the Service Request for auditing purpose. Instead, it uses copies of the configuration files that were collected and stored in the Repository earlier. If the value of this property is set to true , the provisioning server uploads a copy of the configuration file from the routers when it processes the Service Request for auditing purpose. The default value of this property is true .

Table B-1 DCPL Properties (continued)

CleanStagedConfigletWhenForceDeploy	false	The valid values are true and false .	If this value is true , when a service request is force deployed, the staged configlet is removed before provisioning. If this value is the default of false , the staged configlet is considered as part of the base configuration during provisioning.
DownloadTemplateToUnmanagedDevice	false	The valid values are true and false .	If this value is true , for an unmanaged device, ISC attempts to download just the template. The configlet generated by the provision is not part of the download. By default, this value is false and then there is no attempt to download to an unmanaged device.
MaxNumberOfDevicesPerDownload	2	integer	ISC will try to bundle as much devices as possible during a download attempt. This value set the max number of devices allowed during such an attempt. If the number of devices exceeds this limit, multiple download attempts will take place. You should decrease this limit if the download involves many devices with huge configlets in order to conserve memory usage.
ProvisionJITUpload	true	The valid values are true and false .	If the value of this property is set to false , the provisioning server does NOT upload a copy of the configuration file from the routers when it processes the Service Request for provisioning purpose. Instead, it uses copies of the configuration files that were collected and stored in the Repository earlier. If the value of this property is set to true , the provisioning server uploads a copy of the configuration file from the routers when it processes the Service Request for provisioning purpose. The default value of this property is true .
SaveConfigletsFromAllSRs	true	The valid values are true and false .	If the value of this property is set to true, for each device in a SR, the provisioning server will save the configlet contributed from all SRs that are processed in the same provisioning run. If the value is set to false, only the configlet contributed by the current SR is saved for this device in this SR even though this same device may be in multiple SRs that are processed by the same provisioning run. The default value of this property is true .

Table B-1 DCPL Properties (continued)

logLevel	CONFIG	selection	The log Level is the level at which logging is done for this component. These levels are identical to the logging levels defined for JDK1.4 logging package. The levels in descending order are: SEVERE (highest value) WARNING INFO CONFIG FINE FINER FINEST (lowest value).
/Provisioning/Service/			Contains different services and their properties.
Firewall/(Firewall is NOT SUPPORTED in this release.)			Firewall provision related properties.(Firewall is NOT SUPPORTED in this release.)
platform/			ProvDrv service blade mapping.
CISCO_ROUTER/			IOS.
serviceBladeClass	com.cisco.vpnsc. prov.firewall.FW ServiceBlade	string	Service blade class name.
PIX/			PIX firewall.
object_group	true	The valid values are true and false .	whether try to generate object group if platform supports
serviceBladeClass	com.cisco.vpnsc. prov.firewall.FW ServiceBlade	string	Class name.
logLevel	CONFIG	selection	Log level for firewall services.
maxDMZ	5	integer	The maximum dmz value supported. GUI will use this to generate a drop down list for dmz.
sendAuditEvent	true	The valid values are true and false .	Set true to enable sending audit event for this service.
IPSEC/(IPsec is NOT SUPPORTED in this release.)			IPsec Site-to-Site Provisioning.(IPsec is NOT SUPPORTED in this release.)
logLevel	CONFIG	selection	The log Level is the level at which logging is done for this component. These levels are identical to the logging levels defined for JDK1.4 logging package. The levels in descending order are: SEVERE (highest value) WARNING INFO CONFIG FINE FINER FINEST (lowest value).
platform/			IPsec site-to-site supported platforms.
CISCO_ROUTER/			IOS.

Table B-1 DCPL Properties (continued)

generateCryptoLocalIdentity	true	The valid values are true and false .	If enabled the crypto local identity will be generated for the ipsec service.
generateNoXAuth	true	The valid values are true and false .	If enabled will bypass the XAuth authentication for site-to-site remote peers.
iosPresharedKeyLength	127	integer, 1-127	Defines the length of Preshared Keys generated for IOS devices.
serviceBladeClass	com.cisco.vpnsc. prov.ipsec. lan2lan.IPSecIos ServiceBlade	string	IOS IPsec Service Blade Location.
PIX/			PIX.
generateNoXAuth	true	The valid values are true and false .	If enabled will bypass the XAuth for the site-to-site remote peers.
pixPresharedKeyLength	127	integer, 1-127	Defines the length of Preshared Keys generated for PIX devices.
serviceBladeClass	com.cisco.vpnsc. prov.ipsec. lan2lan.IPSecPix ServiceBlade	string	PIX IPsec service blade location.
VPN3000/			Cisco 3000 Route.
serviceBladeClass	com.cisco.vpnsc. prov.ipsec.vpn3k. IPSec3KService Blade	string	IPSEC L2L Service Blade Class Location.
vpn3000PresharedKeyLength	32	integer, 1-32	Defines the length of Preshared Keys generated for VPN 3000 devices.
removeStaleCommands	false	The valid values are true and false .	Set true to remove the stale commands provisioned by VPN3000 2.x.
sendAuditEvent	true	The valid values are true and false .	Set true to enable sending audit event for this service.
IPSEC_RA/ (IPsec is NOT SUPPORTED in this release.)			IPSEC Remote Access Provisioning.
platform/			Platforms supported by IPSEC remote access provisioning.
CAT6K/			Catalyst 6000 VPN3000.
serviceBladeClass	com.cisco.vpnsc. prov.ipsec.ra. framework. RaServiceBlade	string	IPSEC RA Service Blade Class Location.

Table B-1 DCPL Properties (continued)

CISCO_ROUTER/			Cisco IOS Router.
serviceBladeClass	com.cisco.vpnsc. prov.ipsec.ra. framework. RaServiceBlade	string	IPSEC RA Service Blade Class Location.
PIX/			Cisco PIX Firewall.
serviceBladeClass	com.cisco.vpnsc. prov.ipsec. ra.framework. RaServiceBlade	string	IPSEC RA Service Blade Class Location
VPN3000/			Cisco 3000 Router.
serviceBladeClass	com.cisco.vpnsc. prov.ipsec.vpn3k. IPSec3KService Blade	string	IPSEC RA Service Blade Class Location.
logCount	3	integer, 1-32	Set the number of the log files for a provisioned device.
logLevel	CONFIG	selection	The log Level is the level at which logging is done for this component. These levels are identical to the logging levels defined for JDK1.4 logging package. The levels in descending order are: SEVERE (highest value) WARNING INFO CONFIG FINE FINER FINEST (lowest value).
sendAuditEvent	true	The valid values are true and false .	Set true to enable sending audit event for this service.
NAT/ (NAT is NOT SUPPORTED in this release.)			NAT provision related properties. (NAT is NOT SUPPORTED in this release.)
platform/			ProvDrv service blade mapping.
CISCO_ROUTER/			IOS.
serviceBladeClass	com.cisco.vpnsc. prov.nat. NatIosPixService Blade	string	Service blade class name.
PIX/			PIX NAT.
serviceBladeClass	com.cisco.vpnsc. prov.nat. NatIosPixService Blade	string	Class name.

Table B-1 DCPL Properties (continued)

logLevel	CONFIG	selection	The log Level is the level at which logging is done for this component. These levels are identical to the logging levels defined for JDK1.4 logging package. The levels in descending order are: SEVERE (highest value) WARNING INFO CONFIG FINE FINER FINEST (lowest value).
sendAuditEvent	true	The valid values are true and false .	Set true to enable sending audit event for this service.
QoS/			QoS Provisioning Service related properties section.
enableLogging	true	The valid values are true and false .	
managementLanAddress	0.0.0.0/0	string	Management LAN address in the format of a.b.c.d/x. This will become the default value in QoS Policy's TrafficClassification's Mgmt_lan_addr_mask field.
platform/			Used by ProvDrv.
CISCO_ROUTER/			Used by ProvDrv.
serviceBladeClass	com.cisco.vpnsc. prov.qos. ServiceBlade. QosServiceBlade	string	Identifies ServiceBlade class name for ProvDrv.
sendAuditEvent	true	The valid values are true and false .	Set true to enable sending audit event for this service.
TE/			Traffic Engineering Management Provisioning Service related properties section.
enableLogging	true	The valid values are true and false .	When the value is the default of true , detailed delta generation messages are logged. When the value is false , detailed delta generation messages are not logged.
platform/			Used by ProvDrv.
CISCO_ROUTER/			Used by ProvDrv.
serviceBladeClass	com.cisco.vpnsc. prov.te. ServiceBlade. TeServiceBlade	string	Identifies ServiceBlade class name for ProvDrv.

Table B-1 DCPL Properties (continued)

sendAuditEvent	true	The valid values are true and false .	Set true to enable sending audit event for this service.
l2vpn/			MPLS Layer 2 VPN Provisioning.
DownloadWeights/			Specifies the download weights for different devices in an L2VPN service request. The higher the weight, the sooner we download to that device. By default the weights are set to 0, so that all devices get downloaded at the same time during service deployment.
weightForCE	0	integer	Download weight for CE devices.
weightForPE	0	integer	Download weight assigned to PE devices.
weightForPE_CLE	0	integer	download weight for PE_CLE devices.
platform/			Contains properties for L2VPN for different platforms.
CATOS/			Service blade parameters for CATOS.
serviceBladeClass	com.cisco.vpnsc. prov.l2vpn.L2VPNServiceBlade	string	ServiceBladeClass location.
CISCO_ROUTER/			IOS.
serviceBladeClass	com.cisco.vpnsc. prov.l2vpn.L2VPNServiceBlade	string	ServiceBladeClass location.
dataFileSchema	l2vpnData.xsd	string	Layer 2 VPN Data File schema.
logLevel	CONFIG	selection	The log Level is the level at which logging is done for this component. These levels are identical to the logging levels defined for JDK1.4 logging package. The levels in descending order are: SEVERE (highest value) WARNING INFO CONFIG FINE FINER FINEST (lowest value).
parseConfigAfterProvisioning	false	The valid values are true and false .	This property controls the parsing of the configuration file after the provisioning is completed in order to make sure that device inventory is in sync with network.
saveDebugData	true	The valid values are true and false .	If this property is set to true , whenever an SR is provisioned, the uploaded config files and input XML data are saved to a temporary directory for debugging purposes.
sendAuditEvent	true	The valid values are true and false .	Set true to enable sending audit event for this service.

Table B-1 DCPL Properties (continued)

serviceFile	l2vpnService.xml	string	Layer 2 VPN Service definition file.
logLevel/	SEVERE	selection	The log Level is the level at which logging is done for this component. These levels are identical to the logging levels defined for JDK1.4 logging package. The levels in descending order are: SEVERE (highest value) WARNING INFO CONFIG FINE FINER FINEST (lowest value).
mpls/			Contains properties for MPLS/BGP Layer 3 VPN service.
DownloadWeights/			Specifies the download weights for different devices in an MPLS-VPN service request. The higher the weight, the sooner we download to that device. By default the weights are set to 0, so that all devices get downloaded at the same time during service deployment.
weightForCE	0	integer	Download weight for CE devices.
weightForMVRFC	0	integer	Download weight for MVRFC. The higher the weight the sooner we download to this device while deploying a service request.
weightForPE	0	integer	Download weight assigned to PE devices.
weightForPE_CLE	0	integer	Download weight for PE_CLE devices.
platform/			Platform related classes.
CATOS/			Service blade parameters for CATOS.
serviceBladeClass	com.cisco.vpnsc. prov.mpls.MplsS erviceBlade	string	ServiceBladeClass location.
CISCO_ROUTER			IOS.
serviceBladeClass	com.cisco.vpnsc. prov.mpls.MplsS erviceBlade	string	ServiceBladeClass location
allowOverwriteManualAssigned Address	false	The valid values are true and false .	Allow manually-assigned IP address in Service Request overwrite the pre-existing interface IP address. False means if an MPLS service request tries to provision a manually-assigned IP address to an interface that already has a different IP address on it, ISC detects that and reports the error. True means ISC allows the new IP address to overwrite the existing IP address.

