



Cisco IP Solution Center Infrastructure Reference, 5.0.1

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.

Americas Headquarters

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

Text Part Number: OL-15585-01

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.

CCDE, CCVP, Cisco Eos, Cisco StadiumVision, the Cisco logo, DCE, and Welcome to the Human Network are trademarks; Changing the Way We Work, Live, Play, and Learn is a service mark; and Access Registrar, Aironet, AsyncOS, Bringing the Meeting To You, Catalyst, CCDA, CCDP, CCIE, CCIP, CCNA, CCNP, CCSP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Cisco Unity, Collaboration Without Limitation, Enterprise/Solver, EtherChannel, EtherFast, EtherSwitch, Event Center, Fast Step, Follow Me Browsing, FormShare, GigaDrive, HomeLink, Internet Quotient, IOS, iPhone, IP/TV, iQ Expertise, the iQ logo, iQ Net Readiness Scorecard, iQuick Study, IronPort, the IronPort logo, LightStream, Linksys, MediaTone, MeetingPlace, MGX, Networkers, Networking Academy, Network Registrar, PCNow, PIX, PowerPanels, ProConnect, ScriptShare, SenderBase, SMARTnet, Spectrum Expert, StackWise, The Fastest Way to Increase Your Internet Quotient, TransPath, WebEx, and the WebEx logo 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. (0801R)

Cisco IP Solution Center Infrastructure Reference, 5.0.1

Copyright © 2008, Cisco Systems, Inc.

All rights reserved.



CONTENTS

About This Guide xv

Objective xv

Related Documentation xv

Audience xvi

How This Book Is Organized xvii

Obtaining Documentation and Submitting a Service Request xvii

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 1-6

About 1-6

Logout 1-6

Customer 1-6

Common GUI Components 1-7

Filters 1-7

Header Row Check Box 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 1-10

Service Design 1-12

Monitoring 1-13

Diagnostics 1-14

Administration 1-15

CHAPTER 2**WatchDog Commands 2-1**

startdb Command	2-1
Description	2-1
Syntax	2-2
startns Command	2-2
Description	2-2
Syntax	2-2
startwd Command	2-2
Description	2-2
Syntax	2-3
stopall Command	2-3
Description	2-3
Syntax	2-3
stopdb Command	2-3
Description	2-3
Syntax	2-4
stopns Command	2-4
Description	2-4
Syntax	2-4
stopwd Command	2-4
Description	2-4
Syntax	2-5
wdclient Command	2-5
wdclient disk Subcommand	2-5
Description	2-6
Syntax	2-6
wdclient group <i><group_name></i> Subcommand	2-6
Description	2-6
Syntax	2-6
wdclient groups Subcommand	2-6
Description	2-6
Syntax	2-6
wdclient health Subcommand	2-6
Description	2-6
Syntax	2-7
wdclient restart Subcommand	2-7
Description	2-7
Syntax	2-7

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

CHAPTER 3

Service Inventory — Inventory and Connection Manager 3-1

Service Requests	3-2
Traffic Engineering Management	3-5
Inventory Manager	3-5
Accessing the Inventory Manager Window	3-5
Importing Devices	3-6
Opening and Editing Devices	3-7
General Attributes Devices	3-9
Password Attributes Devices	3-10
SNMP Attributes Devices	3-11
CNS Attributes Devices	3-12
Platform Attributes Devices	3-13
Interfaces Devices	3-14
Opening and Editing PEs	3-16
General Attributes Provider	3-18
Password Attributes Provider	3-19
SNMP Attributes Provider	3-21
CNS Attributes Provider	3-22
Platform Attributes Provider	3-23
PE Attributes Provider	3-24
Interfaces Provider	3-25

Opening and Editing CEs	3-26
General Attributes Customer	3-29
Password Attributes Customer	3-30
SNMP Attributes Customer	3-31
CNS Attributes Customer	3-32
Platform Attributes Customer	3-33
CPE Attributes Customer	3-34
Interfaces Customer	3-35
Assigning Devices	3-36
Topology Tool	3-38
Introduction	3-39
Launching Topology Tool	3-39
Conventions	3-41
Accessing the Topology Tool for ISC-VPN Topology	3-44
Types of Views	3-46
VPN View	3-47
Logical View	3-52
Physical View	3-55
Viewing Device and Link Properties	3-56
Device Properties	3-57
Link Properties	3-60
Filtering and Searching	3-63
Filtering	3-63
Searching	3-66
Using Maps	3-67
Loading a map	3-68
Layers	3-69
Map data	3-70
Node locations	3-70
Adding new maps	3-71
Devices	3-71
Configuring SSH or SSHv2	3-72
Configuring SSH on Cisco IOS Routers Using a Domain Name	3-72
Configuring SSHv1 or SSHv2 on Cisco IOS Routers Using RSA Key Pairs	3-73
Configuring SSH or SSHv2 on Cisco IOS XR Routers	3-73
Setting Up SNMP	3-75
Setting Up SNMPv1/v2c on Cisco IOS Routers	3-76
Setting SNMPv3 Parameters on Cisco IOS Routers	3-76
Manually Enabling RTR Responder on Cisco IOS Routers	3-77
Accessing the Devices Window	3-77

Creating a Device	3-79
Creating a Catalyst Switch	3-80
Creating a Cisco Device	3-85
Creating a Terminal Server	3-91
Creating a Cisco CNS IE2100	3-96
Editing a Device	3-97
Deleting Devices	3-100
Editing a Device Configuration	3-101
E-mailing a Device's Owner	3-103
Copying a Device	3-104
Device Groups	3-105
Accessing the Device Groups Window	3-106
Creating a Device Group	3-106
Editing a Device Group	3-109
Deleting Device Groups	3-109
E-mailing a Device Group	3-110
Customers	3-111
Accessing the Customers Window	3-112
Creating a Customer	3-112
Editing a Customer	3-113
Deleting Customers	3-114
Creating Customer Sites	3-115
CPE Devices	3-116
Create CPE Device	3-117
Edit CPE Device	3-118
Delete CPE Device	3-119
Providers	3-119
Accessing the Providers Window	3-120
Creating a Provider	3-120
Editing a Provider	3-121
Deleting Providers	3-122
Creating Provider Regions	3-123
Creating PE Devices	3-124
Creating Access Domains	3-125
Resource Pools	3-126
Accessing the Resource Pools Window	3-127
Creating an IP Address Pool	3-128
Creating a Multicast Pool	3-129
Creating a Route Distinguisher and Route Target Pool	3-130

Creating a Site of Origin Pool	3-132
Creating a VC ID Pool	3-134
Creating a VLAN Pool	3-134
Deleting Resource Pools	3-136
CE Routing Communities	3-136
Accessing the CE Routing Communities Window	3-137
Creating CE Routing Communities	3-138
Deleting CE Routing Communities	3-139
VPNs	3-140
Accessing the VPNs Window	3-140
Creating a VPN	3-141
Deleting VPNs	3-144
Named Physical Circuits	3-144
Accessing the Named Physical Circuits Window	3-145
Creating a Named Physical Circuit	3-146
Deleting Named Physical Circuits	3-150
Creating NPC Rings	3-150
Editing NPC Rings	3-154
Deleting NPC Rings	3-154

CHAPTER 4

Service Inventory—Discovery 4-1

Overview of ISC Discovery	4-1
Technical Notes for ISC Discovery	4-5
General Notes	4-6
Using the Discovery Log Files	4-6
Using ISC Discovery with Cisco IP Solution Center MPLS VPN Management	4-6
Using ISC Discovery With Cisco IP Solution Center L2VPN Management	4-7
Using ISC Discovery with Cisco IP Solution Center MPLS Diagnostics Expert	4-7
Using ISC Discovery With Cisco IP Solution Center Traffic Engineering Management	4-8
Summary of Tasks for Discovery (Cisco ISC MPLS VPN Management and L2VPN Management)	4-8
Summary of ISC Discovery Steps for MPLS Diagnostics Expert	4-12
Step 1: Perform Preliminary Steps	4-15
Review System Requirements	4-16
Install Licenses	4-17
Discovery in Large Networks	4-17
(CDP Discovery Only) Verify That a Unique TIBCO Port Is Defined	4-17
(CDP Discovery Only) Verify That CDP Is Running on Devices To Be Discovered	4-18
Code XML Files Required for Discovery	4-19
Sample XML Files	4-19

Coding the policy.xml File	4-19
Coding the device.xml File	4-22
Coding the topology.xml File	4-23
Step 2: Perform Device Discovery	4-25
Starting Device Discovery	4-26
Editing Device Configurations	4-31
Setting Password Attributes (Required Step)	4-33
Setting General Device Attributes	4-35
Setting Cisco CNS Attributes	4-36
Saving the Device Configuration	4-37
Step 3: Perform Discovery Data Collection	4-37
Step 4: Perform Role Assignment	4-37
Initiating Device Role Assignment	4-38
Changing the Device Assignment Display	4-39
Changing Device Assignments	4-40
Assigning Devices Individually or in Bulk	4-40
Determine Device Roles	4-41
Assigning the PE Role	4-41
Editing the PE Role	4-43
Assigning the CE Role	4-44
Editing the CE Role	4-46
Saving the Role Assignment Information	4-49
Step 5: Perform NPC Discovery	4-50
Preliminary Steps Before Completing NPC Discovery for Metro Ethernet Networks	4-50
Create Access Domains	4-51
Create Resource Pools	4-51
Edit Inter-N-PE Interfaces	4-51
Starting NPC Assignment	4-52
Adding a Device for an NPC	4-54
Adding a Ring	4-55
Inserting a Device	4-56
Inserting a Ring	4-56
Deleting a Device or a Ring	4-56
Saving the NPC Configuration	4-57
Step 6: Perform MPLS VPN Service Discovery (Optional)	4-57
Filtering the MPLS VPN View	4-59
Splitting a VPN	4-59
Creating a VPN	4-62

Viewing VPN Link Details	4-64
Saving the MPLS VPNs and Initiating MPLS VPN Service Creation	4-65
Step 7: Perform L2VPN (Metro Ethernet) Service Discovery (Optional)	4-66
Viewing Discovered Layer 2 Services Grouped by VPN	4-67
Editing Discovered Layer 2 Services Grouped by VPN	4-69
Deleting Discovered Layer 2 Services Grouped by VPN	4-70
Viewing Discovered Layer 2 End to End Wires	4-70
Editing the VPN Associated with an End to End Wire	4-72
Splitting Layer 2 Service End to End Wires	4-73
Joining Layer 2 Service End to End Wires	4-74
Deleting Layer 2 Service End to End Wires	4-74
Viewing Discovered Layer 2 VPLS Links	4-74
Editing Discovered Layer 2 VPLS Links	4-76
Deleting Discovered Layer 2 VPLS Links	4-77
Saving the L2VPN Metro Ethernet Policy and Initiating Service Creation	4-78
Step 8: Commit Discovered Devices and Services to ISC Repository	4-78
Step 9: Create and Run a Collect Config Task for the Discovered Devices	4-79
Step 10: View and Edit Services	4-79