Table B-1 DCPL Properties (continued)

auditIpAddressViaUnnumbered	false	The valid values are true and false .	When the value is the default of false , the auditor only looks for the IP address of a provisioned interface. When the value is true , the auditor tries to match the IP address of the unnumbered interface, if one exists.
auditMaxrouteThreshold	true	The valid values are true and false .	When the value is the default of true ,
dataFileSchema	l3vpnData.xsd	string	Specifies the schema for the data XML file for MPLS/BGP layer3 VPNs.
forceRemoveNonBroadcastStaticRouteOnPE	false	The valid values are true and false .	The default value is false . When the value is set to true , ISC removes the non-broadcast type static route command that has a pre-existing long syntax, even if the command was not provisioned by ISC. The non-broadcast type static route command is removed from a PE router prior to provisioning. Long syntax contains both an outgoing interface name and a next hop IP address.
logLevel	CONFIG	selection	The log Level is the level at which logging is done for this component. These levels are identical to the logging levels defined for JDK1.4 logging package. The levels in descending order are: SEVERE (highest value) WARNING INFO CONFIG FINE FINER FINEST (lowest value).
parseConfigAfterProvisioning	false	The valid values are true and false .	This property controls the parsing of the configuration file after the provisioning is completed in order to make sure that device inventory is in sync with network.
reapplyIpAddress	false	The valid values are true and false .	Re-apply the same IP address to the interface when decommission a service request. This option is only applicable to manually-assigned IP addresses. It does not work for automatically-assigned IP addresses. When this property is in effect, the interface negate command will not be generated.
removeSubInterface	true	The valid values are true and false .	Removing the ISC generated subinterface commands in decommission service requests.

Table B-1 DCPL Properties (continued)

saveDebugData	true	The valid values are true and false .	If this property is set to true , whenever an SR is provisioned, the uploaded config files and input XML data are saved to a temporary directory for debugging purposes.
sendAuditEvent	true	The valid values are true and false .	Set true to enable sending audit event for this service.
serviceFile	l3vpnService.xml	string	Specifies the XML file containing the service definition for MPLS/BGP layer3 VPNs. The schema for this file is specified by Provisioning.Engine.serviceSchema
skipAddressValidationOnUnmanaged CE	false	The valid values are true and false .	When the value is false , the IP addresses between a PE and an unmanaged CE are validated to ensure they are in the same subnetwork and valid host addresses. When the value is true , this validation is by-passed.
useNextHopAddressForStaticRoutes	false	The valid values are true and false .	For Static Routes, use local router outbound interface or IP address of the next hop to reach the destination network.
useOnlyExtraCEloopbackForGrey AccessList	false	The valid values are true and false .	With Extra CE loopback, the user can select this option to add only the loopback address instead of the interface ip address and extra CE loopback.
shared/			Properties shared by MPLS VPN, L2VPN and VPLS.
FeatureQuery/			ISC components that check if certain features are available for certain devices based on their software version and platform information.
enableValidation	true	The valid values are true and false .	If enabled, FeatureQuery will check if the features are available based on the feature matrix and device OS version (IOS Version or PIX Version). If disable it will assume that all features are available on all platforms (should be used for testing only).
actionTakenOnUNIVlanList	prune	string	Action taken when switch port allowed vlan cmd is absent for ERS service.

Table B-1 DCPL Properties (continued)

overwriteInterfaceDescription	true	The valid values are true and false .	By default, ISC generates a description subcommand for all the physical interfaces it provisioned. Set this property to false if this behavior is not desirable. This property does not apply to logical interfaces or other CLI objects that have a description subcommand (Ex. crypto map entries, gre Interfaces, etc.)
transferUNIDescToVlanName	false	The valid values are true and false .	Controls provisioning of the VLAN name on the PE-POP. If set to true , the VLAN name is assigned from the description for the UNI. If set to the default of false , no VLAN name is assigned.
vpls/			Contains properties for Virtual Private LAN Service.
DownloadWeights/			Specifies the download weights for different devices in an MPLS VPN service request. The higher the weight, the sooner we download to that device. By default the weights are set to 0, so that all devices get downloaded at the same time during service deployment.
weightForCE	0	integer	Download weight for CE devices.
weightForPE	0	integer	Download weight assigned to PE devices.
weightForPE_CLE	0	integer	Download weight for PE_CLE devices.
dataFileSchema	vplsData.xsd	string	Specifies the schema for the data XML file for VPLS.
logLevel	CONFIG	selection	The log Level is the level at which logging is done for this component. These levels are identical to the logging levels defined for JDK1.4 logging package. The levels in descending order are: SEVERE (highest value) WARNING INFO CONFIG FINE FINER FINEST (lowest value).
parseConfigAfterProvisioning	false	The valid values are true and false .	This property controls the parsing of the configuration file after the provisioning is completed to make sure that device inventory is in sync with network.
platform/			Platform related classes.
CATOS/			Service blade parameters for CATOS.
serviceBladeClass	com.cisco.vpnsc. prov.vpls. VplsService Blade	string	ServiceBladeClass location.
CISCO_ROUTER/			IOS.

Table B-1 DCPL Properties (continued)

serviceBladeClass	com.cisco.vpnsc. prov.vpls. VplsService Blade	string	ServiceBladeClass location.
saveDebugData	true	The valid values are true and false .	If this property is set to true , whenever an SR is provisioned, the uploaded config files and input XML data are saved to a temporary directory for debugging purposes.
sendAuditEvent	true	The valid values are true and false .	Set true to enable sending audit event for this service.
serviceFile	vplsService.xml	string	Specifies the XML file containing the service definition for VPLS. The schema for this file is specified by Provisioning.Engine.serviceSchema.
SLA Properties:			Service Level Agreement. This component deals with creating SAA probes between different devices and to collect/aggregate the data corresponding to those probes, in order to provide different SLA reports.
/SLA/copyRunningToStartup	true	The valid values are true and false .	If true and if showInRunningConfig is true - the running configuration will be copied to startup after the router SA Agent configuration has been changed.
/SLA/daysToKeepDailyStats	365	integer, 30-3650 days	Specifies how many days should the SLA database keep the daily statistics. Specifying a low number keeps the database small but you will not be able to access daily reports beyond this period.
/SLA/daysToKeepHourlyStats	60	integer, 7-1000 days	Specifies how many days should the SLA database keep the hourly statistics. Specifying a low number keeps the database small but you will not be able to access hourly reports beyond this period.
/SLA/logLevel	CONFIG	selection	The log Level is the level at which logging is done for this component. These levels are identical to the logging levels defined for JDK1.4 logging package. The levels in descending order are: SEVERE (highest value) WARNING INFO CONFIG FINE FINER FINEST (lowest value).
/SLA/rowAgeOut	3600	integer, 0-2073600 seconds	The time after which a probe is completely removed after its life is over. In seconds.

Table B-1 DCPL Properties (continued)

/SLA/showInRunningConfig	true	The valid values are true and false .	If true, the configured SLAs appear in the router's running configuration.
SYSTEM Properties:			The properties common to all sub-systems in ISC can be found under this component. Most of the values here are set at the time of installation.
/SYSTEM/app_dir	<vpnsc_home>	string	Location of the ISC installation.
/SYSTEM/databaseServer	<db_server>	string	The database server fully qualified name.
/SYSTEM/email/			Properties related to e-mails sent out by ISC.
from	<mailfrom>	string	The from field in the e-mail header of the mails sent out by ISC.
smtpHost	<mailhost>	string	The server using which e-mail messages from ISC should be sent out.
/SYSTEM/fullyManaged/			Properties related to e-mails sent out by ISC in case of fully managed devices.
enforcementAuditScript		string	Script to be invoked when failure of enforcement audit is detected.
externalEventsEmailRecipients	<mailto>	string	The comma or space separated list of email addresses to which notification should be sent out when receiving a config-change event originated outside ISC.
/SYSTEM/license/			Properties related to ISC Licensing.
emailRecipients	<mailto>	string	The comma separated list of e-mail addresses to which the License Threshold e-mails should be sent out.
refreshInterval	1	integer, 1-24 hours	License refresh interval in hours.
threshold	90	integer, 1-100%	VPN and ACTIVATION Threshold in percent for e-mail notification.
/SYSTEM/masterServer	<master_server>	string	The master server fully qualified name.
/SYSTEM/maxTaskLimit	500	integer	maxTaskLimit.
/SYSTEM/role	master	string	Identifies the role in the distribution system. Possible values are: master ps (processing server) cs (collection server) is (interface server).
/SYSTEM/tibco/			TIBCO related properties.
port	<tibco_port>	integer	The port on which TIBCO Rendezvous listens for events.
prefix	cisco.vpnsc.	string	Prefix for all TIBCO messages originating from ISC.

Table B-1 DCPL Properties (continued)

rva-http-port	<rva_http_port>	integer	The http port for TIBCO Rendezvous agent web interface.
rva-port	<rva_port>	integer	The port on which TIBCO Rendezvous agent listens for events.
/SYSTEM/tmpdir	<vpnsc_tmp>	string	Location for temporary files.
Scheduler Properties:			Scheduler reads the task repository and schedules tasks on every minute boundary. Each scheduled task is passed to Task manager for execution.
/Scheduler/logLevel	CONFIG	selection	The log Level indicates the level at which logging is done for this component. These levels are identical to the logging levels defined for JDK1.4 logging package. The levels in descending order are: SEVERE (highest value) WARNING INFO CONFIG FINE FINER FINEST (lowest value).
/Scheduler/syncInterval	5	integer, 0-10 minutes	When scheduler starts up for the first time, it reads all the scheduling information from the task repository. After that, it depends on the events generated by task repository for receiving changes to the scheduling information. It can also periodically synchronize with the task repository by re-reading it at regular intervals. This property specifies, in minutes, that interval. If the value for the interval is 0, scheduler will not synchronize with the task repository and only depends on the events.
SnmpService Properties:			The Snmp Service package provides APIs to perform SNMP get() and set() operations.
/SnmpService/defaultSNMPVersion	1	integer, 1-2	The default SNMP version used to connect to Cisco router. Used if the SNMP version is not specified per router. Valid Values: SNMPv1/SNMPv2c - 1 SNMPv3 - 2.
/SnmpService/defaultSecurityLevel	3	integer, 1-3	The default security level used to connect to Cisco router. Used if the security level is not specified per router. Values: authentication no encryption - 1 authentication encryption - 2 no authentication no encryption - 3.

Table B-1 DCPL Properties (continued)

/SnmpService/logLevel	CONFIG	selection	The log Level is the level at which logging is done for this component. These levels are identical to the logging levels defined for JDK1.4 logging package. The levels in descending order are: SEVERE (highest value) WARNING INFO CONFIG FINE FINER FINEST (lowest value).
/SnmpService/retries	3	integer, 0-10	The number of retries to be used by the SNMP protocol.
/SnmpService/timeout	5	integer, 0-300 seconds	Timeout value to be used by the SNMP protocol. Unit: seconds
TE Properties:			
/TE/Deployment			Traffic Engineering Management (TEM) Properties
maxCacheSize	60	integer, >0	Maximum cache size.
oneDeviceEachTimeThreshold	500	integer, >0	When the total number of tunnels to be provisioned exceeds this threshold number, provision one device at a time.
partialConfigAudit	false	The valid values are true and false .	When the value is the default of false , the config audit is not limited. When the value is set to true , only a partial config audit (audit of only the PENDING tunnels) occurs for primary and backup tunnel deployment.
/TE/repository			TEM Repository-related Properties
checkPermissionEnabled	false	The valid values are true and false .	This property enables or disables Role-Based Access Control (RBAC) checking during particular TEM operations, such as topology population, discovery, and service deployment. When the value is the default of false , RBAC permission checking is not enabled. When the values is set to true , RBAC permission checking is enabled and performance degrades.
TE Topology Properties:			
/TE Topology/TrafficData			Color Control for Traffic Data Displays
Green	0-25	integer, 0-100 (percentage)	Topology representations for a link performance utilization range, specified as a percentage (default: 0-25), are displayed in the color green.

Table B-1 DCPL Properties (continued)

Orange	26-50	integer, 0-100 (percentage)	Topology representations for a link performance utilization range, specified as a percentage (default: 26-50), are displayed in the color orange.
Red	51-75	integer, 0-100 (percentage)	Topology representations for a link performance utilization range, specified as a percentage (default: 51-75), are displayed in the color red.
Yellow	76-100	integer, 0-100 (percentage)	Topology representations for a link performance utilization range, specified as a percentage (default: 76-100), are displayed in the color yellow.
TaskManager Properties:			Task manager executes tasks that are scheduled by scheduler. Task execution consists of executing different actions that comprise the task. Task manager manages the dependencies between these actions.
/TaskManager/logLevel	CONFIG	selection	The log Level indicates the level at which logging is done for this component. These levels are identical to the logging levels defined for JDK1.4 logging package. The levels in descending order are: SEVERE (highest value) WARNING INFO CONFIG FINE FINER FINEST (lowest value).
VpnInvServer Properties:			Corba Server for VpnInvServer IDL backward compatibility.
/VpnInvServer/logLevel	SEVERE	selection	The log Level is the level at which logging is done for this component. These levels are identical to the logging levels defined for JDK1.4 logging package. The levels in descending order are: SEVERE (highest value) WARNING INFO CONFIG FINE FINER FINEST (lowest value).
aagent Properties:			AAgent component related defines.
/aagent/defaultVersion	3.6.3	string	The default 3k firmware version for AAgent.
/aagent/directories/			Various directories for aagent.
dmd	<vpnsc_home>/resources/AAgent/DMDFiles	string	File path and name.

Table B-1 DCPL Properties (continued)

input	<vpnsc_home>/resources/java/classes/common/AAgent/com/cisco/vpn3000/vpnscagent (VPN 3000 is NOT SUPPORTED in this release.)	string	File path and name.
working	<vpnsc_home>/resources/java/archives	string	File path and name.
dtd Properties:			The component for XML-based properties.
/dtd/ipsec12l/			Path to the ipsec 12l dtd.
filepath	<vpnsc_home>/resources/dtd/servicemodel/Lan2LanSm.dtd	string	DTD file path and name.
/dtd/ipsecra/			Path to the ipsec 12l dtd.
filepath	<vpnsc_home>/resources/dtd/servicemodel/RaSm.dtd	string	DTD file path and name.
lockmanager Properties:			Component that handles device locking. When different jobs (such as provisioning) try to update the config on the device, they obtain software locks so that two different jobs do not update the config at the same time. LockManager provides a way to obtain and later release such software locks.
/lockmanager/lockTimeoutInHours	8	integer, 1-168 hours	Timeout in hours for a lock held by a lock holder. If the lock holder does not free a lock within this time the lockmanager will automatically release the device lock.
/lockmanager/logLevel	SEVERE	selection	The log Level is the level at which logging is done for this component. These levels are identical to the logging levels defined for JDK1.4 logging package. The levels in descending order are: SEVERE (highest value) WARNING INFO CONFIG FINE FINER FINEST (lowest value).

Table B-1 DCPL Properties (continued)

nbi Properties:			Northbound API (Nbi) component related defines.
/nbi/BackwardCompatible			Path for execQuery requests.
RecordNumber	false	The valid values are true and false .	For execQuery requests, the number embedded in the output class name include Record for the default, false , or Record#1 for true .
/nbi/CompositeDir	<vpnsd_home>/resources/java/xml/com/cisco/vpnsd/repository/meta/xml/composite	string	Path to composite XML files. Do not change it or the composite meta XML files will not be backed up.
/nbi/CustomerReportMetaDir	<vpnsd_home>/resources/java/xml/com/cisco/vpnsd/repository/meta/xml	string	Path to user defined report meta XML files. Do not change it or the report meta XML files will not be backed up.
/nbi/Formatter	com.cisco.vpnsd.nbi.io.NbiSimpleFormatter	string	File path and name.
/nbi/Logger	com.cisco.vpnsd.nbi.util.NbiVpnsdLogger	string	File path and name.
/nbi/MetaCheckInterval	300000	string	Set the time for next meta check to happen.
/nbi/MetaDir	<vpnsd_home>/resources/java/xml/com/cisco/vpnsd/repository/meta/xml	string	Path to meta XML files. Do not change it or the meta XML will not be backed up.
/nbi/ProvidedReportMetaDir	<vpnsd_home>/resources/java/xml/com/cisco/vpnsd/repository/meta/xml	string	Path to ISC provided report meta XML files. Do not change it or the report meta xml files will not be backed up.
/nbi/Reader	com.cisco.vpnsd.nbi.io.NbiSoapReader	string	File path and name.
/nbi/RequestParserMgr	com.cisco.vpnsd.nbi.parser.NbiRequestParserMgr	string	File path and name.
/nbi/SSLfilepath	<vpnsd_home>/bin/client.keystore	string	Path to client.keystore file for NBI SSL connections.
/nbi/SessionTimeout	1200000	string	Amount of time the session is valid.

Table B-1 DCPL Properties (continued)

/nbi/TransactionParser	com.cisco.vpnsc.nbi.parser.NbiWsdlParser	string	File path and name.
/nbi/Validation	true	The valid values are true and false .	Variable to enable validation of incoming Nbi API XML attributes.
/nbi/Writer/			
SoapEncapsulation	false	The valid values are true and false .	SoapEncapsulation.
/nbi/Writer	com.cisco.vpnsc.nbi.io.NbiSoapWriter	string	File path and name.
/nbi/logHandler	com.cisco.vpnsc.nbi.util.VpnscLogHandler	string	Custom log handler for nbi. This handler allows NBI to use alternate formatter from default one used by rest of ISC. In this case, NBI defaults to using SimpleFormatter which dumps simple output as opposed to XML output.
/nbi/logLevel	WARNING	selection	The log Level is the level at which logging is done for this component. These levels are identical to the logging levels defined for JDK1.4 logging pack age. The levels in descending order are: SEVERE (highest value) WARNING INFO CONFIG FINE FINER FINEST (lowest value).
notification Properties:			Event notification related defines.
/notification/Logger	com.cisco.vpnsc.nbi.util.NbiVpnscLogger	string	File path and name.
/notification/clientEnabled	false	The valid values are true and false .	Set to true for enabling the example event receiving servlet.
/notification/clientHost	<master_server>	string	TIBCO event client host.
/notification/clientMethod	/notification/servlet/eventListener	string	TIBCO event client method.
/notification/clientPort	<http_port>	string	TIBCO event client port.
/notification/clientRegFile	<vpnsc_home>/resources/nbi/notification/clientReg.txt	string	Client TIBCO event registration file name.
/notification/logFormatter	java.util.logging.SimpleFormatter	string	File path and name.

Table B-1 DCPL Properties (continued)

/notification/logHandler	com.cisco.vpnsc.nbi.util.VpnscLogHandler	string	Custom log handler.
/notification/logLevel	WARNING	selection	The log Level is the level at which logging is done for this component. These levels are identical to the logging levels defined for JDK1.4 logging package. The levels in descending order are: SEVERE (highest value) WARNING INFO CONFIG FINE FINER FINEST (lowest value).
/notification/password	cisco	string	Both user name and password are same as the ones used for GUI login.
/notification/remotePassword		string	User password for remote system authentication, if required, for example, when LDAP is in use.
/notification/remoteUsername		string	User name for remote system authentication, if required, for example, when LDAP is in use.
/notification/username	admin	string	Both user name and password are s same as the ones used for GUI login.
repository Properties:			The component for Database related properties.
/repository/Concurrency/			To setup properties for re-try loop to avoid deadlock
NOICE_FACTOR	500	integer	Add random noise to each process that is being retried.
NO_OF_RETRIES	3	integer	Number of retries before throwing deadlock exception.
TIME_BASE	2	integer	The base number to calculate the wait time. For example, a value of 2 for this property and 3 retries means, the process will be retried every 2^0 , 2^1 , and 2^2 seconds.
/repository/IPAddressPool/			IP Address Pool Constants.
AGE_TIME	1440	integer	The Aging interval for released IP Address, in minutes. The default is 24 hours (1440 minutes).
releaseAndReuseAgedAddresses	true	The valid values are true and false .	The default value is false . When the value is set to true , the address will be released from the Aged Pool and moved to the Allocated pool when manually allocated.
/repository/deviceConfig/		null	Configuration file related properties.

Table B-1 DCPL Properties (continued)

maxVersions	10	integer, 1-50	Maximum number of configuration files to be stored per device in the repository before older versions automatically get purged.
/repository/mlshare/			Share directory for both MPLS and L2VPN.
logLevel	SEVERE	selection	The log Level is the level at which logging is done for this component. These levels are identical to the logging levels defined for JDK1.4 logging package. The levels in descending order are: SEVERE (highest value) WARNING INFO CONFIG FINE FINER FINEST (lowest value).
/repository/persistence/			Properties for database.
Versions	5	integer	The number of maximum versions for a Versioning Persistent Objects.
catalog	directory	string	Catalog.
driver	<db_driver>	string	The class name for the driver.
initialConnections	1	integer, 1-20	Number of initial connections.
location	<repository_home>	string	The directory containing the repository.db and repository.log files.
password	sql	string	Password for opening a DB connection.
schema	DBA	string	Schema.
slaur	jdbc:sybase:Tds:<local_db_server>:<db_port_sla>/?JCONNECT_VERSION=5&serviceName=sla	string	The url for opening a JDBC connection to the SLA database.
url	<db_url>	string	The url for opening a JDBC connection.
username	dba	string	User id to open a db connection.
/repository/rbac/			The component for RBAC User Access Model, user Authentication.
checkCreatorPermissionEnabled	true	The valid values are true and false .	The creator of objects can give the permissions of Modify or Delete to others. If this flag is false, enable RBAC permission checkin.
checkPermissionEnabled	true	The valid values are true and false .	The creator of objects can give the permissions of Modify or Delete to others. If this flag is false, enable RBAC permission checkin.