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	5-13

CHAPTER 6

Service Design 6-1

Policies	6-1
Templates	6-2
View Templates Tree and Data Pane	6-3
Create Folders and Subfolders	6-4
Copying Folders or Subfolders	6-4
Create Template	6-5
Copying Templates	6-13
Create Data File	6-13
Edit	6-18
Delete	6-20
List All SRs	6-21

Template Examples	6-22
Summary of Repository Variables	6-23
Importing and Exporting Templates	6-36

CHAPTER 7

Monitoring 7-1

Task Manager	7-1
Tasks	7-2
Starting Task Manager	7-2
Create	7-3
Audit	7-5
Details	7-6
Schedules	7-6
Logs	7-7
Delete	7-7
Task Logs	7-7
Ping	7-8
SLA	7-11
Setup Prior to Using SLA	7-12
Probes	7-12
Create Common Parameters	7-13
Create From Any SA Agent Device(s)	7-16
Create from MPLS CPE	7-18
Create From MPLS PE or MVRP-CE	7-22
Protocols	7-24
Details	7-30
Delete	7-31
Enable Probes	7-32
Enable Traps	7-33
Disable Probes	7-34
Disable Traps	7-35
Reports	7-36
Summary Report	7-36
HTTP Report	7-39
Jitter Report	7-39
Summary CoS Report	7-40
HTTP CoS Report	7-41
Jitter CoS Report	7-41
TE Performance Report	7-41

Reports	7-41
Introducing Reports	7-42
Accessing Reports	7-43
Using Reports GUI	7-43
Layout	7-43
Filters	7-43
Output Fields	7-44
Sorting	7-44
Running Reports	7-44
Using the Output from Reports	7-45
Exporting Reports	7-46
Printing Reports	7-46
E-mailing Reports	7-46
Invoking Help	7-47
Creating Custom Reports	7-47

CHAPTER 8

Diagnostics 8-1

CHAPTER 9

Administration 9-1

Security	9-1
Users	9-2
Details	9-3
Create	9-3
Copy	9-6
Edit	9-6
Delete	9-6
User Groups	9-7
Create	9-8
Edit	9-8
Delete	9-9
User Roles	9-9
Create	9-11
Copy	9-13
Edit	9-14
Delete	9-14
Object Groups	9-15
Create	9-16
Edit	9-17
Delete	9-17

User Roles Design Example	9-18
Example	9-18
Illustration of Setup	9-19
Steps to Set Up Example	9-20
Control Center	9-21
Hosts	9-21
Details	9-22
Config	9-23
Servers	9-24
Watchdog	9-25
Logs	9-26
Collection Zones	9-26
Licensing	9-28
Active Users	9-30
User Access Log	9-31
Manage TIBCO Rendezvous	9-33

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-7

APPENDIX B
ISC XML Reference B-1

APPENDIX C
Property Settings C-1

APPENDIX D
Template Usage D-1

How do I split a string?	D-1
How do I obtain address information from the given IP address?	D-2
How do I obtain the octets from the given IP address?	D-2
How do I call a subtemplate in a template?	D-2
How do I concatenate two strings?	D-3
How can I convert a string to an integer and how can I increase the last octet of the IP address by one?	D-3
Can I use nested if statements?	D-3
How can I perform basic arithmetic operations?	D-4
How can I retrieve data from a two-dimensional array and what is the use of \$velocityCount?	D-4

How can I print \$a instead of its value?	D-4
What is the difference between #include() and #parse()?	D-5
What is a macro and how is it used?	D-6
What is a range operator and how can I use it?	D-6
How can I split strings containing special characters?	D-7
How can I use repository variables?	D-7
How can I use a variable as a dynamic URL?	D-7
Can I see more examples?	D-7
Usage of Strings	D-8
Usage of a Macro	D-9
Usage of Subtemplates	D-10

GLOSSARY

INDEX



About This Guide

This preface defines the following:

- [Objective, page xv](#)
- [Related Documentation, page xv](#)
- [Audience, page xvi](#)
- [How This Book Is Organized, page xvii](#)
- [Obtaining Documentation and Submitting a Service Request, page xvii](#)

Objective

This guide provides details about the WatchDog commands and the 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, 5.0.1 can be accessed at:

http://www.cisco.com/en/US/products/sw/netmgts/ps4748/tsd_products_support_series_home.html



Tip

To cut and paste a two-line URL into the address field of your browser, you must cut and paste each line separately to get the entire URL without a break.

The following documents comprise the ISC 5.0.1 documentation set.

General documentation (in suggested reading order)

- *Cisco IP Solution Center Getting Started and Documentation Guide, 5.0.*
http://www.cisco.com/en/US/products/sw/netmgts/ps4748/products_documentation_roadmap09186a008081dd8e.html
- *Release Notes for Cisco IP Solution Center, 5.0.1.*
http://www.cisco.com/en/US/products/sw/netmgts/ps4748/prod_release_note09186a00809330fe.html

- *Cisco IP Solution Center Installation Guide, 5.0.*
http://www.cisco.com/en/US/products/sw/netmgtsw/ps4748/products_installation_guide_book09186a008081d37b.html
- *Cisco IP Solution Center Infrastructure Reference, 5.0.1.*
http://www.cisco.com/en/US/products/sw/netmgtsw/ps4748/products_technical_reference_book09186a00809353f3.html
- *Cisco IP Solution Center System Error Messages, 5.0.*
http://www.cisco.com/en/US/products/sw/netmgtsw/ps4748/products_system_message_guide_book09186a008081d383.html

Application and technology documentation (listed alphabetically)

- *Cisco IP Solution Center Metro Ethernet and L2VPN User Guide, 5.0.*
http://www.cisco.com/en/US/products/sw/netmgtsw/ps4748/products_user_guide_book09186a008081c7fb.html
- *Cisco IP Solution Center MPLS VPN User Guide, 5.0.1.*
http://www.cisco.com/en/US/products/sw/netmgtsw/ps4748/products_user_guide_book09186a0080932257.html
- *Cisco IP Solution Center Traffic Engineering Management User Guide, 5.0.*
http://www.cisco.com/en/US/products/sw/netmgtsw/ps4748/products_user_guide_book09186a008081d385.html
- *Cisco MPLS Diagnostics Expert 2.1 Failure Scenarios Guide on ISC 5.0.*
http://www.cisco.com/en/US/products/sw/netmgtsw/ps4748/products_technical_reference_book09186a008081d70d.html
- *Cisco MPLS Diagnostics Expert 2.1 User Guide on ISC 5.0.*
http://www.cisco.com/en/US/products/sw/netmgtsw/ps4748/products_user_guide_book09186a008081d364.html

API Documentation

- *Cisco IP Solution Center API Programmer Guide, 5.0.*
http://www.cisco.com/en/US/products/sw/netmgtsw/ps4748/products_programming_usage_guide_book09186a008081e909.html
- *Cisco IP Solution Center API Programmer Reference, 5.0.*
http://www.cisco.com/application/x-zip-compressed/en/us/guest/products/ps7229/c1667/ccmigration_09186a00808231b6.zip



Note

All documentation *might* be upgraded over time. All upgraded documentation will be available at the same URLs specified in this document.

Audience

This guide 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 guide 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 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.
- [Chapter 4, “Service Inventory—Discovery,”](#) explains the navigation path from the **Service Inventory** tab to **Discovery** and how to discover devices, connections, and services.
- [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, “Diagnostics,”](#) explains the **Diagnostics** tab and where to navigate for a full explanation.
- [Chapter 9, “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, “ISC XML Reference,”](#) explains XML files for Discovery.
- [Appendix C, “Property Settings,”](#) explains the Dynamic Component Properties Library (DCPL) properties, their defaults, and ranges and rules.
- [Appendix D, “Template Usage,”](#) gives questions and answers to help troubleshoot the Template Manager.
- [Glossary](#) explains terminology used in the ISC product.

Obtaining Documentation and Submitting a Service Request

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

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

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



CHAPTER 1

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 guide. It contains the following sections:

- [System Recommendations, page 1-1](#)
- [Introduction, page 1-1](#)
- [Structural Overview, page 1-2](#)
- [Service Inventory, page 1-10](#)
- [Service Design, page 1-12](#)
- [Monitoring, page 1-13](#)
- [Diagnostics, page 1-14](#)
- [Administration, page 1-15](#)

System Recommendations

The system recommendations and requirements are listed in Chapter 1, “System Recommendations” of the [Cisco IP Solution Center Installation Guide, 5.0](#) and the [Release Notes for Cisco IP Solution Center, 5.0.1](#). 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.

Introduction

Cisco IP Solution Center 5.0.1 (ISC 5.0.1) is a follow-on release to Cisco IP Solution Center 5.0 (ISC 5.0), with the changes listed in the [Release Notes for Cisco IP Solution Center, 5.0.1](#).

This guide lists many features that are common among multiple 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 and for other common features.

Before explaining the tabs in the Graphical User Interface (GUI), see the “[Structural Overview](#)” section on [page 1-2](#). It explains elements common to many windows in ISC.

The GUI is separated into the following large sections (tabs):

- “[Service Inventory](#)” section on [page 1-10](#)

- “Service Design” section on page 1-12
- “Monitoring” section on page 1-13
- “Diagnostics” section on page 1-14
- “Administration” section on page 1-15

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

Structural Overview

After you log in to 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 9](#), “Administration”(Administration > Security > User Roles). The choices shown in this guide 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 1-7

Product Category Tabs

The organization of this guide 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 1-10 and detailed information is given in [Chapter 3](#), “Service Inventory — Inventory and Connection Manager,” [Chapter 4](#), “Service Inventory—Discovery,” and [Chapter 5](#), “Service Inventory—Device Console.”
- **Service Design** An overview is given in the “Service Design” section on page 1-12 and detailed information is given in [Chapter 6](#), “Service Design.”
- **Monitoring** An overview is given in the “Monitoring” section on page 1-13 and detailed information is given in [Chapter 7](#), “Monitoring.”
- **Diagnostics** An overview is given in the “Diagnostics” section on page 1-14 and a pointer to detailed information is given in [Chapter 8](#), “Diagnostics.”
- **Administration** An overview is given in the “Administration” section on page 1-15 and detailed information is given in [Chapter 9](#), “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 1-6
- [About](#), page 1-6
- [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 choose day to day operations. In addition, by grouping these shortcuts together into folders, you can create work flows specific to your operating environment. To get more information about shortcuts, follow these 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... Set

Description:

Folder: New 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 list 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*

Index				
Service Inventory	Service Design	Monitoring	Diagnostics	Administration
<i>Inventory and Connection Manager</i> 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 Named Physical Circuits NPC Rings <i>Discovery</i> <i>Device Console</i>	<i>Policies</i> <i>Templates</i>	<i>Task Manager</i> Task Logs <i>Ping</i> <i>SLA</i> Probes Reports <i>TE Performance Report</i> <i>Reports</i>	<i>MPLS Diagnostics Expert</i> CE to CE PE to attached CE CE to PE across Core PE to PE (in VRF) PE to PE (Core)	<i>Security</i> Users User Groups User Roles Object Groups <i>Control Center</i> Collection Zones Licensing <i>Active Users</i> <i>User Access Log</i>

158177

Help

When you click **Help**, you receive a pointer to the documentation set:

http://www.cisco.com/en/US/products/sw/netmgts/ps4748/tsd_products_support_series_home.html

From that location, you can choose the type of ISC document you want to see.