Table B-1 DCPL Properties (continued)

enableAutologin	true	The valid values are true and false .	The property controls whether user may store login information in form of cookies on the computer from which the user connects. If enabled, automatic login, based on the cookie information is permitted. Also user is presented with a screen in which he or she can elect to store login information on the local user's computer. With this property set to false no autologin or options associated with it are available.
logLevel	CONFIG	selection	The log Level is the level at which logging is done for this component. These levels are identical to the logging levels defined for JDK1.4 logging package. The levels in descending order are: SEVERE (highest value) WARNING INFO CONFIG FINE FINER FINEST (lowest value).
partialQueryResultExpected	true	The valid values are true and false .	When checking Permission on a list of Persistent Objects, and the current user does not the specified permission to all the objects in the result list, partial results will be returned if this flag is true; Insufficient Permission exception will be generated if the flag is false .
webSessionTimeoutSec	1800	integer	Timeout of inactive web client session in seconds. Default is 30 minutes.
/repository/ual/			User Access/Audit Log
cleanUALogs	true	The valid values are true and false .	whether to let system automatically clean up UAL log entries based on ual.maxAgeInDays.
maxAgeInDays	30	integer	Maximum age of the User Access/Audit Logs in days after which the UALog Cleanup Service will delete them. if 0 then UALogs deletion is disabled even if cleanUALogs is set to true.
watchdog Properties:			All the servers in ISC are launched and managed by the Watchdog.
/watchdog/byRole/			This component contains the watchdog properties that based on the role of the host.
cs/			Watchdog properties for machine playing the role of a cs (Collection Server/Agent).
servers	httpd nspoller worker dbpoller	string	Names of the servers to be run.

Table B-1 DCPL Properties (continued)

db/			Watchdog properties for a machine playing the role of a db (DB server).
servers	dbpoller	string	The servers to be run on a installation with the role db .
is/			Watchdog properties for a machine playing the role of a Interface Server.
servers	httpd dbpoller	string	Names of servers to be run on an installation with role is .
master/			Watchdog properties of a machine playing the role of a master.
servers	httpd nspoller dbpoller dispatcher worker scheduler lockmanager cornerstonebridg e cnsserver	string	The servers to be run.
ps/			Watchdog properties for a machine playing the role of a ps (Processing Server/Agent).
servers	httpd nspoller worker dbpoller	string	Names of servers to be run.
/watchdog/criticalServers		string	If any of these servers enters the disabled state, then it would mean that the system is NOT healthy. If this value is null/empty then every single server is critical.
/watchdog/diskspace/			Contains properties related to disk space monitoring.
dirsToMonitor		string	The directories (and ultimately the disks that contain them) to be monitored.
disksToMonitor		string	The disks to be monitored for space constraints.
emailRecipients	<mailto>	string	The comma separated list of e-mail addresses to which the disk space related e-mails should be sent out.
highWatermark	<highwater>	string	High watermark for the directories (disks) being monitored. The value should be a number followed by a < (for percent) or m or M (for Mbytes). These values should correspond to the available/free space on the disk. If the available disk space stabilizes above this value (after falling below the low watermark), an e-mail is sent to the addresses specified in the property watchdog.diskspace.emailRecipients.

Table B-1 DCPL Properties (continued)

lowWatermark	<lowwater>	string	Low watermark for the directories (disks) being monitored. The value should be a number followed by a % (for percent) or m or M (for Mbytes). These values should correspond to the available/free space on the disk. If the available disk space falls below this value, an e-mail is sent to the addresses specified in the property watchdog.diskspace.emailRecipients.
sleepInterval	60000	integer, 30000-300000 milliseconds	Time between two status checks for disk space limits in milliseconds.
/watchdog/group/			Group.
database_users	scheduler httpd	string	The servers that access database.
/watchdog/groups	database_users	string	The space separated list of different groups in the system.
/watchdog/heartbeat/			Properties related to watchdog heartbeat mechanism are specified here.
period	120000	integer, 30000-86400000 milliseconds	The minimum time between each heartbeat request in milliseconds.
sendEvents	false	The valid values are true and false .	If set to true, watchdog sends out TIBCO events every time a heartbeat succeeds or fails. If set to false, no such events will be sent.
startDelay	5000	integer, 0-60000 milliseconds	Time to wait before making the first heartbeat request in milliseconds.
timeout	3000	integer, 1000-600000 milliseconds	The period of time before which response for heartbeat request should be received by the watchdog, in milliseconds.
wds/			Heartbeat properties for intra-watchdog communication.
delay	5000	integer, 1000-60000 milliseconds	The period in between heartbeats. (from master watchdog to slave watchdog and vice-versa) in milliseconds.
initDelay	1000	integer, 1000-5000 milliseconds	The initial period of time for which the heartbeat thread waits before trying for a heartbeat after a watchdog registers with the MasterWatchdog, in milliseconds.
masterReconnectAttemptDelay	2000	integer, 100-60000 milliseconds	The sleep time between two successive attempts by a slave watchdog to reconnect to master watchdog, in milliseconds.

Table B-1 DCPL Properties (continued)

maxAllowedMisses	3	integer	The maximum number of consecutive misses that a watchdog should miss for the master to consider it inactive or unregistered.
maxAttemptsForMasterReconnect	500	integer	Once the slave watchdog loses connection with the master, it will try this many times to try and establish the connection. If it cannot re-establish a connection with the master even after making these many attempts, it shuts itself down. Between attempts, it sleeps watchdog.heartbeat.wds.masterReconnectAttemptDelay time. The value for this property should be specified in milliseconds. A value of 0 indicates that the slave watchdog has no upper limit on the number of reconnect attempts.
/watchdog/java/			Java.
flags	-XX:+UseAltSigs	string	Any other flags to be passed on to java .
vmtype	-server	string	The flag to be passed on to java (-server or -client).
/watchdog/logLevel	FINEST	selection	The log Level is the level at which logging is done for this component. These levels are identical to the logging levels defined for JDK1.4 logging package. The levels in descending order are: SEVERE (highest value) WARNING INFO CONFIG FINE FINER FINEST (lowest value).
/watchdog/server/	httpd nspoller dbpoller dispatcher worker scheduler lockmanager cornerstonebridge	string	Server.
cnsserver/			Monitors CNS events from IE2100 boxes. Communication between client and server is completely handled using TIBCO events.
heartbeat/			Heartbeat related properties.
startDelay	10000	integer, 0-60000 milliseconds	Time to wait before making the first heartbeat request in milliseconds.

Table B-1 DCPL Properties (continued)

timeout	3000	integer, 1000-600000 milliseconds	The period of time before which response for heartbeat request should be received by the watchdog, in milliseconds.
java/			Java attributes for this server.
flags		string	Any additional java flags specific to this server. If the value is changed, watchdog restart is required for the new value to take effect.
class	com.cisco.vpnsc. watchdog.servers .WDCnsServer	string	Heartbeat Handler - Checks for valid TIBCO Connection.
cmd	java com.cisco.vpnsc. cns.CnsServer	string	Implementation to monitor CNS events from IE2100 boxes.
dependencies	dbpoller	string	Dependencies.
logLevel	CONFIG	selection	The log Level is the level at which logging is done for this component. These levels are identical to the logging levels defined for JDK1.4 logging package. The levels in descending order are: SEVERE (highest value) WARNING INFO CONFIG FINE FINER FINEST (lowest value).
cornerstonebridge/			Acts as a gateway for remote application access to Auto Discovery. Communication between client and server is completely handled using TIBCO events.
class	com.cisco.vpnsc. watchdog.servers .WDCornerstone Bridge	string	Heartbeat Handler - Checks for valid TIBCO Connection.
cmd	java com.cisco.vpnsc. apps.cornerstone. CornerstoneBrid ge	string	Implementation to communicate with Auto Discovery.
dependencies	dbpoller	string	Dependencies.
heartbeat/			Heartbeat related properties.
startDelay	10000	integer, 0-60000 milliseconds	Time to wait before making the first heartbeat request in milliseconds.
timeout	3000	integer, 1000-600000 milliseconds	The period of time before which response for heartbeat request should be received by the watchdog, in milliseconds.
java/			Java attributes for this server.

Table B-1 DCPL Properties (continued)

flags		string	Any additional java flags specific to this server. If the value is changed, watchdog restart is required for the new value to take effect.
logLevel	CONFIG	selection	The log Level is the level at which logging is done for this component. These levels are identical to the logging levels defined for JDK1.4 logging package. The levels in descending order are: SEVERE (highest value) WARNING INFO CONFIG FINE FINER FINEST (lowest value).
dbpoller/			This server keeps polling the database to see if it is functional.
class	com.cisco.vpnsc. watchdog.servers .WDDatabase	string	Name of class responsible for getting heartbeats.
logLevel	CONFIG	selection	The log Level is the level at which logging is done for this component. These levels are identical to the logging levels defined for JDK1.4 logging package. The levels in descending order are: SEVERE (highest value) WARNING INFO CONFIG FINE FINER FINEST (lowest value).
dispatcher/			Dispatcher service of the Distribution framework.
app_args	Dispatcher com.cisco.vpnsc. dist.vpnsc.Vpnsc DispatcherImpl	string	Args to the class that starts this service.
class	com.cisco.vpnsc. watchdog.servers .WDDispatcher	string	The class that proxies this service for the watchdog.
cmd	java com.cisco.vpnsc. watchdog.ext.Ser viceLauncherImp l	string	Command to start the server.
dependencies	dbpoller nspoller	string	The other services that this service depends on Heartbeat related properties.
heartbeat/			
startDelay	45000	integer, 0-60000 milliseconds	Time to wait before making the first heartbeat request in milliseconds.

Table B-1 DCPL Properties (continued)

timeout	3000	integer, 1000-60000 milliseconds	The period of time before which response for heartbeat request should be received by the watchdog, in milliseconds.
java/			Java attributes for this server
flags		string	Any additional java flags specific to this server. If the value is changed, watchdog restart is required for the new value to take effect.
logLevel	CONFIG	selection	The log Level is the level at which logging is done for this component. These levels are identical to the logging levels defined for JDK1.4 logging package. The levels in descending order are: SEVERE (highest value) WARNING INFO CONFIG FINE FINER FINEST (lowest value).
httpd/		httpd	httpd
class	com.cisco.vpnsc. watchdog.servers .WDHttpd	string	Class.
cmd	<vpnsc_home>/ bin/tomcat. sh start fg	string	The command to start httpd on this host.
dependencies	dbpoller	string	Dependencies.
dependenciesByRole/			Dependencies of httpd based on the role of installation (higher priority than normal dependencies)
cs		string	Dependencies on a CS.
ps		string	Dependencies on a PS.
heartbeat/			Heartbeat.
port	<http_port>	integer	The port on which httpd should run.
startDelay	45000	integer, 0-60000 milliseconds	Time to wait before making the first heartbeat request in milliseconds.
timeout	10000	integer, 1000-60000 milliseconds	The period of time before which response for heartbeat request should be received by the watchdog, in milliseconds.
url	http://localhost: <http_port>/isc/ about.htm	string	url

Table B-1 DCPL Properties (continued)

logLevel	CONFIG	selection	The log Level is the level at which logging is done for this component. These levels are identical to the logging levels defined for JDK1.4 logging package. The levels in descending order are: SEVERE (highest value) WARNING INFO CONFIG FINE FINER FINEST (lowest value).
lockmanager/			Component that handles locking.
class	com.cisco.vpnsc. watchdog.servers .WDLockManager	string	Class that keeps track of lockmanager heartbeats.
cmd	java com.cisco.vpnsc. lockmanager.Lock ManagerImpl	string	Command that starts up the lockmanager.
dependencies	nspoller	string	Lock Manager depends on the NS.
heartbeat/			Heartbeat related properties.
startDelay	10000	integer, 0-60000 milliseconds	Time to wait before making the first heartbeat request in milliseconds.
timeout	3000	integer, 1000-600000 seconds	The period of time before which response for heartbeat request should be received by the watchdog, in milliseconds.
java/			Java attributes for this server.
flags		string	Any additional java flags specific to this server. If the value is changed, watchdog restart is required for the new value to take effect.
logLevel	CONFIG	selection	The log Level is the level at which logging is done for this component. These levels are identical to the logging levels defined for JDK1.4 logging package. The levels in descending order are: SEVERE (highest value) WARNING INFO CONFIG FINE FINER FINEST (lowest value).
maxQuickDieCount	3	integer	The maximum number of times a server can die consecutively without having a successful heartbeat. If this number is exceeded, the server is marked as disabled.
nspoller/			This server polls the NameServer to see if it is running.