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. To set the Customer Context, follow these steps:

- 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** Click the radio button for the customer for which you want information and click **Select**.
- 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](#)
- [Header Row Check Box, 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, Header Row Check Box, Rows per Page, and Changing Pages,”](#) you can click the drop-down list for categories, then in the **matching** field enter the search criteria, using * if you want to indicate anything is 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**.

Header Row Check Box

Many windows have a check box in the header row, where the column names exist, as shown in [Figure 1-6, Example of Filtering, Header Row Check Box, Rows per Page, and Changing Pages](#). If you check this check box, then all check boxes in the window are chosen.

Rows per Page

In the bottom left corner of many windows, as shown in [Figure 1-6, “Example of Filtering, Header Row Check Box, 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 list and you can select **5, 10, 20, 30, 40, 50, 100, 500, 1000, or 2500**.

Go To Page

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

Figure 1-6 Example of Filtering, Header Row Check Box, Rows per Page, and Changing Pages

Devices

ShowDevices with matching

Showing 1 - 8 of 8 records

#	☐	Device Name	Management IP Address	Type	Parent Device Name
1.	☐	pe1		Cisco IOS Device	
2.	☐	pe3		Cisco IOS Device	
3.	☐	sw2		Cisco IOS Device	
4.	☐	sw3		Cisco IOS Device	
5.	☐	sw4		Cisco IOS Device	
6.	☐	ce3		Cisco IOS Device	
7.	☐	ce8		Cisco IOS Device	
8.	☐	ce13		Cisco IOS Device	

Rows per page: Go to page: of 1

129048

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 check box causes the window 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 - 2 of 2 records

#	☐	Job ID	State	Type	Operation Type	Creator	Customer Name	Policy Name	Last Modified	Description
1.	☐	1	REQUESTED	MPLS	ADD	admin	Customer1	MPLSPolicy_PECE	10/27/05 5:25 PM	
2.	☐	2	REQUESTED	MPLS	ADD	admin	Customer1	MPLSPolicyNO_CE	10/27/05 5:25 PM	

Rows per page: Go to page: of 1

Auto Refresh: ☒

129049

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 - 10 of 11 records									
#	☐	Job ID	State	Type	Operation Type	Creator	Customer Name	Policy Name	Last Modified
1.	☐	3	PENDING	L2VPN	MODIFY	admin	Customer1	L2VpnPolicy1	9/15/05 2:23 PM
2.	☐	4	PENDING	QoS	ADD	admin	Customer1	3550-DSCP	9/15/05 2:23 PM
3.	☐	6	PENDING	VPLS	ADD	admin	Customer2	VPLSPolicy1	9/15/05 2:23 PM
4.	☐	13	DEPLOYED	L2VPN	ADD	admin	Customer1	L2vpnErsCe	9/15/05 2:15 PM
5.	☐	17	INVALID	L2VPN	ADD	admin	Customer1	L2vpnEwsCe	9/15/05 2:51 PM
6.	☐	18	DEPLOYED	L2VPN	ADD	admin	Customer3	L2vpnErsNoCe	9/15/05 3:02 PM
7.	☐	19	REQUESTED	L2VPN	ADD	admin	Customer1	L2vpnEwsNoCe	9/14/05 11:38 AM
8.	☐	22	REQUESTED	L2VPN	ADD	admin	Customer1	L2tpv3AtmCe	9/14/05 3:32 PM
9.	☐	25	REQUESTED	L2VPN	ADD	admin	Customer2	L2tpv3AtmNoCe	9/14/05 3:58 PM
10.	☐	26	REQUESTED	VPLS	ADD	admin	Customer1	VplsMplsErsCe	9/15/05 10:57 AM
Rows per page: 10 Go to page: 1 of 2 Go									
Auto Refresh: ☒ Create Details Status Edit Deploy Decommission Purge									

138470

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 3-3 in the [Topology Tool](#) section of [Chapter 3, “Service Inventory — Inventory and Connection Manager.”](#)

Figure 1-9 Devices—Icons



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,”](#) [Chapter 4, “Service Inventory—Discovery,”](#) 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.”](#)

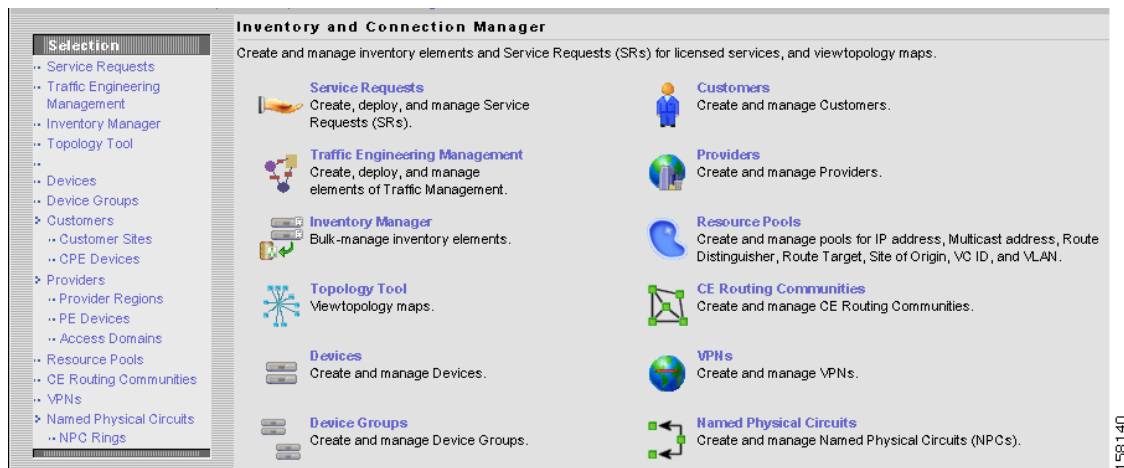
Figure 1-10 Service Inventory Selections

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 the *Cisco IP Solution Center Traffic Engineering Management User Guide, 5.0*).
- **Inventory Manager** Bulk-manage inventory elements.
- **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.
- **Named Physical Circuits** Create and manage Named Physical Circuits (NPCs).

Figure 1-11 Inventory and Connection Manager Selections

- **Discovery** Discover devices, connections, and services (explained in detail in [Chapter 4, “Service Inventory—Discovery”](#)).
- **Device Console** Download commands and configlets to devices and view device configuration (explained in detail in [Chapter 5, “Service Inventory—Device Console”](#)).

The functions with Device Console are as follows:

- **Download Commands**
- **Download Template**
- **Device Configuration Manager**
- **EXEC Commands**
- **Reload**

Service Design

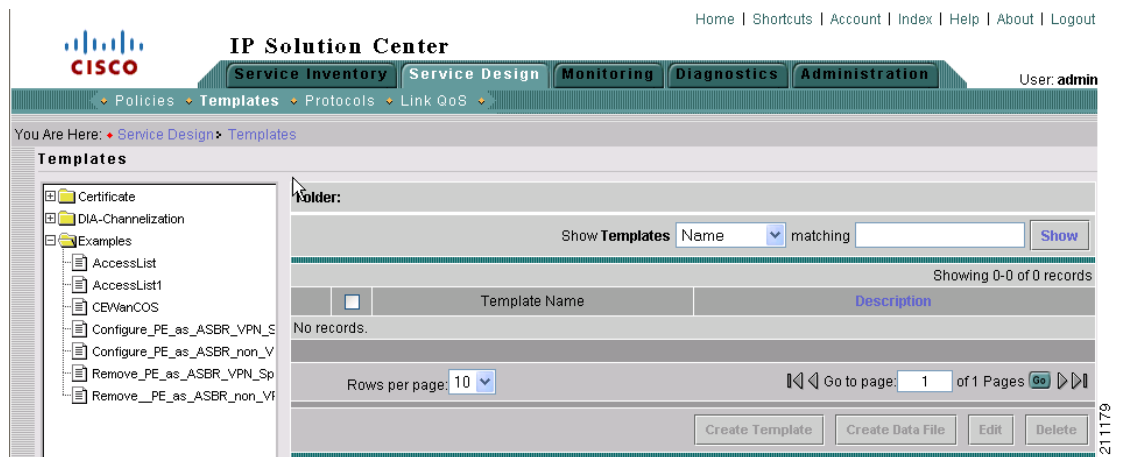
Service Design contains management tools for creating and managing policies and templates. This is explained in [Chapter 6, “Service Design.”](#)

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**

Monitoring

Monitoring contains tools to manage tasks, ping parameters, Service Level Agreement (SLA) probes, Traffic Engineering performance reports, and other 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 1-14](#), “[Monitoring Selections](#).”

Figure 1-14 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.
- **Reports** Create and schedule reports.

Diagnostics

Diagnostics contains automated troubleshooting and diagnostics for MPLS VPNs. This is explained in the [Cisco MPLS Diagnostics Expert 2.1 User Guide on ISC 5.0](#).