Table B-1 DCPL Properties (continued)

class	com.cisco.vpnsc. watchdog.servers .WDNameServer	string	Class.
logLevel	CONFIG	selection	The log Level is the level at which logging is done for this component. These levels are identical to the logging levels defined for JDK1.4 logging package. The levels in descending order are: SEVERE (highest value) WARNING INFO CONFIG FINE FINER FINEST (lowest value).
scheduler/			Scheduler.
class	com.cisco.vpnsc. watchdog.servers .WDScheduler	string	Class.
cmd	java com.cisco.vpnsc. scheduler.Schedu ler	string	Command to start the scheduler.
dependencies	dbpoller worker	string	Dependencies.
heartbeat/			Heartbeat related properties.
startDelay	30000	integer, 0-60000 milliseconds	Time to wait before making the first heartbeat request in milliseconds.
timeout	3000	integer, 1000-600000 milliseconds	The period of time before which response for heartbeat request should be received by the watchdog, in milliseconds.
java/			Java attributes for this server.
flags		string	Any additional java flags specific to this server. If the value is changed, watchdog restart is required for the new value to take effect.
logLevel	CONFIG	selection	The log Level is the level at which logging is done for this component. These levels are identical to the logging levels defined for JDK1.4 logging package. The levels in descending order are: SEVERE (highest value) WARNING INFO CONFIG FINE FINER FINEST (lowest value).
startTimeout	240000	integer, 5000-600000	The timeout for the initial heartbeat response. The first heartbeat should happen within this time.
worker/			Worker service of the distribution framework.

Table B-1 DCPL Properties (continued)

app_args	Worker com.cisco.vpnsc. dist.WorkerImpl, com.cisco.vpnsc. sla.sql.SlaMainte nanceService, com.cisco.vpnsc. repository.ual.U ALCleanupServi ceImpl, com.cisco.vpnsc. license.LicenseS ynchronize, com.cisco.vpnsc. cleanup.TaskLog CleanupService, com.cisco.vpnsc. cleanup.TempFil eCleanupService, com.cisco.vpnsc. cleanup.Runtime TaskCleanupServ ice”	string	Arguments to the class specified in the cmd property.
class	com.cisco.vpnsc. watchdog.servers .WDWorker	string	The server class that proxies Worker service for the watchdog.
cmd	java com.cisco.vpnsc. watchdog.ext.Ser viceLauncherImp l	string	Command to start the worker.
dependencies	nspoller	string	Servers that have to be functioning for this server to function normally.
dependenciesByRole/			Dependencies of httpd based on the role of installation (higher priority than normal dependencies)
cs		string	Dependencies on a CS.
ps		string	Dependencies on a PS.
heartbeat/			Heartbeat related properties.
startDelay	45000	integer, 0-60000 milliseconds	Time to wait before making the first heartbeat request in milliseconds.
timeout	3000	integer, 1000-600000 milliseconds	The period of time before which response for heartbeat request should be received by the watchdog, in milliseconds.
java/			Java attributes for this server.

Table B-1 DCPL Properties (continued)

flags	-Xmx512m -Xbootclasspath/ p:<vpnsc_home> /thirdparty/jar/ AdventNetSnm p3_3.2.jar: <vpnsc_home>/ thirdparty/jar/ cryptix32.jar -Dcom.cisco. insmbu.template mgr.backend. PropFile= <vpnsc_home>/ resources/ templatesystem/ Template. properties	string	Any additional java flags specific to this server. If the value is changed, watchdog restart is required for the new value to take effect.
logLevel	CONFIG	selection	The log Level is the level at which logging is done for this component. These levels are identical to the logging levels defined for JDK1.4 logging package. The levels in descending order are: SEVERE (highest value) WARNING INFO CONFIG FINE FINER FINEST (lowest value).
/watchdog/serverStatus/			The properties related to the server status monitoring function provided by the watchdog are specified here.
emailRecipients	<mailto:Restart>	string	Comma separated list of e-mail addresses to which notices about server state changes should be e-mailed
stableTime	60000	integer, 20000-300000 milliseconds	Time in milliseconds that has to pass before a server's status can be considered stable (for the purpose of sending out a server status e-mail notification).
/watchdog/servers	httpd nspoller dbpoller dispatcher worker scheduler lockmanager cornerstonebridg e	string	Server.
/watchdog/waitDelay	3000	integer, 20000-300000 milliseconds	The time period for which the wait() calls in watchdog wait, before checking the wait condition, in milliseconds.
xml Properties:			The component for XML-based properties.

Table B-1 DCPL Properties (continued)

/xml/queries/			Properties for RepQueryLoader.
filepath	<vpnsc_home>/resources/java/xml/com/cisco/vpnsc/repository/Queries.xml	string	File path and name.



GLOSSARY

A

access control list	See <i>ACL</i> .
ACL	access control list. A list kept by routers to control access to or from the router for a number of services.
antialiasing	Algorithm used to smooth lines in a topology layout.
API	application programming interface. APIs are supplied as XML schema and CORBA IDL files to customers with Cisco VPN Solutions Center products. After compiling these IDL files to produce language-specific implementation files for the <i>target language</i> of your choosing, you can use these APIs to incorporate MPLS-VPN features in third-party client-application source code. The CORBA version is being deprecated from the product and will not be supported in subsequent versions.
Application Programming Interface	See <i>API</i> .
area	Segments and their attached devices. Areas are usually connected to other areas through routers, making up a single autonomous system. See also <i>AS</i> . See also <i>region</i> .
AS	Collection of networks under a common administration sharing a common routing strategy. Autonomous systems are subdivided by <i>areas</i> or <i>regions</i> . An autonomous system must be assigned a unique 16-bit number by the <i>IANA</i> . Specific to BGP for MPLS VPN Solutions.
ASN	autonomous system number.
ATM	Asynchronous Transfer Mode. The international standard for cell relay in which multiple service types (such as voice, video, or data) are conveyed in fixed-length (53-byte) cells. Fixed-length cells allow cell processing to occur in hardware, thereby reducing transit delays. ATM is designed to take advantage of high-speed transmission media, such as E3, SONET, and T3.
audit SR (TE)	Tool for auditing the protection of protected TE elements using all existing backup tunnels and proposed changes.
auto bandwidth / auto-bw	A way to configure a tunnel for automatic bandwidth adjustment and to control the manner in which the bandwidth for a tunnel is adjusted.
autonomous system	See <i>AS</i> .
autonomous system number	See <i>ASN</i> .

B

backing store	Function that stores graphics content when moved to the background and regenerates it when moved to the foreground. This helps avoid superfluous refreshing.
baseline	A set of data collected from targets. For example, the latest configuration files for a list of Cisco Routers, or the latest configuration files, IP unnumbered information, and PVC information for a list of Cisco Routers. MPLS VPN Solution software automatically maintains baselines that correspond to: 1) the latest PE configuration files in the Provider Administrative Domain (with one baseline per PAD); 2) the latest configuration files of the customer edge routers (CEs) and provider edge routers (PEs) in the virtual private networks (VPNs) that the customer has defined. MPLS VPN Solution uses these baselines to create audit and topology reports.
BECN	backwards explicit congestion notification. This is a concept in Frame Relay networking.
BGP	Border Gateway Protocol. An interdomain routing protocol designed for the global Internet. Exterior border gateway protocols (EBGPs) communicate among different autonomous systems. Interior border gateway protocols (IBGPs) communicate among routers within a single autonomous system.
Border Gateway Protocol	See BGP .
border router	A router at the edge of a provider network that interfaces to another provider's border router using the EBGp protocol.

C

CAR	Committed Access Rate. CAR is Cisco's traffic policing tool for instituting a QoS policy at the edge of a network. CAR allows you to identify packets of interest for classification with or without rate limiting. CAR allows you to define a traffic contract in routed networks.
CE	customer edge router. A CE is part of a customer network and interfaces to a provider edge router (PE). A CE can join any set of virtual private networks (VPNs). Each CE connects a customer site to a PE , obtaining the VPN service for that customer site , and belongs to exactly one customer. Each CE may have many configlets and may be configured by multiple service requests.
CEF	Cisco express forwarding. A layer 3 switching technology inside a router. It defines the fastest method by which a Cisco router uses to forward packets from ingress to egress interfaces.
CERC	customer edge routing community. A component of a VPN that is configured for either full mesh or hub-and-spoke connectivity. A method (using route-target attributes) of describing how CEs in a VPN communicate with each other. CERCs organize a complex VPN into simpler subgroups. Each CERC belongs to one and only one VPN. CERCs can be used to describe the logical topology of the VPN itself.
CERC membership	Relationship between a VRF definition and a CERC. It dictates which CERC a VRF definition is joining and whether it is joining the CERC as either a hub or a spoke.
CIM	Common Information Model from the DMTF. Describes components of a managed environment using an object-oriented modeling approach.

C

CIM-CX	Common Information Model - Cisco eXtensions. A DMTF CIM-based model.
CIR	committed information rate. This is a concept in Frame Relay networking.
Cisco Service Management	See CSM .
committed access rate	See CAR .
configlet	A configuration fragment that can be downloaded to a CE or PE to modify its current IOS command-set configuration.
conformant tunnel	A well-behaved tunnel that meets the TE management paradigm of ISC. A conformant primary tunnel with zero hold and setup priorities is a managed tunnel.
CORBA	Common Object Request Broker Architecture.
CSM	Cisco Service Management System. The name of Cisco's large-picture project for service management. Many interdependent products fall within this project.
customer	Requests VPN service from a provider . Each customer may own many customer sites.
customer edge router	See CE .
customer edge routing community	See CERC .
customer network	A network under the control of an end customer. The VPN connects the single customer network by connecting the isolated sites.
customer site	A set of IP systems with mutual IP connectivity between them without the use of a VPN. Each customer site belongs to exactly one customer. A customer site can contain any number of CEs.

D

data-link connection identifier	See DLCI .
data model	A concrete representation of an information model in terms appropriate to a specific data store and access technology.
dCEF	Distributed Cisco expressed forwarding routing. Enables distributed forwarding on versatile interface processors (VIPs).
DHCP	Dynamic Host Configuration Protocol.
DLCI	data-link connection identifier. A value that specifies a private virtual circuit (PVC) or a switched virtual circuit (SVC) in a Frame Relay network.

D

DMTF	Distributed Management Task Force.
DNS	Domain Naming System. System used in the Internet for translating names of network nodes into addresses.
document type definition	See <i>DTD</i> .
Domain Naming System	See <i>DNS</i> .
double buffer	Smooths the lines in the topology display when dragging elements.
DRAM	dynamic random-access memory. RAM that stores information in capacitors that must be periodically refreshed.
DSCP	Differentiated services code point. A field in the IPv4 ToS byte of the packet header that allows you classify packets into any of 64 classes.
DTD	document type definition.
Dynamic Host Configuration Protocol	See <i>DHCP</i> .
dynamic path	A dynamic path is provisioned by allowing the head router to find a path. The dynamic keyword is then provisioned to the routers.
dynamic random-access memory	See <i>DRAM</i> .