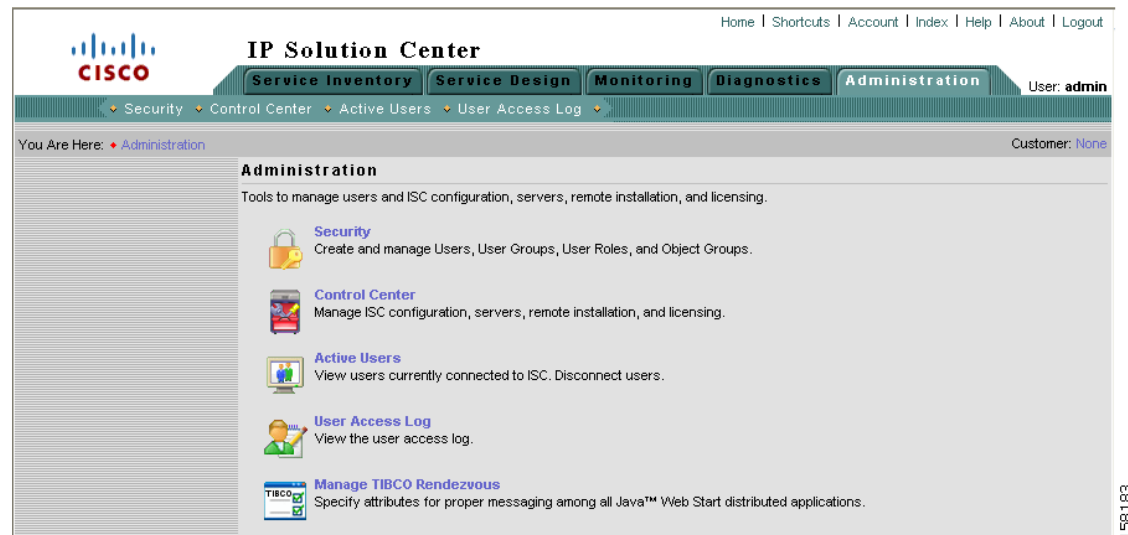
From the Home window you receive upon logging in, click the **Diagnostics** tab and you receive a window as shown in [Figure 1-15](#), “Diagnostics Selections.”

Figure 1-15 **Diagnostics Selections**

Administration

Administration contains tools to manage users, ISC configuration, servers, and licensing, to view users and the user access log, and to specify attributes for some messages. This is explained in detail in [Chapter 9, “Administration.”](#)

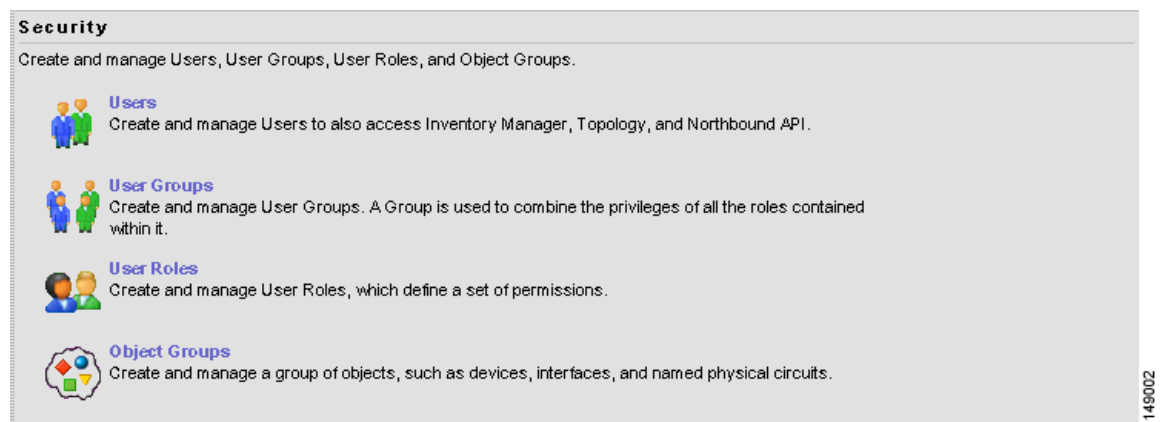
From the Home window you receive upon logging in, click the **Administration** tab and you receive a window as shown in [Figure 1-16, “Administration Selections.”](#)

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, and licensing. The following choices are shown in the left column of [Figure 1-18](#), “Control Center Selections”:
 - **Hosts**

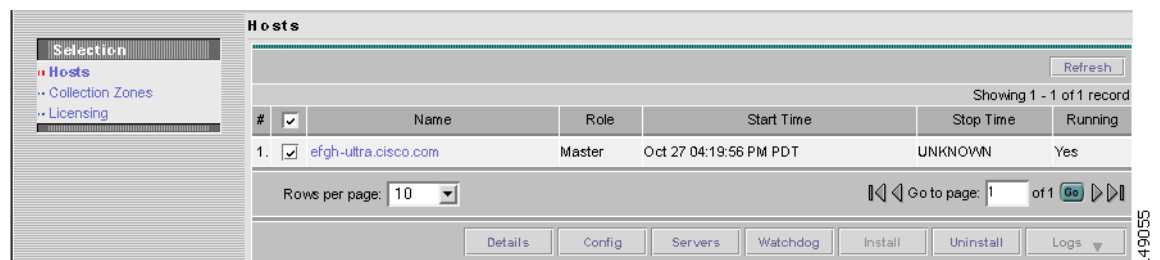


Note

If you want to do a **custom** install, this is only available through the Installation procedure explained in the [Cisco IP Solution Center Installation Guide, 5.0](#).

- **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.



CHAPTER 2

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 can be configured to automatically start any time the machine is rebooted.

In addition to the commands that are specified in this chapter, in the product you can choose **Admin > Control Center > Servers** and from there you can start, stop, restart, and view log files for the individual ISC servers.

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 **startdb** in the background. Do *not* enter **startdb &**.

startns Command

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

Description

The **startns** command starts the name server. The **orbd** process provides the name server functionality. **orbd** (from JDK) is required, but **startwd** starts it if it is not already running. The **startns** and **stopns** commands deal with **orbd**.

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.

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

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 a new version 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 database?” 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. The **startns** and **stopns** commands deal with **orbd**.

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 nameserver?” 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]

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 **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 2-6](#)
- [wdclient restart Subcommand, page 2-7](#)
- [wdclient start Subcommand, page 2-7](#)
- [wdclient status Subcommand, page 2-8](#)
 - [Information Produced: Name Column, page 2-8](#)
 - [Information Produced: State Column, page 2-9](#)
 - [Information Produced: Gen Column, page 2-9](#)
 - [Information Produced: Exec Time Column, page 2-9](#)
 - [Information Produced: PID Column, page 2-10](#)
 - [Information Produced: Success Column, page 2-10](#)
 - [Information Produced: Missed Column, page 2-10](#)
- [wdclient stop Subcommand, page 2-10](#)



Note

If you enter **wdclient -help**, you receive a listing of all the **wdclient** subcommands.

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 disk
```

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 group <group_name>
```

where:

<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 groups
```

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.

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 restart [**all** | *<server_name>* | **group** *<group_name>*]

where 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 start [**all** | *<server_name>* | **group** *<group_name>*]

where 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 2-8](#), “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 [-poll `<seconds>`] **status**

where:

-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.
dbpoller	Monitors database server.
discovery	Devices and Service Discovery Engine.
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.
rgserver	Executes various ISC traffic engineering computations, such as tunnel repairing.

Table 2-1 Servers and Their Functions (continued)

Server	Function
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.
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 stop [all | <server_name> | group <group_name>]
```

where 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.



CHAPTER 3

Service Inventory — Inventory and Connection Manager

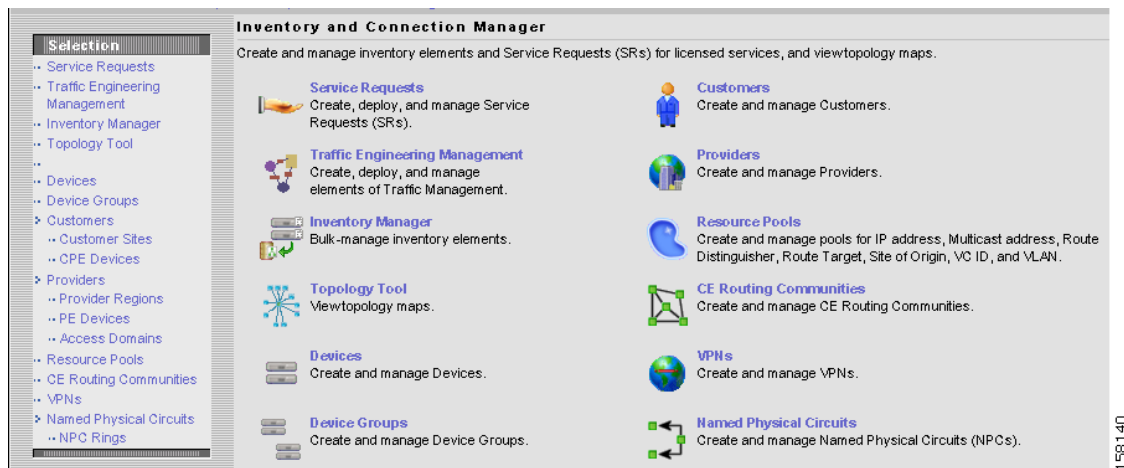
From the Home window of Cisco IP Solution Center (ISC), which appears upon logging in, click the **Service Inventory** tab and a window as shown in [Figure 3-1](#), “[Service Inventory Selections Window](#),” appears.

Figure 3-1 *Service Inventory Selections Window*



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

158178

Figure 3-2 *Inventory and Connection Manager Selections Window*

From the **Inventory and Connection Manager** window, you can choose any of the following functions:

- **Service Requests, page 3-2** 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 3-38** View topology maps.
- **Devices, page 3-71** Create and manage Devices.
- **Device Groups, page 3-105** Create and manage Device Groups.
- **Customers, page 3-111** Create and manage Customers.
- **Providers, page 3-119** Create and manage Providers.
- **Resource Pools, page 3-126** Create and manage pools for IP address, Multicast address, Route Distinguisher, Route Target, Site of Origin, VC ID, and VLAN.
- **CE Routing Communities, page 3-136** Create and manage CE Routing Communities.
- **VPNs, page 3-140** Create and manage VPNs.
- **Named Physical Circuits, page 3-144** Create and manage Named Physical Circuits (NPCs).

Service Requests

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

Figure 3-3, “Service Request States Transition Diagram,” shows a high-level diagram of the relationships and movement among ISC service request states.



Note

ISC service requests are processed in parallel, except when multiple service requests attempt to configure the same device. In this case, the service requests are processed sequentially (that is, only one write to the device can happen at a time).