E

EBGP	exterior border gateway protocol. EBGP (see <i>BGP</i>) communicate among different network domains.
egress	Traffic leaving the network or device.
Extensible Markup Language	See <i>XML</i> .
exterior border gateway protocol	See <i>EBGP</i> .

F

Fast Re-Route (FRR) protection	Provides link protection to Label-Switched Paths (LSPs). This enables all traffic carried by LSPs that traverse a failed link to be rerouted around the failure.

G

Gigabit Switch Router	See <i>GSR</i> .
global pool	The bandwidth of TE enabled interfaces is assigned a number of nested bandwidth pools. The global pool represents the total reservable bandwidth out of the total link bandwidth.
grooming	Grooming is a TE tool that works on the whole network to optimize the placement of existing managed tunnels. It is only available when no tunnel attributes have been changed.
GSR	Gigabit Switch Router.

H

hold priority	Priority associated with a Label-Switched Path (LSP) for the tunnel to determine if it should be preempted by other LSPs that are being signaled.
Hyper text Transfer Protocol	See <i>HTTP</i> .
HTTP	Hyper text Transfer Protocol. An application protocol running on TCP/IP and the World Wide Web
HTTPS	Secure HTTP. Secure HTTP (HTTPS) provides the capability to connect to the Cisco IOS HTTPS server securely. It uses Secure Sockets Layer (SSL) and Transport Layer Security (TLS) to provide device authentication and data encryption.

I

IANA	Internet Assigned Numbers Authority. Organization operated under the auspices of the ISOC as a part of the IAB. IANA delegates authority for IP address-space allocation and domain-name assignment to the InterNIC and other organizations. IANA also maintains a database of assigned protocol identifiers used in the TCP/IP stack, including BGP autonomous system numbers.
IBGP	interior border gateway protocol. IBGPs (see BGP) communicate among routers within a single network domain.
ICMP	Internet Control Message Protocol. Network layer Internet protocol that reports errors and provides other information relevant to IP packet processing.
IDL	Interface Definition Language. Generic language for describing APIs for API servers. IDL API files must be compiled using an IDL compiler from an approved CORBA vendor to produce language-specific API files in a CORBA-supported target language . Using the generated target-language files you can add API-supported features to third-party client-application source code.
information model	An abstraction and representation of the entities in a managed environment - their properties, operations, and relationships. It is independent of any specific repository, application, protocol, or platform.

I

ingress	Traffic entering the network or device.
Interface Definition Language	See IDL .
interior border gateway protocol	See IBGP .
Internet Control Message Protocol	See ICMP .
internet-service provider	See ISP .
inter-switch link	See ISL .
IPv4	Internet Protocol, version 4. A version of IP that support a 32-bit address space.
IPv6	Internet Protocol, version 6. A version of IP that support a 128-bit address space.
ISL	Inter-Switch Link. Provider of internet access and services through single BGP autonomous system.
ISP	internet-service provider. Provider of internet access and services through single BGP autonomous system.

L

L2VPN	Layer 2 Virtual Private Network.
L2TPv3	Layer 2 Tunnel Protocol Version 3.
link speed factor	TE multiplication factor to be applied to the link speed to determine the amount of bandwidth that must be protected.

M

managed tunnel	The concept of managed tunnels is at the center of TE planning activities. A managed tunnel is a primary TE tunnel characterized by having a setup/hold priority of zero, a non-zero bandwidth, and a valid explicit path. A non-zero bandwidth is defined to be non-zero Resource Reservation Protocol (RSVP) bandwidth or non-zero maximum auto bandwidth if auto bandwidth is enabled.
manage lock	Whenever a task updates the TE database and it might affect the resource and hence the result of a tunnel computation, it locks the system before the update and releases it at completion of the update. Manage lock is a capability provided in the GUI to release the lock under error conditions.
management information base	See MIB .

M

MCE	Management Customer Edge Router. The MCE is a required element in some MPLS VPN topologies. The network management subnet, which consists of the MPLS VPN Solution and Cisco IP Manager workstations on a single local area network (LAN), connects directly to an MCE.
MIB	management information base.
MLPPP	Multilink Point-to-Point Protocol. Method of splitting, recombining, and sequencing datagrams across multiple, logical data links.
MPE	Management Provider Edge Router. The MPE is an element in some MPLS VPN topologies. The network management subnet connect directly to an MCE, which in turn is connected to an MPE.
MPLS	multi protocol label switching. An emerging standard based on a Cisco Tag Switching technology.
MPLS TE tunnel	multiprotocol label switching traffic engineering (MPLS TE) tunnel. Can be a primary or a backup tunnel.
MPLS VPN	multi protocol label switching virtual private network. For MPLS VPN Solution, it is a set of <i>PEs</i> that are connected via a common “backbone” network to supply private IP interconnectivity between two or more <i>customer sites</i> for a given <i>customer</i> . Each VPN has a set of provisioning templates/policies (<i>CERC</i>) and can span multiple <i>Provider Administrative Domains</i> but has a default provider administrative domain for <i>RD</i> and <i>RT</i> auto-allocation purposes. CERCs in a VPN break down complex topology into multiple subgroups.
mutilink point-to-point protocol	<i>See</i> MLPP.
multi protocol label switching	<i>See</i> MPLS.
multi protocol label switching virtual private network	<i>See</i> MPLS VPN.

N

network	In MPLS VPN Solution, a collection of targets with unique names.
network management subnet	Consists of the MPLS VPN Solution and Cisco IP Manager workstations on a single LAN. The network management subnet connects directly to an MCE.
non-conformant tunnel	A TE tunnel, which might impact ISC TM's ability to meet bandwidth guarantees. This could be due to unknown bandwidth requirements such as no max bandwidth configured for auto-bandwidth, potential for pre-emption, dynamic paths, etc. A zero priority unmanaged tunnel would also be a non-conformant tunnel.

O

OSS Operations Support System. Network management system supporting a specific management function, such as alarm surveillance and provisioning, in a carrier network.

operations support system See *OSS*.

P

PAD Provider Administrative Domain. Set of all PE devices in one BGP autonomous system. An administrative domain defined by an Internet Service Provider. The network owned by the PAD is called a backbone network. Each PAD includes a route distinguisher and route target and IP address pools. Each PAD can have any number of regions within it. If an ISP requires two AS numbers, it must consist of two provider administrative domains. Each provider administrative domain has regions that have a route distinguisher (*RD*), a route target (*RT*), and an IP address pool from which to automatically generate IP values during provisioning. Each provider administrative domain can have many *regions*.

PE provider edge router. A router at the edge of a provider network that interfaces to CE routers. Each PE belongs to exactly one *region* of a *Provider Administrative Domain* and connects to one or more *customer sites*. Each PE can have many *VRF* definitions and configlets, and each can be configured by many service requests.

permanent virtual circuit. See *PVC*.

projection (topology map) A map projection is a topology function, which maps a sphere onto a plane.

propagation delay The time it takes for traffic to travel along a link from the head interface to the tail interface.

provider A party supplying internet service for its *customer*. See also *ISP*.

Provider Administrative Domain See *PAD*.

provider edge router See *PE*.

provider network A backbone network under the control of a service provider that provides transport services between customer sites.

PVC permanent virtual circuit. This is applicable to Frame Relay and Asynchronous Transfer Mode.

Q

QoS	Quality of Service. The mechanisms that give network managers the ability to control the mix of bandwidth, delay, jitter, and packet loss in the network. QoS is not a device feature, it is an end-to-end system architecture.
quality of Service	See <i>QoS</i> .

R

RD	Route Distinguisher. A 64-bit value that is added to an IPv4 prefix to create a unique VPN prefix. Each VRF has an RD.
region	A group of provider edge routers (PEs) within a single BGP autonomous system. Provider Administrative Domains are divided into regions just as customers are divided into sites. Each region belongs to exactly one provider administrative domain and can have many PEs. Regions allow a provider to employ unique IP address pools in large geographical regions. Each region is represented in the VPN Inventory Repository by a Region object.
response time reporter	Renamed to service assurance agent (SA Agent).
RIP	Routing Information Protocol. The simplest Interior Gateway Protocol (IGP) in the Internet.
round-trip time	See RTT .
route distinguisher	See RD .
route target	See RT .
Routing Information Protocol	See RIP .
RT	Route Target. A 64-bit value by which the IOS discriminates routes for route updates in VRFs.
RTR	Renamed to Service Assurance Agent (SA Agent).
RTT	Round-trip time. The total time required for a packet to traverse a network to its destination and back again.

S

SA Agent	Service Assurance Agent. SA Agent provides Round-Trip Time for various protocols: DHCP, DNS, HTTP, ICMP Echo, Jitter, TCP Connect, and UDP Echo.
schema	A set of data models that describe a set of objects to be managed.
seed router	The TE network discovery process uses a seed router as an initial communication point to discover the MPLS TE network topology.

S

Service Assurance Agent	See SA Agent .
service level agreement	See SLA .
setup priority	Priority used when signaling a Label-Switched Path (LSP) for the tunnel to determine which of the existing tunnels can be preempted.
site	A component of a customer. A collection of one or more customer edge routers (CEs).
SLA	Service Level Agreement. Service-Level Agreements (SLAs) are negotiated contracts between VPN providers and their subscribers. An SLA defines the criteria for the specific services that the subscriber expects the provider to deliver. The SLA is the only binding mechanism at the subscriber's disposal to ensure that the VPN provider delivers the services as agreed.
SOAP	A lightweight protocol for exchange of information in a decentralized, distributed environment. It is an XML based protocol that consists of three parts: an envelope that defines a framework for describing what is in a message and how to process it, a set of encoding rules for expressing instances of application-defined datatypes, and a convention for representing remote procedure calls and responses.
SNMP	Simple Network Management Protocol.
SP	Service Provider.
Static route	Route that is explicitly configured and entered into the routing table. Static routes take precedence over routes chosen by dynamic routing protocols.
sub pool	The bandwidth of TE enabled interfaces is assigned a number of nested bandwidth pools. A sub pool is a bandwidth pool nested inside a global pool. Thus, if for example a primary tunnel reserves bandwidth from the sub pool, it will also reserve the same bandwidth from the global pool.
system path	An ISC system generated explicit path (immovable unless the tunnel is set to be reroutable). The first path has to be an explicit path.

T

target	Single device from which information may be collected. A target may be a router. Any device (customer edge router, provider edge router, or RMON probe) from which the MPLS VPN Solution software can collect information.
target language	CORBA -supported programming language to be generated by the IDL compiler based on the IDL API files. The generated target-language files can then be used to incorporate API-supported features in third-party client-application source code. For a complete list of CORBA-supported target languages, see the Object Modeling Group web site.
TCP	Transmission Control Protocol. Connection-oriented transport layer protocol that provides reliable full-duplex data transmission.
TE	traffic engineering.

T

TE discovery	An ISC task used to populate the repository with the TE network element and data.
TE explicit path	A fixed path from a specific head to a specific destination device. Paths are defined between source and destination routers, possibly with one or more hops in between.
TE functional audit	A task that checks the Label-Switched Path (LSP) used on a router at a given moment against the LSP stored in the repository.
TE link	A link between two TE enabled interfaces.
TE metric	Metric used to override the Interior Gateway Protocol (IGP) administrative weight (cost) of a TE link.
TE node	A TE enabled node.
TE policy	A set of rules established for a tunnel to carry TE traffic.
TE provider	The TE provider is a concept designed to allow the network management application to manage many different operators simultaneously, each working on different networks.
TE topology	A TE topology provides a graphical representation of the various network elements in a TE network, such as devices, links, and tunnels.
TE traffic admission	Also referred to as tunnel admission. It is the first step towards enabling services on TE tunnels by assigning traffic to traffic-engineered tunnels.
TE tunnel	See MPLS TE tunnel.
Transmission Control Protocol	See TCP .
tunnel audit	When any type of change to the TE network is required, whether tunnel or resource modifications, a tunnel audit is run to determine what inconsistencies the change might cause, if any.
tunnel placement	Tunnel placement is a TE tool for calculating optimal paths for new or changed tunnels in the existing network.
tunnel repair	As changes are made to bandwidth requirements or delay parameters of existing TE tunnels, tunnel placement can create inconsistencies. Tunnel repair is designed to address such inconsistencies. The objective of tunnel repair is to try to move as few existing tunnels as possible to accommodate the changes.

U

UDP	User Datagram Protocol. Connectionless transport layer protocol in the TCP/IP protocol stack. UDP is a simple protocol that exchanges datagrams without acknowledgments or guaranteed delivery, requiring that error processing and retransmission be handled by other protocols.
unmanaged tunnel	An unmanaged tunnel is any tunnel that is not managed. See managed tunnel.
User Datagram Protocol	See UDP .

V

VCI	virtual channel identifier. Used in ATM networking concept.
virtual channel identifier	See <i>VCI</i> .
virtual LAN	See <i>VLAN</i> .
virtual path identifier	See <i>VPI</i> .
virtual private network	See <i>VPN</i> .
VLAN	virtual LAN. Group of devices on a LAN that are configured so they can communicate as if they were attached to the same wire, when in fact they are located on a number of different LAN segments.
VoIP	voice over internet protocol.
VPI	virtual path identifier. The VPI, together with the VCI, is used to identify the next destination of a cell as it passes through a series of ATM switches on its way to its destination.
VPIM	VPN Provisioning and Inventory Manager.
VPLS	Virtual Private LAN Service.
VPN	Virtual Private Network. A framework that provides private IP networking over a public infrastructure such as the Internet. In MPLS VPN Solution, a VPN is a set of customer sites that are configured to communicate through a VPN service. A VPN is a network in which two sites can communicate over the provider's network in a private manner; that is, no site outside the VPN can intercept their packets or inject new packets. The provider network is configured such that only one VPN's packets can be transmitted through that VPN—that is, no data can come in or out of the VPN unless it is specifically configured to allow it. There is a physical connection from the provider edge network to the customer edge network, so authentication in the conventional sense is not required. A VPN is a private network constructed within a public network infrastructure, such as the Internet. A VPN is a communications environment in which access is controlled to permit peer connections only within a defined community of interest, and is constructed through some form of partitioning of a common underlying communications medium, where this communications medium provides services to the network on a nonexclusive basis.
VPN customer	Owner of VPN.
VPN routing/forwarding instance	See <i>VRF</i> .
VRF definition	The configuration information for a <i>VPN routing/forwarding instance</i> (<i>VRF</i>) table for <i>PEs</i> that share a common route-target (<i>RT</i>) signature. In the VPN inventory repository, a VRF definition is a template by which to define a VRF table in a <i>PE</i> .

V

VRF VPN routing/forwarding instance. A routing table that is populated with VPN routes. A VRF is an IOS route table instance for connecting a set of sites to a VPN service.

W

WSDL Web Services Definition Language

X

XML Extensible Markup Language.

XML API A programmatic interface to ISC used by OSS systems. The XML API is implement in a SOAP over HTTP format and provides full ISC functionality.

XML Schema A specific format (.xsd) to describe XML structures (for example, metadata).



A

AAA server [1-12, 3-2, 3-121](#)
 access [3-121](#)
 define [3-121](#)
 delete [3-123](#)
aagent Properties [B-32](#)
about [1-5](#)
access domain
 create [3-101](#)
Account [1-5](#)
Active Users [1-18, 8-1, 8-37](#)
active users [8-37](#)
admin [1-2](#)
Administration [1-2, 1-3, 1-16, 8-1](#)
advanced filter [8-38](#)
aggregated traffic shaper [6-52](#)
audience [xxxii](#)
Auto Discovery [4-6](#)
AutoDiscovery Property [B-1](#)
auto refresh [1-8](#)

B

background daemon [2-1](#)
bootstrapping [2-1](#)
Broken state [3-3](#)

C

CERC [3-114](#)
 access [3-115](#)
 delete [3-117](#)

CERCs [3-2](#)
CE routing community [1-12, 3-2, 3-114](#)
 access [3-115](#)
 delete [3-117](#)
Certificate Enrollment Audit [7-5](#)
Cleanup Properties [B-1](#)
closed state [3-3](#)
cnserver server [2-9](#)
Collect Config [7-3](#)
Collections Zones [8-32](#)
Collection Zones [1-17](#)
commands
 startwd [2-2](#)
 stopwd [2-3, 2-4](#)
 watchdog [2-1](#)
 wdclient [2-5](#)
Config Audit [7-5](#)
configuration files [4-5](#)
configurations
 view [6-3](#)
Control Center [1-17, 8-1, 8-25](#)
conventions [xxxiii](#)
cornerstone bridge server [2-9](#)
CPE devices
 configuring SSH connectivity [3-39, 3-40](#)
create [3-81](#)
 user groups [8-9](#)
 user role [8-14, 8-20](#)
Create Data File [6-3, 6-14](#)
create ICMP [6-47](#)
create IGMP [6-47](#)
create IP [6-48](#)
create TCP [6-44](#)

Create Template [6-3, 6-5](#)

create UDP [6-45](#)

customer [1-12, 3-2, 3-86](#)

access [3-86](#)

associating with devices [8-16](#)

create [3-87](#)

definition [8-11](#)

delete [3-89](#)

edit [3-88](#)

customer site

create [3-90](#)

D

Data File

Delete [6-21](#)

Edit [6-19](#)

data file name [6-16](#)

dbpoller server [2-9](#)

DCPL properties [B-1](#)

DCS Properties [B-2](#)

Delete [6-3](#)

delete

user groups [8-10](#)

user roles [8-18, 8-21](#)

users [8-7](#)

deployed state [3-3](#)

DeploymentFlow Property [B-9](#)

device [1-12, 3-2, 3-38](#)

copy [3-79](#)

creation [3-45](#)

delete [3-75](#)

edit [3-73](#)

e-mail [3-85](#)

device configuration, edit [3-76](#)

Device Configuration Manager [5-8](#)

Device Console [1-13, 5-1](#)

Device Discovery [4-50](#)

device group [1-12, 3-2, 3-80, 3-81](#)

access [3-81](#)

delete [3-84](#)

edit [3-84](#)

device owner, e-mail [3-77](#)

diagnostic tools [2-5](#)

disabled_dependent state [2-10](#)

disabled state [2-10](#)

disconnect button [8-37](#)

dispatcher server [2-9](#)

DistributionFramework Properties [B-9](#)

documentation [xxxi](#)

Download Commands [5-2](#)

Download Template [5-3](#)

dtd Properties [B-33](#)

Dynamic Java Class type [6-13](#)

Dynamic URL type [6-13](#)

E

Edit [6-3](#)

edit

user groups [8-10](#)

user roles [8-17, 8-21](#)

users [8-7](#)

e-mail, device group [3-85](#)

e-mail device owner [3-77](#)

EXEC Commands [5-10](#)

exec time column [2-10](#)

F

failed audit state [3-3](#)

failed deploy state [3-3](#)

filter [1-7](#)

advanced [8-38](#)

simple [8-38](#)

find

- user groups [8-11](#)

- users [8-8](#)

finding the discovered NPCs in IM [4-11, 4-96](#)

finding the discovered SRs in IM [4-12](#)

Firewall

- marking Interfaces for Firewall in IM [4-9](#)

firewall example template [6-22](#)

Float type [6-10](#)

Functional state [3-3](#)

G

gen column [2-10](#)

getting started [1-1](#)

glossary [1](#)

Grey Management Discovery [4-110](#)

GSAM Property [B-11](#)

GTL Properties [B-11](#)

GUI Properties [B-13](#)

H

help [1-5](#)

Home screen [1-2, 1-3, 7-1, 8-1](#)

Hosts [1-17, 8-25](#)

- config [8-27](#)

- details [8-26](#)

- servers [8-28](#)

- Watchdog [8-29](#)

HTTP CoS Report [7-59](#)

httpd server [2-9](#)

HTTP report [7-57](#)

I

ICPM

- create [6-47](#)

IGMP

- create [6-47](#)

IM

- accessing GUI [4-34](#)

- Cell Editing Examples [4-40](#)

- choosing all the POPs [4-7](#)

- choosing the seed devices and hub [4-7](#)

- create a new Device Group [4-36](#)

- discovering devices [4-50](#)

- editing cells [4-40](#)

- Edit menu [4-84](#)

- enabling passwords into the defaults row [4-8](#)

- File menu [4-35](#)

- finding the discovered NPCs [4-11, 4-96](#)

- finding the discovered SRs [4-12](#)

- GUI reference [4-34](#)

- Importing devices with Auto Discovery [4-6](#)

- importing devices with configuration files [4-5](#)

- importing devices without configuration files [4-6](#)

- launching IM [3-7, 4-3](#)

- Logging menu [4-104](#)

- marking interfaces [4-97](#)

- marking Interfaces for IPsec, Firewall, NAT, or QoS [4-9](#)

- open a rule editor [4-97](#)

- rule editor [4-97](#)

- running NPC discovery [4-11](#)

- specifying the maximum hop count [4-7](#)

- spreadsheet [4-13](#)

- Tasks menu [4-90](#)

- Tools menu [4-97](#)

- View menu [4-90](#)

- importing devices with configuration files [4-5](#)

- importing devices without configuration files [4-6](#)

Index [1-5](#)

installation

- remote [8-30](#)

Integer type [6-9](#)

interface example template [6-22](#)

interface rules [4-97](#)
 introduction [1-1](#)
 invalid state [3-4](#)
 Inventory and Connection Manager [1-12, 3-1](#)
 Inventory Manager [1-12, 3-5](#)
 See IM
 inventory manager [3-2](#)
 IOS [3-39](#)
 IP
 create [6-48](#)
 IP address
 create [3-104](#)
 IP address pool [3-102](#)
 IPsec
 marking Interfaces for IPsec in IM [4-9](#)
 IPsec Functional Audit [7-5](#)
 IPv4 type [6-11](#)

J

Jitter CoS Report [7-59](#)
 Jitter report [7-58](#)

K

keys [3-39](#)

L

Licensing [1-17, 8-34](#)
 link efficiency [6-53](#)
 Link QoS [1-15, 6-51](#)
 Link QoS Manager [6-1](#)
 lockmanager Properties [B-33](#)
 lockmanager server [2-9](#)
 Logging Properties [B-15](#)
 logout [1-6](#)

logs [8-31](#)
 lost state [3-4](#)