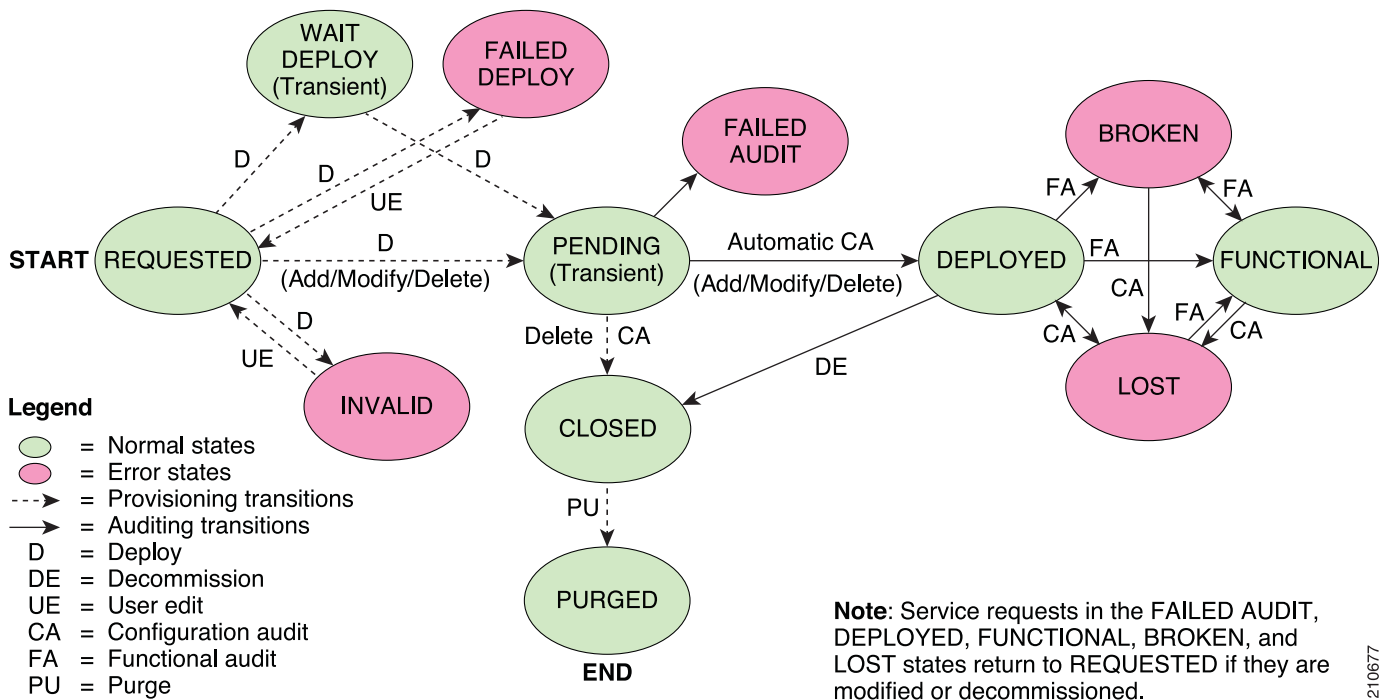
Figure 3-3 Service Request States Transition Diagram

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

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

Service Request State	Description
Broken (valid only for L2TPv3 and MPLS services)	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.
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.

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

Service Request State	Description
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 (valid only for L2TPv3 and MPLS services)	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.
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.

Table 3-2, “User Operations on ISC Service Requests,” describes user operations and their impact on ISC service requests.

Table 3-2 User Operations on ISC Service Requests

User Operations	Description
Decommission	This user operation removes the service from all devices in the service request.
Force Deploy	This user operation allows you to Deploy a service request from any state except Closed . This is equivalent to restarting the state diagram. The service request can move from its current state to any other possible state. However, it does not move to the Requested state.
Force Purge	This user operation removes a service request from the database irrespective of its state. If you Force Purge a service request from the ISC repository before first decommissioning the service request, the service remains running on the network (specifically, the configuration remains on the devices on which the service was provisioned), but all record of the service request that created the service is removed from ISC.
Purged	When a service request is Purged , it is removed from the ISC database.

Traffic Engineering Management

Traffic Engineering Management allows you to create, deploy, and manage elements of Traffic Engineering Management. This is explained in detail in the [Cisco IP Solution Center Traffic Engineering Management User Guide, 5.0](#).

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 from configuration files and configures CPEs and PEs by associating devices with a Customer or Provider.
- Edits devices, CPEs or PEs stored in the ISC repository.
- Assigns a device to a provider or customer.

Accessing the Inventory Manager Window

To access the Inventory Manager, follow these steps:

- Step 1** Choose **Service Inventory > Inventory and Connection Manager > Inventory Manager** to access the Inventory Manager window shown in [Figure 3-4](#).

Figure 3-4 *Inventory Manager Window*

The screenshot shows the 'Inventory Manager' window. At the top, it says 'General Attributes - Devices'. Below this is a search bar with the text 'Show entries with Host matching' followed by an asterisk in a text box and a 'Find' button. Below the search bar, it says 'Showing 0 of 0 records'. The main area is a table with the following columns: #, Host, Device Type, Description, Management IP Address, Device Domain Name, Terminal Session Protocol, Config Access Protocol, and Device Groups. Each column has a small square icon next to it. Below the table, there is a 'Rows per page' dropdown set to '10' and a 'Go to page: 1 of 1' with a 'Go' button. At the bottom right, there are two buttons: 'Import Devices' and 'Open'.

From the Inventory Manager window you can import devices or open a list of devices, providers or customers.

Importing Devices

To import a device, it must be in an existing directory on the same server that is running ISC. After a device is imported into the ISC repository, you can assign it to a customer or provider, if desired.

To import devices with configuration files, follow these steps:

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

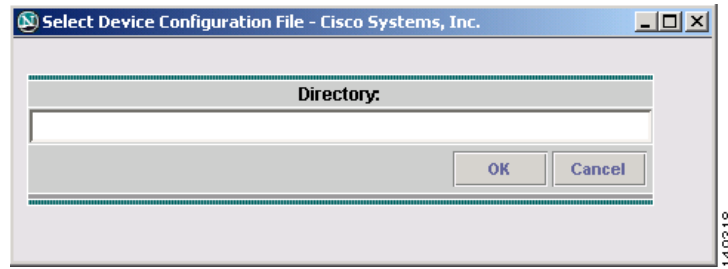
The Import Devices from Configuration Files window appears, as shown in [Figure 3-5](#).

Figure 3-5 *Import Devices from Configuration Files Window*

The screenshot shows the 'Import Devices from Configuration Files' window. It has a title bar with the same text. Below the title bar, it says 'Showing 0 of 0 records'. The main area is a table with the following columns: #, Configuration Files. Below the table, there is a 'Rows per page' dropdown set to '10' and a 'Go to page: 1 of 1' with a 'Go' button. At the bottom right, there are three buttons: 'Select', 'Import', and 'Cancel'.

- Step 3** Click the **Select** button.

The Select Device Configuration File dialog box appears, as shown in [Figure 3-6](#).

Figure 3-6 **Select Device Configuration File Dialog**

- Step 4** At the **Select Device Configuration File** dialog box, enter the directory on the ISC server where the configuration files reside.
- Step 5** The **Import Devices from Configuration Files** window appears.
- Step 6** Select as many of the configuration files as you want to import by checking the box to the left of the Configuration File name.
- Step 7** If you want to import devices from more than one directory, you can repeat Steps 3 through 6.
- Step 8** Click **Import**.
The **General Attributes** window appears with the added information.
- Step 9** Click **Save**.

Opening and Editing Devices

To open device configuration files to bulk edit, follow these steps:

- Step 1** Choose **Service Inventory > Inventory and Connection Manager > Inventory Manager**.
- Step 2** Click the **Open** button.

The **Open** drop-down list appears. The **Open** options include the following:

- **Devices**—Every network element that ISC manages.



Note To edit a PE, **Open Provider**, *not* **Open Devices**.

- **Provider**—PEs belonging to a specific provider.
- **Customer**—CEs belonging to a specific customer.

- Step 3** Select **Devices**.

The Select Device window appears, as shown in [Figure 3-7](#).

Figure 3-7 *Select Devices Window*

Showing 1 - 8 of 8 records

#	☐	Device Name	Management IP Address	Type	Parent Device Name
1.	☐	pe1		Cisco IOS Device	
2.	☐	pe3		Cisco IOS Device	
3.	☐	sw2		Cisco IOS Device	
4.	☐	sw3		Cisco IOS Device	
5.	☐	sw4		Cisco IOS Device	
6.	☐	ce3		Cisco IOS Device	
7.	☐	ce8		Cisco IOS Device	
8.	☐	ce13		Cisco IOS Device	

Rows per page: 10 Go to page: 1 of 1

Select Cancel

Step 4 Select a device to open by checking the check box to the left of the Device Name. You can select more than one device to open.

Step 5 Click the **Select** button.

The General Attributes window appears containing information on the selected devices, as shown in [Figure 3-8](#).

Figure 3-8 *General Attributes Devices Window*

Showing 1 - 3 of 3 records

#	☐	Host	Device Type	Description	Management IP Address	Device Domain Name	Terminal Session Protocol	Config Access Protocol	Device Groups
1.	☐	pe1	Cisco IOS Device				Default	Default	Device-Group-1
2.	☐	pe3	Cisco IOS Device				Default	Default	Device-Group-2
3.	☐	sw2	Cisco IOS Device				Default	Default	

Rows per page: 10 Go to page: 1 of 1

Attributes Assign CE/PE Edit Save

Step 6 To view specific attributes click the **Attributes** button.

The Attributes options appear, as shown in [Figure 3-9](#).

Figure 3-9 *Attributes Options Window*

Inventory Manager

General Attributes - Devices

Show entries with Host matching **Find**

Showing 1 - 3 of 3 records

#	☐	Host	Device Type	☐	Description	☐	Management IP Address	☐	Device Domain Name	☐	Terminal Session Protocol	☐	Config Access Protocol	☐	Device Groups
1.	☐	pe1	Cisco IOS Device								Default		Default		group1
2.	☐	pe3	Cisco IOS Device								Default		Default		
3.	☐	sw2	Cisco IOS Device								Default		Default		

Rows per page: 10

Go to page: 1 of 1

Attributes **Assign CE/PE** **Edit** **Save**

Step 7 Select the type of attribute to display.
See the following sections for descriptions of these attribute fields.

- [General Attributes Devices, page 3-9](#)
- [Password Attributes Devices, page 3-10](#)
- [SNMP Attributes Devices, page 3-11](#)
- [CNS Attributes Devices, page 3-12](#)
- [Platform Attributes Devices, page 3-13](#)
- [Interfaces Devices, page 3-14](#)

Step 8 To bulk edit an attribute, do the following:

- Check the one or more boxes to the left of the Device Name.
- Check the check box above the attribute name column.
- Click the **Edit** button.

Step 9 Enter the changes you want to make.

Step 10 Click **Save**.

The changes are saved.

General Attributes Devices

The General Attributes Devices window appears, as shown in [Figure 3-10](#).

Figure 3-10 General Attributes Devices Window

Inventory Manager

General Attributes - Devices

Show entries with Host matching

Showing 1 - 3 of 3 records

#	Host	Device Type	Description	Management IP Address	Device Domain Name	Terminal Session Protocol	Config Access Protocol	Device Groups
1.	pe1	Cisco IOS Device				Default	Default	Device-Group-1
2.	pe3	Cisco IOS Device				Default	Default	Device-Group-2
3.	sw2	Cisco IOS Device				Default	Default	

Rows per page:

The General Attributes Devices window contains the following:

- **Host**—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
 - IE2100 (Cisco CNS appliance)
- **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 IP 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.
- **Device 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.
- **Terminal Session Protocol**—Configures the method of communication between ISC and the device. Choices include: Telnet, Secure Shell (SSH), SSH version 2 (SSHv2), CNS, and RSH. Default: Telnet.
- **Config Access Protocol**—Administers the access protocol for config upload and download. Choices include: Terminal, TFTP, FTP, and RCP. Default: Terminal
- **Device Groups**—Lists the names of the Device Groups. You can add and modify Device Groups in this column.

Password Attributes Devices

The Password Attributes Devices window appears, as shown in [Figure 3-11](#).

Figure 3-11 Password Attributes Devices Window

Password Attributes

Password Attributes - Devices

Show entries with Host matching

Showing 1 - 3 of 3 records

#	☐ Device Name	☐ Login User	☐ Login Password	☐ Enable User	☐ Enable Password	☐ Community String RO	☐ Community String RW
1.	☐ pe1		*****		*****	public	private
2.	☐ pe3		*****		*****	public	private
3.	☐ sw2		*****		*****	public	private

Rows per page:

Go to page: of 1

149436

The Password Attributes Devices window contains the following:

- **Device 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.
- **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.
- **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.

SNMP Attributes Devices

The SNMP Attributes Devices window appears, as shown in [Figure 3-12](#).

Figure 3-12 *SNMP Attributes Devices Window*

The screenshot shows the 'SNMP Attributes - Devices' window. It features a search bar at the top with the text 'Show entries with Host matching' and a 'Find' button. Below the search bar, it indicates 'Showing 1 - 3 of 3 records'. The main area contains a table with the following columns: #, Device Name, SNMP Version, Security Level, Authentication User Name, Authentication Password, Authentication Algorithm, Encryption Password, and Encryption Algorithm. The table lists three devices: pe1, pe3, and sw2. Each device has 'Default' for SNMP Version and Security Level, and 'None' for Authentication Algorithm and Encryption Algorithm. The Authentication User Name and Authentication Password fields are empty. At the bottom, there is a 'Rows per page' dropdown set to 10, a 'Go to page' field set to 1 of 1, and buttons for 'Attributes', 'Assign CE/PE', 'Edit', and 'Save'.

#	Device Name	SNMP Version	Security Level	Authentication User Name	Authentication Password	Authentication Algorithm	Encryption Password	Encryption Algorithm
1.	pe1	Default	Default			None		None
2.	pe3	Default	Default			None		None
3.	sw2	Default	Default			None		None

The SNMP Attributes Devices window contains the following:

- **Device 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.
- **SNMP Version**—Choices include: SNMP v1/v2c, and SNMP v3. The default value is determined by the setting in the DCPL property SnmpService\defaultSNMPVersion. (See [Appendix C, “Property Settings”](#) for more details.)
- **Security Level**—Choices include: No Authentication/No Encryption, Authentication/No Encryption, and Authentication/Encryption. Default: No Authentication/No Encryption.
- **Authentication User Name**—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 Devices

The CNS Attributes Devices window appears, as shown in [Figure 3-13](#).

Figure 3-13 **CNS Attributes Devices Window**

The screenshot shows the 'CNS Attributes - Devices' window. It features a search bar at the top with the text 'Show entries with Host matching' and a 'Find' button. Below the search bar, it indicates 'Showing 1 - 3 of 3 records'. The main area contains a table with the following columns: #, Device Name, IE2100 Name, Device State, Event Identification, and CNS Identification. There are three rows of data: 1. pe1, None, Active, Host Name; 2. pe3, None, Active, Host Name; 3. sw2, None, Active, Host Name. At the bottom, there is a 'Rows per page' dropdown set to 10, a 'Go to page' field set to 1 of 1, and buttons for 'Attributes', 'Assign CE/PE', 'Edit', and 'Save'.

#	Device Name	IE2100 Name	Device State	Event Identification	CNS Identification
1.	pe1	None	Active	Host Name	
2.	pe3	None	Active	Host Name	
3.	sw2	None	Active	Host Name	

The CNS Attributes Devices window contains the following:

- **Device 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 Attributes Devices

The Platform Attributes Devices window appears, as shown in [Figure 3-14](#).

Figure 3-14 Platform Attributes Devices Window

Platform Attributes

Platform Attributes - Devices

Show entries with Host matching

Showing 1 - 3 of 3 records

#	Device Name	Platform	Software Version	Image Name	Serial Number
1.	pe1	7204VXR	12.2(16.6)S	16.6/c7200-p-mz.122-16.6.S	
2.	pe3	7204VXR	12.2(16.6)S	16.6/c7200-p-mz.122-16.6.S	
3.	sw2	WS-C3550-24	12.1(14)EA1	C3550-I9Q3L2-M:c3550-i9q3l2-mz.121-11.EA1/c3550-i9q3l2-mz.121-11.EA1.bin	

Rows per page:

The Platform Attributes Devices window contains the following:

- **Device 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 Version**—Should match what is configured on the target router device. Limited to 80 characters.
- **Image Name**—Should match what is configured on the target router device. Limited to 80 characters.
- **Serial Number**—Should match what is configured on the target router device. Limited to 80 characters.

Interfaces Devices

The Interfaces Devices window appears, as shown in [Figure 3-15](#).

Figure 3-15 *Interfaces Devices Window*

Interface Attributes

Interfaces - Devices

Show entries with Host matching

Showing 1 - 10 of 14 records

#	☐	Host	Interface Name	Interface Type	Interface Description	☐ Interface IP Address	Interface IPv6 Address	☐ Encapsulation	☐ Port Type
1.	☐	sw2	FastEthernet0/1	fastethernet					None
2.	☐	sw2	FastEthernet0/10	fastethernet					None
3.	☐	sw2	FastEthernet0/11	fastethernet					None
4.	☐	sw2	FastEthernet0/12	fastethernet					None
5.	☐	sw2	FastEthernet0/2	fastethernet	L11: Link to pe2				None
6.	☐	sw2	FastEthernet0/3	fastethernet	L14: Link to sw1				None
7.	☐	sw2	FastEthernet0/4	fastethernet					None
8.	☐	sw2	FastEthernet0/5	fastethernet					None
9.	☐	sw2	FastEthernet0/6	fastethernet					None
10.	☐	sw2	FastEthernet0/7	fastethernet					None

Rows per page: 10

The Interfaces Devices window contains the following:

- **Host**—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.
- **Interface 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. Limited to 256 characters.
- **Interface Type**—Specifies the type of interface. It is a display-only field.
- **Interface Description**—Description of the interface. This field is display-only. Field is populated by importing a configuration file.
- **Interface IP Address**—IPv4 address associated with this interface.
- **Interface IPv6 Address**—IPv6 address associated with this interface.
- **Encapsulation**—The Layer 2 Encapsulation for this device. It is a display-only field. Choices include:
 - DEFAULT
 - DOT1Q
 - ETHERNET
 - ISL
 - FRAME_RELAY
 - FRAME_RELAY_IETF
 - HDLC
 - PPP

- ATM
 - AAL5SNAP
 - AAL0
 - AAL5
 - AAL5MUX
 - AAL5NLPID
 - AAL2
 - ENCAP_QinQ
 - GRE
- **Port Type**—Choices include: Access, Trunk, Routed, and None.

Opening and Editing PEs

To open PE files to bulk edit, follow these steps:

Step 1 Choose **Service Inventory > Inventory and Connection Manager > Inventory Manager**.

Step 2 Click the **Open** button.

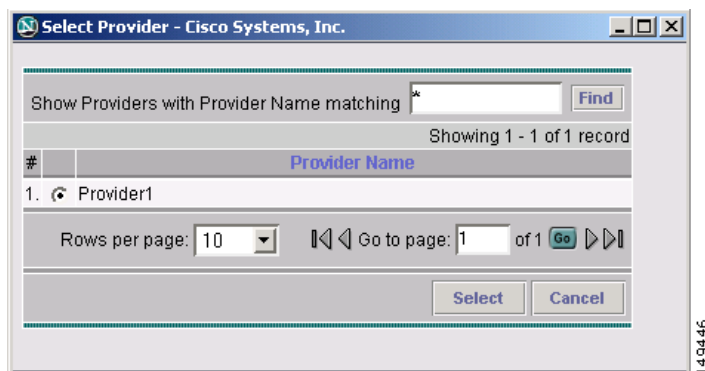
The **Open** drop-down list appears. The **Open** options include the following:

- **Devices**—Every network element that ISC manages.
- **Provider**—PEs belonging to a specific provider.
- **Customer**—CEs belonging to a specific customer.

Step 3 Select **Provider**.

The Select Provider window appears, as shown in [Figure 3-16](#).

Figure 3-16 *Select Provider Window*



Step 4 Select a provider by clicking the radio button to the left of the Provider Name.

Step 5 Click the **Select** button.

The General Attributes Provider window appears showing the PEs assigned to the selected provider, as shown in [Figure 3-17](#).

Figure 3-17 General Attributes Provider Window

Inventory Manager

General Attributes - PEs for Provider Provider1

Show entries with Host matching **Find**

Showing 1 - 5 of 5 records

#	☐	Host	Device Type	Description	Management IP Address	Device Domain Name	Terminal Session Protocol	Config Access Protocol	Device Groups
1.	☐	pe1	Cisco IOS Device				Default	Default	Device-Group-1
2.	☐	pe3	Cisco IOS Device				Default	Default	Device-Group-2
3.	☐	sw2	Cisco IOS Device				Default	Default	
4.	☐	sw3	Cisco IOS Device				Default	Default	Device-Group-1
5.	☐	sw4	Cisco IOS Device				Default	Default	Device-Group-2

Rows per page: 10 **Go to page:** 1 of 1 **Go**

Attributes **Edit** **Save**

149447

- Step 6** To view specific attributes click the **Attributes** button.
The Attributes options appear, as shown in [Figure 3-18](#).

Figure 3-18 Attributes Options Window

Inventory Manager

General Attributes - PEs for Provider Provider1

Show entries with Host matching **Find**

Showing 1 - 5 of 5 records

#	☐	Host	Device Type	Description	Management IP Address	Device Domain Name	Terminal Session Protocol	Config Access Protocol	Device Groups
1.	☐	pe1	Cisco IOS Device				Default	Default	group1
2.	☐	pe3	Cisco IOS Device				Default	Default	
3.	☐	sw2	Cisco IOS Device				Default	Default	
4.	☐	sw3	Cisco IOS Device				Default	Default	
5.	☐	sw4	Cisco IOS Device				Default	Default	

Rows per page: 10 **Go to page:** 1 of 1 **Go**

Attributes **Edit** **Save**

General Attributes
Password Attributes
SNMP Attributes
CNS Attributes
Platform Attributes
PE Attributes
Interfaces

158144

Step 7 Select the type of attribute to display.