M

Manage TIBCO Rendezvous [1-18, 8-1, 8-39](#)
 manual, objective [xxxi](#)
 manual organization [xxxii](#)
 maps [3-34](#)
 maps, adding [3-38](#)
 maximum hop count [4-7](#)
 missed column [2-10](#)
 Monitoring [1-3, 1-15, 7-1](#)
 mouse terminology [xxxiii](#)
 MPLS Functional Audit [7-5](#)
 MPLS Service Discovery [4-108](#)
 Multicast pool [3-102](#)
 create [3-105](#)

N

name column [2-9](#)
 Named Physical Circuit [1-12, 3-123](#)
 access [3-124](#)
 create [3-125](#)
 delete [3-128](#)
 Named Physical Circuits [3-2](#)
 NAT
 marking Interfaces for NAT in IM [4-9](#)
 nbi Properties [B-34](#)
 Network Objects [1-15, 6-57](#)
 create [6-57](#)
 delete [6-59](#)
 edit [6-59](#)
 Network Objects Manager [6-1](#)
 node locations [3-37](#)
 notification Properties [B-35](#)

NPC 3-123

- access [3-124](#)
- create [3-125](#)
- delete [3-128](#)

NPC discovery

- running NPC discovery in IM [4-11](#)

nspoller server 2-9

O**Object Groups 1-17**

- objective [xxxix](#)
- one-dimensional array [6-17](#)
- orbd [2-2](#)
- organization of manual [xxxix](#)

P**parent role**

- definition [8-11](#)

passwords

- enabling passwords into the defaults [4-8](#)

PE device

- create [3-100](#)

pending state 3-4**permission for others**

- definition [8-5](#)

permissions

- user roles [8-11](#)

pid column 2-10**Ping 1-16, 7-1, 7-8**

- IPsec [7-11](#)
- MPLS [7-9](#)

PIX Firewall

- configuring SSH for [3-40](#)

Policies 1-14, 6-2**Policy Manager 6-1****POPs**

- choosing all the POPs [4-7](#)

probes 7-15

- create from any SA Agent device [7-16](#)
- create from IPsec CPE [7-36](#)
- create from MPLS CPE [7-22](#)
- create from MPLS PE [7-29](#)
- delete [7-47](#)
- details [7-46](#)
- disable [7-51](#)
- enable [7-49](#)

product introduction 1-1**properties B-1****Protocol Bundles 1-15, 6-49**

- create [6-50](#)
- delete [6-51](#)
- edit [6-50](#)

Protocol Manager 6-1**Protocols 1-14, 6-43, 6-44**

- delete [6-49](#)
- edit [6-48](#)

protocols 7-41**provider 1-12, 3-2, 3-95**

- access [3-96](#)
- create [3-97](#)
- definition [8-11](#)
- delete [3-98](#)
- edit [3-97](#)

provider region

- create [3-99](#)

Provisioning Properties B-16

Q**QoS**

- marking Interfaces for QoS in IM [4-9](#)

R

RD pool [3-103](#)
 create [3-106](#)
 recommendations, system [1-1](#)
 related documentation [xxxi](#)
 Reload [5-15](#)
 remote installation [8-30](#)
 remote uninstallation [8-31](#)
 repository Properties [B-36](#)
 requested state [3-4](#)
 resource pool [1-12, 3-2, 3-102](#)
 access [3-103](#)
 delete [3-113](#)
 restart_delay state [2-10](#)
 right to use [8-36](#)
 Route Distinguisher pool [3-103](#)
 create [3-106](#)
 Route Target pool [3-103](#)
 create [3-106](#)
 rows per page [1-7](#)
 RT pool [3-103](#)
 create [3-106](#)
 Runtime Actions [7-7](#)

S

SA agents, enabling [3-43](#)
 Scheduler Properties [B-28](#)
 scheduler server [2-9](#)
 Security [1-2, 1-16, 8-1, 8-2](#)
 seed devices
 choosing the seed devices and hub [4-7](#)
 Select & Click Go [6-7](#)
 server names [2-9](#)
 Service Deployment [7-3, 7-5](#)
 Service Design [1-3, 1-13, 6-2](#)
 Service Inventory [1-3, 1-11, 3-1, 4-1](#)

Service Level Agreement [7-14](#)
 setup [7-14](#)
 Service Request [1-12](#)
 service request [3-2, 3-3](#)
 states [3-3](#)
 Services
 IPsec [6-17](#)
 IPsecRA [6-17](#)
 L2VPN [6-17](#)
 MPLS [6-17](#)
 NAT [6-17](#)
 Show button [6-3](#)
 Show Data File Matching [6-3](#)
 Show Template Matching [6-3](#)
 simple filter [8-38](#)
 site of origin pool [3-103](#)
 create [3-109](#)
 SLA [1-16, 7-1, 7-14](#)
 HTTP CoS Report [7-59](#)
 HTTP report [7-57](#)
 Jitter CoS Report [7-59](#)
 Jitter report [7-58](#)
 setup [7-14](#)
 Summary CoS Report [7-58](#)
 summary report [7-55](#)
 SLA Collection [7-3](#)
 SLA Properties [B-28](#)
 SLA reports [7-54](#)
 SNMP
 setting up [3-41](#)
 SNMPv1 [3-42](#)
 SNMPv3 [3-42](#)
 SnmpService Properties [B-30](#)
 specifying the maximum hop count [4-7](#)
 SSH
 configuring for CPE devices [3-39, 3-40](#)
 configuring on Cisco routers [3-39](#)
 configuring on PIX Firewalls [3-40](#)
 configuring on VPN 3000 [3-40](#)

SSH connections, configuring [3-39](#)

start_depends state [2-9](#)

startdb command [2-1, 2-2](#)

started state [2-9](#)

starting device discovery [4-6](#)

starting state [2-9](#)

startns command [2-2](#)

startwd [2-1](#)

startwd command [2-2](#)

state

Broken [3-3](#)

closed [3-3](#)

deployed [3-3](#)

disabled [2-10](#)

disabled_dependent [2-10](#)

failed audit [3-3](#)

failed deploy [3-3](#)

Functional [3-3](#)

invalid [3-4](#)

lost [3-4](#)

pending [3-4](#)

requested [3-4](#)

restart_delay [2-10](#)

start_depends [2-9](#)

started [2-9](#)

starting [2-9](#)

stop_depends [2-9](#)

stopped [2-10](#)

stopping_gently [2-10](#)

stopping_hard [2-10](#)

Wait Deployed [3-4](#)

state column [2-9](#)

states of service requests [3-3](#)

states transition diagram [3-5](#)

stop_depends state [2-9](#)

stopall command [2-3](#)

stopdb command [2-3](#)

stopns command [2-3, 2-4](#)

stopped state [2-10](#)

stopping_gently state [2-10](#)

stopping_hard state [2-10](#)

stopwd command [2-4](#)

String type [6-8, 6-9](#)

Sub-Template type [6-12](#)

success column [2-10](#)

Summary CoS Report [7-58](#)

summary report [7-55](#)

SYSTEM Properties [B-29](#)

system recommendations [1-1](#)

T

task, creating new [7-3](#)

Task Logs [7-6](#)

Task Manager [1-16, 7-1](#)

starting [7-2](#)

Task Service Requests [7-4](#)

TCP

create [6-44](#)

Template

Delete [6-21](#)

Edit [6-19](#)

template examples [6-22](#)

Template Manager [6-1](#)

data pane [6-3](#)

Template Name [6-6](#)

Templates [1-14, 6-2](#)

tree [6-3](#)

TE Performance Report [1-16](#)

terminology [xxxiii](#)

topology [3-2, 3-5](#)

accessing [3-11](#)

areas [3-12](#)

conventions [3-9](#)

filtering [3-30](#)

introduction [3-6](#)

logical view [3-19](#)

maps [3-34](#)

- maps, adding [3-38](#)
- node locations [3-37](#)
- physical view [3-22](#)
- searching [3-33](#)
- view types [3-13](#)
- VPN view [3-15](#)
- topology tool [1-12](#)
- traps
 - disable [7-53](#)
 - enable [7-50](#)
- two-dimensional array [6-18](#)
- Type
 - Dynamic Java Class [6-13](#)
 - Dynamic URL [6-13](#)
 - float [6-10](#)
 - integer [6-9](#)
 - IPv4 [6-11](#)
 - string [6-8, 6-9](#)
 - sub-template [6-12](#)
- typographical conventions [xxxiii](#)

U

- UDP
 - create [6-45](#)
- uninstallation
 - remote [8-31](#)
- user
 - deleting [8-7](#)
 - finding [8-8](#)
 - managing [8-2](#)
- User Access Log [1-18, 8-1, 8-37](#)
- user group
 - creating [8-9](#)
 - deleting [8-10](#)
 - editing [8-10](#)
 - finding [8-11](#)
 - managing [8-8](#)
- User Groups [1-16](#)

- user management
 - user groups [8-8](#)
 - user roles [8-11](#)
 - users [8-2](#)
- user role
 - creating [8-14, 8-20](#)
 - customer [8-11](#)
 - deleting [8-18, 8-21](#)
 - editing [8-17, 8-21](#)
 - managing [8-11](#)
 - parent role [8-11](#)
 - provider [8-11](#)
- User Roles [1-2, 1-16](#)
- Users [1-16](#)
- users
 - assigned roles [8-6](#)
 - editing [8-7](#)
 - group membership [8-6](#)
 - permission for others [8-5](#)
- users, active [8-37](#)

V

- Validate [6-7](#)
- Variables [6-7](#)
- VC ID pool
 - create [3-111](#)
- VC IP pool [3-103](#)
- View configurations [6-3](#)
- VLAN ID pool [3-103](#)
- VLAN pool
 - create [3-112](#)
- VPLS Service Discovery [4-112](#)
- VPN [1-12, 3-2, 3-117](#)
 - access [3-118](#)
 - console, overview [1-2](#)
 - create [3-118](#)
 - delete [3-120](#)
- vpn3000 events template examples [6-24](#)

vpn3000 routing template examples [6-24](#)
 vpn3000 server template examples [6-25](#)
 VpnInvServer Properties [B-32](#)
 VPN Service Module
 See VPNSM

W

Wait Deployed state [3-4](#)
 watchdog commands [2-1](#)
 startwd [2-2](#)
 stopwd [2-4](#)
 wdclient [2-5](#)
 wdgui [2-11](#)
 watchdog Properties [B-38](#)
 wdclient command [2-5](#)
 wdclient disk subcommand [2-5](#)
 wdclient group [2-5, 2-6](#)
 wdclient groups [2-6](#)
 wdclient groups subcommand [2-6](#)
 wdclient group subcommand [2-6](#)
 wdclient health subcommand [2-7](#)
 wdclient log [2-7](#)
 wdclient restart [2-7](#)
 wdclient restart subcommand [2-7](#)
 wdclient start [2-7](#)
 wdclient start subcommand [2-7](#)
 wdclient status [2-8](#)
 wdclient status subcommand [2-8](#)
 wdclient stop [2-10](#)
 wdclient stop subcommand [2-10](#)
 wdclient subcommands
 exec time column [2-10](#)
 gen column [2-10](#)
 missed column [2-10](#)
 name column [2-9](#)
 pid column [2-10](#)
 state column [2-9](#)
 success column [2-10](#)

wdclient group [2-5, 2-6](#)
 wdclient groups [2-6](#)
 wdclient log [2-7](#)
 wdclient restart [2-7](#)
 wdclient start [2-7](#)
 wdclient status [2-8](#)
 wdclient stop [2-10](#)
 wdclient syshealth subcommand [2-11](#)
 worker server [2-9](#)

X

xml Properties [B-48](#)