See the following sections for descriptions of these attribute fields.

- [General Attributes Provider, page 3-18](#)
- [Password Attributes Provider, page 3-19](#)
- [SNMP Attributes Provider, page 3-21](#)
- [CNS Attributes Provider, page 3-22](#)
- [Platform Attributes Provider, page 3-23](#)
- [PE Attributes Provider, page 3-24](#)
- [Interfaces Provider, page 3-25](#)

Step 8 To bulk edit an attribute, do the following:

- Check the one or more boxes to the left of the Host or Device Name.
- Check the check box above the attribute name column.
- Click the **Edit** button.

Step 9 Enter the changes you want to make.

Step 10 Click **Save**.

The changes are saved.

General Attributes Provider

The General Attributes Provider window appears, as shown in [Figure 3-19](#).

Figure 3-19 General Attributes Provider Window

Inventory Manager

General Attributes - PEs for Provider Provider1

Show entries with Host matching **Find**

Showing 1 - 5 of 5 records

#	☐	Host	Device Type	☐ Description	☐ Management IP Address	☐ Device Domain Name	☐ Terminal Session Protocol	☐ Config Access Protocol	☐ Device Groups
1.	☐	pe1	Cisco IOS Device				Default	Default	Device-Group-1
2.	☐	pe3	Cisco IOS Device				Default	Default	Device-Group-2
3.	☐	sw2	Cisco IOS Device				Default	Default	
4.	☐	sw3	Cisco IOS Device				Default	Default	Device-Group-1
5.	☐	sw4	Cisco IOS Device				Default	Default	Device-Group-2

Rows per page: 10

Attributes

The General Attributes Provider window contains the following:

- **Host**—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
 - IE2100 (Cisco CNS appliance)
- **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 IP 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.
- **Device 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.
- **Terminal Session Protocol**—Configures the method of communication between ISC and the device. Choices include: Telnet, Secure Shell (SSH), SSH version 2 (SSHv2), CNS, and RSH. Default: Telnet.
- **Config Access Protocol**—Administers the access protocol for config upload and download. Choices include: Terminal, TFTP, FTP, and RCP. Default: Terminal
- **Device Groups**—Lists the names of the Device Groups. You can add and modify Device Groups in this column.

Password Attributes Provider

The Password Attributes Provider window appears, as shown in [Figure 3-20](#).

Figure 3-20 Password Attributes Provider Window

Password Attributes

Password Attributes - PEs for Provider Provider1

Show entries with Host matching *

Showing 1 - 5 of 5 records

#	☐ Device Name	☐ Login User	☐ Login Password	☐ Enable User	☐ Enable Password	☐ Community String RO	☐ Community String RW
1.	☐ pe1		*****		*****	public	private
2.	☐ pe3		*****		*****	public	private
3.	☐ sw2		*****		*****	public	private
4.	☐ sw3		*****		*****	public	private
5.	☐ sw4		*****		*****	public	private

Rows per page:

Go to page: of 1

149450

The Password Attributes Provider window contains the following:

- **Device 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.
- **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.
- **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.

SNMP Attributes Provider

The SNMP Attributes Provider window appears, as shown in [Figure 3-21](#).

Figure 3-21 *SNMP Attributes Provider Window*

The screenshot shows the 'SNMP Attributes' window. At the top, it says 'SNMP Attributes - PEs for Provider Provider1'. Below this is a search bar with the text 'Show entries with Host matching' and a 'Find' button. A status bar indicates 'Showing 1 - 5 of 5 records'. The main area is a table with the following columns: #, Device Name, SNMP Version, Security Level, Authentication User Name, Authentication Password, Authentication Algorithm, Encryption Password, and Encryption Algorithm. The table contains five rows of data for devices pe1, pe3, sw2, sw3, and sw4. At the bottom, there is a 'Rows per page' dropdown set to 10, a 'Go to page' field set to 1 of 1, and buttons for 'Attributes', 'Edit', and 'Save'.

#	Device Name	SNMP Version	Security Level	Authentication User Name	Authentication Password	Authentication Algorithm	Encryption Password	Encryption Algorithm
1.	pe1	Default	Default			None		None
2.	pe3	Default	Default			None		None
3.	sw2	Default	Default			None		None
4.	sw3	Default	Default			None		None
5.	sw4	Default	Default			None		None

The SNMP Attributes Provider window contains the following:

- **Device 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.
- **SNMP Version**—Choices include: SNMP v1/v2c, and SNMP v3. The default value is determined by the setting in the DCPL property SnmpService\defaultSNMPVersion. (See [Appendix C](#), “Property Settings” for more details.)
- **Security Level**—Choices include: No Authentication/No Encryption, Authentication/No Encryption, and Authentication/Encryption. Default: No Authentication/No Encryption.
- **Authentication User Name**—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 Provider

The CNS Attributes Provider window appears, as shown in [Figure 3-22](#).

Figure 3-22 CNS Attributes Provider Window

The screenshot shows the 'CNS Attributes' window for 'Provider1'. It features a search bar at the top right with the text 'Show entries with Host matching' and a 'Find' button. Below the search bar, it indicates 'Showing 1 - 5 of 5 records'. The main area contains a table with the following columns: '#', 'Device Name', 'IE2100 Name', 'Device State', 'Event Identification', and 'CNS Identification'. The table lists five devices: pe1, pe3, sw2, sw3, and sw4. Each device has a checkbox in the first column. The 'IE2100 Name' column shows 'None' for all devices. The 'Device State' column shows 'Active' for all devices. The 'Event Identification' column shows 'Host Name' for all devices. The 'CNS Identification' column is empty for all devices. At the bottom of the window, there is a 'Rows per page' dropdown set to '10', a 'Go to page' field set to '1 of 1', and three buttons: 'Attributes', 'Edit', and 'Save'.

#	Device Name	IE2100 Name	Device State	Event Identification	CNS Identification
1. ☐	pe1	None	Active	Host Name	
2. ☐	pe3	None	Active	Host Name	
3. ☐	sw2	None	Active	Host Name	
4. ☐	sw3	None	Active	Host Name	
5. ☐	sw4	None	Active	Host Name	

The CNS Attributes Provider window contains the following:

- **Device 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 Attributes Provider

The Platform Attributes Provider window appears, as shown in [Figure 3-23](#).

Figure 3-23 Platform Attributes Provider Window

Platform Attributes

Platform Attributes - PEs for Provider Provider1

Show entries with Host matching

Showing 1 - 5 of 5 records

#	Device Name	Platform	Software Version	Image Name	Serial Number
1.	☐ pe1	7204VXR	12.2(16.6)S	16.6/c7200-p-mz.122-16.6.S	
2.	☐ pe3	7204VXR	12.2(16.6)S	16.6/c7200-p-mz.122-16.6.S	
3.	☐ sw2	WS-C3550-24	12.1(14)EA1	C3550-I9Q3L2-M:c3550-i9q3l2-mz.121-11.EA1/c3550-i9q3l2-mz.121-11.EA1.bin	
4.	☐ sw3	WS-C3550-24	12.1(14)EA1	C3550-I9Q3L2-M:c3550-i9q3l2-mz.121-11.EA1/c3550-i9q3l2-mz.121-11.EA1.bin	
5.	☐ sw4	WS-C3550-24	12.1(14)EA1	C3550-I9Q3L2-M:c3550-i9q3l2-mz.121-11.EA1/c3550-i9q3l2-mz.121-11.EA1.bin	

Rows per page: 10

The Platform Provider window contains the following:

- **Device 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 Version**—Should match what is configured on the target router device. Limited to 80 characters.
- **Image Name**—Should match what is configured on the target router device. Limited to 80 characters.
- **Serial Number**—Should match what is configured on the target router device. Limited to 80 characters.

PE Attributes Provider

The PE Attributes Provider window appears, as shown in [Figure 3-24](#).

Figure 3-24 PE Attributes Provider Window

The screenshot shows the 'PE Attributes' window for 'Provider1'. It includes a search bar, a table with 5 records, and pagination controls. The table columns are: #, Device Name, Provider, Region*, Role, Loopback Interface, and Managed. The records are for devices pe1, pe3, sw2, sw3, and sw4, all associated with Provider1 and region_1. The 'Managed' column is checked for all records.

#	Device Name	Provider	Region*	Role	Loopback Interface	Managed
1.	pe1	Provider1	region_1	N-PE	: 10.8.0.101	Yes
2.	pe3	Provider1	region_1	N-PE	: 10.8.0.103	Yes
3.	sw2	Provider1	region_1	U-PE		Yes
4.	sw3	Provider1	region_1	U-PE		Yes
5.	sw4	Provider1	region_1	U-PE		Yes

Rows per page: 10 Go to page: 1 of 1

Note: * - Required Field

The PE Attributes Provider window contains the following:

- **Device 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**—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**—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: N-PE, U-PE, P, PE_AGG.
- **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.
- **Managed**—Provisioned by ISC. Check the check box for yes. Default is no.

Interfaces Provider

The Interfaces Provider window appears, as shown in [Figure 3-25](#).

Figure 3-25 *Interfaces Provider Window*

Interface Attributes

Interfaces - PEs for Provider Provider1

Show entries with Host matching *

Showing 1 - 10 of 75 records

#	☐	Host	Interface Name	Interface Type	Interface Description	☐ Interface IP Address	Interface IPv6 Address	☐ Encapsulation	☐ Port Type
1.	☐	pe1	ATM2/0	atm					None
2.	☐	pe1	ATM2/1	atm					None
3.	☐	pe1	ATM2/2	atm					None
4.	☐	pe1	ATM2/3	atm					None
5.	☐	pe1	Ethernet4/0	ethernet		172.29.146.21/26			None
6.	☐	pe1	Ethernet4/1	ethernet					None
7.	☐	pe1	Ethernet4/2	ethernet					None
8.	☐	pe1	Ethernet4/3	ethernet					None
9.	☐	pe1	Ethernet4/4	ethernet					None
10.	☐	pe1	FastEthernet0/0	fastethernet	L4: Link To sw3				None

Rows per page: 10

The Interfaces Provider window contains the following:

- **Host**—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.
- **Interface 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. Limited to 256 characters.
- **Interface Type**—Specifies the type of interface. It is a display-only field.
- **Interface Description**—Description of the interface. This field is display-only. Field is populated by importing a configuration file.
- **Interface IP Address**—IPv4 address associated with this interface.
- **Interface IPv6 Address**—IPv6 address associated with this interface.
- **Encapsulation**—The Layer 2 Encapsulation for this device. It is a display-only field. Choices include:
 - DEFAULT
 - DOT1Q
 - ETHERNET
 - ISL
 - FRAME_RELAY

- FRAME_RELAY_IETF
 - HDLC
 - PPP
 - ATM
 - AAL5SNAP
 - AAL0
 - AAL5
 - AAL5MUX
 - AAL5NLPID
 - AAL2
 - ENCAP_QinQ
 - GRE
- **Port Type**—Choices include: Access, Trunk, Routed, and None.

Opening and Editing CEs

To open CE files to bulk edit, follow these steps:

Step 1 Choose **Service Inventory > Inventory and Connection Manager > Inventory Manager**.

Step 2 Click the **Open** button.

The **Open** drop-down list appears. The **Open** options include the following:

- **Devices**—Every network element that ISC manages.
- **Provider**—PEs belonging to a specific provider.
- **Customer**—CEs belonging to a specific customer.

Step 3 Select **Customer**.

The Select Customer window appears, as shown in [Figure 3-26](#).

Figure 3-26 *Select Customer Window*

Select Customer - Cisco Systems, Inc.

Show Customers with Customer Name matching **Find**

Showing 1 - 2 of 2 records

#	Customer Name
1. ☒	Customer1
2. ☐	Customer2

Rows per page: 10 Go to page: 1 of 1 **Go**

Select **Cancel**

Step 4 Select a customer by clicking the radio button to the left of the Customer Name.

Step 5 Click the **Select** button.

The General Attributes Customer window appears showing the CEs assigned to the selected customer, as shown in [Figure 3-27](#).

Figure 3-27 *General Attributes Customer Window*

Inventory Manager

General Attributes - CEs for Customer Customer1

Show entries with Host matching **Find**

Showing 1 - 3 of 3 records

#	Host	Device Type	Description	Management IP Address	Device Domain Name	Terminal Session Protocol	Config Access Protocol	Device Groups
1. ☐	ce3	Cisco IOS Device				Default	Default	
2. ☐	ce8	Cisco IOS Device				Default	Default	Device-Group-1
3. ☐	ce13	Cisco IOS Device				Default	Default	Device-Group-2

Rows per page: 10 Go to page: 1 of 1 **Go**

Attributes **Edit** **Save**

Step 6 To view specific attributes click the **Attributes** button.

The Attributes options appear, as shown in [Figure 3-28](#).

Figure 3-28 Attributes Options Window

Inventory Manager

General Attributes - CEs for Customer Customer1

Show entries with Host matching * **Find**

Showing 1 - 3 of 3 records

#	☐	Host	Device Type	☐ Description	☐ Management IP Address	☐ Device Domain Name	☐ Terminal Session	☐ Config Access Protocol	☐ Device Groups
1.	☐	ce3	Cisco IOS Device					Default	
2.	☐	ce13	Cisco IOS Device					Default	
3.	☐	ce8	Cisco IOS Device					Default	

Rows per page: 10

1 of 1

General Attributes
Password Attributes
SNMP Attributes
CNS Attributes
Platform Attributes
CPE Attributes
Interfaces
Attributes **Edit** **Save**

158145

Step 7 Select the type of attribute to display.

See the following sections for descriptions of these attribute fields.

- [General Attributes Customer, page 3-29](#)
- [Password Attributes Customer, page 3-30](#)
- [SNMP Attributes Customer, page 3-31](#)
- [CNS Attributes Customer, page 3-32](#)
- [Platform Attributes Customer, page 3-33](#)
- [CPE Attributes Customer, page 3-34](#)
- [Interfaces Customer, page 3-35](#)

Step 8 To bulk edit an attribute, do the following:

- Check the one or more boxes to the left of the Host or Device Name.
- Check the check box above the attribute name column.
- Click the **Edit** button.

Step 9 Enter the changes you want to make.

Step 10 Click **Save**.

The changes are saved.

General Attributes Customer

The General Attributes Customer window appears, as shown in [Figure 3-29](#).

Figure 3-29 General Attributes Customer Window

#	Host	Device Type	Description	Management IP Address	Device Domain Name	Terminal Session Protocol	Config Access Protocol	Device Groups
1.	ce3	Cisco IOS Device				Default	Default	
2.	ce8	Cisco IOS Device				Default	Default	Device-Group-1
3.	ce13	Cisco IOS Device				Default	Default	Device-Group-2

The General Attributes Customer window contains the following:

- **Host**—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
 - IE2100 (Cisco CNS appliance)
- **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 IP 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.
- **Device 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.
- **Terminal Session Protocol**—Configures the method of communication between ISC and the device. Choices include: Telnet, Secure Shell (SSH), SSH version 2 (SSHv2), CNS, and RSH. Default: Telnet.
- **Config Access Protocol**—Administers the access protocol for config upload and download. Choices include: Terminal, TFTP, FTP, and RCP. Default: Terminal
- **Device Groups**—Lists the names of the Device Groups. You can add and modify Device Groups in this column.

Password Attributes Customer

The Password Attributes Customer window appears, as shown in [Figure 3-30](#).

Figure 3-30 Password Attributes Customer Window

The screenshot shows the 'Password Attributes' window for 'Customer 1'. It features a table with columns for Device Name, Login User, Login Password, Enable User, Enable Password, Community String RO, and Community String RW. The table contains three rows of data. Below the table, there are controls for rows per page (set to 10), a 'Go to page' field (set to 1 of 1), and buttons for 'Attributes', 'Edit', and 'Save'.

#	Device Name	Login User	Login Password	Enable User	Enable Password	Community String RO	Community String RW
1.	ce3		*****		*****	public	private
2.	ce8		*****		*****	public	private
3.	ce13		*****		*****	public	private

Rows per page: 10 Go to page: 1 of 1

Buttons: Attributes, Edit, Save

The Password Attributes Customer window contains the following:

- **Device 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.
- **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.
- **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.

SNMP Attributes Customer

The SNMP Attributes Customer window appears, as shown in [Figure 3-31](#).

Figure 3-31 *SNMP Attributes Customer Window*

SNMP Attributes

SNMP Attributes - CEs for Customer Customer1

Show entries with Host matching

Showing 1 - 3 of 3 records

#	Device Name	SNMP Version	Security Level	Authentication User Name	Authentication Password	Authentication Algorithm	Encryption Password	Encryption Algorithm
1.	ce3	Default	Default			None		None
2.	ce8	Default	Default			None		None
3.	ce13	Default	Default			None		None

Rows per page: 10

149337

The SNMP Attributes Customer window contains the following:

- **Device 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.
- **SNMP Version**—Choices include: SNMP v1/v2c, and SNMP v3. The default value is determined by the setting in the DCPL property `SnmpService\defaultSNMPVersion`. (See [Appendix C](#), “Property Settings” for more details.)
- **Security Level**—Choices include: No Authentication/No Encryption, Authentication/No Encryption, and Authentication/Encryption. Default: No Authentication/No Encryption.
- **Authentication User Name**—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 Customer

The CNS Attributes Customer window appears, as shown in [Figure 3-32](#).

Figure 3-32 CNS Attributes Customer Window

The screenshot shows the 'CNS Attributes' window for 'Customer Customer1'. It features a search bar with the text 'Show entries with Host matching' and a 'Find' button. Below the search bar, it indicates 'Showing 1 - 3 of 3 records'. The main table has the following columns: #, Device Name, IE2100 Name, Device State, Event Identification, and CNS Identification. The table contains three rows of data:

#	Device Name	IE2100 Name	Device State	Event Identification	CNS Identification
1.	☐ ce3	None	Active	Host Name	
2.	☐ ce8	None	Active	Host Name	
3.	☐ ce13	None	Active	Host Name	

At the bottom of the window, there is a 'Rows per page' dropdown set to 10, a 'Go to page' field with '1' of '1', and buttons for 'Attributes', 'Edit', and 'Save'. A vertical label '149313' is visible on the right side of the window.

The CNS Attributes Customer window contains the following:

- **Device 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 Attributes Customer

The Platform Attributes Customer window appears, as shown in [Figure 3-33](#).

Figure 3-33 Platform Attributes Customer Window

The screenshot shows the 'Platform Attributes' window for 'Customer 1'. It displays a table of records for CE devices. The table has columns for Device Name, Platform, Software Version, Image Name, and Serial Number. There are three records listed. Below the table, there are controls for rows per page (set to 10) and a 'Go to page' field (set to 1 of 1). At the bottom right, there are buttons for 'Attributes', 'Edit', and 'Save'.

#	Device Name	Platform	Software Version	Image Name	Serial Number
1.	ce3	2621	12.2(5d)	C2600-JS-M:c2600-js-mz.122-16.6	
2.	ce8	2621	12.2(5d)	C2600-JS-M:c2600-js-mz.122-16.6	
3.	ce13	2621	12.2(5d)	C2600-JS-M:c2600-js-mz.122-16.6	

Rows per page: 10 Go to page: 1 of 1

Buttons: Attributes, Edit, Save

The Platform Customer window contains the following:

- **Device 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 Version**—Should match what is configured on the target router device. Limited to 80 characters.
- **Image Name**—Should match what is configured on the target router device. Limited to 80 characters.
- **Serial Number**—Should match what is configured on the target router device. Limited to 80 characters.

CPE Attributes Customer

The CPE Attributes Customer window appears, as shown in [Figure 3-34](#).

Figure 3-34 CPE Attributes Customer Window

The screenshot shows the 'CPE Attributes' window for 'Customer Customer1'. It features a search bar with a 'Find' button and a table of records. The table has columns for '#', 'Device Name', 'Customer', 'Site*', and 'Management Type'. There are three records listed, all with 'Managed' management type. At the bottom, there are controls for rows per page (set to 10), a 'Go to page' field (set to 1 of 1), and buttons for 'Attributes', 'Edit', and 'Save'. A note at the bottom left states '* - Required Field'.

#	Device Name	Customer	Site*	Management Type
1.	ce3	Customer1	east	Managed
2.	ce8	Customer1	east	Managed
3.	ce13	Customer1	east	Managed

Rows per page: 10 Go to page: 1 of 1

Note: * - Required Field

The CPE Attributes Customer window contains the following:

- **Device 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**—Lists the names of customers. 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 customer name.
- **Site**—Lists the names of sites. 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 site name.
- **Management Type**—Choices include: Managed, Unmanaged, Managed - Management LAN, Unmanaged - Management LAN, Directly Connected, Directly Connected Management Host, Multi-VRF, and Unmanaged Multi-VRF.

Interfaces Customer

The Interfaces Customer window appears, as shown in [Figure 3-35](#).

Figure 3-35 *Interfaces Customer Window*

The screenshot shows the 'Interfaces - CEs for Customer Customer1' window. It features a search bar with the text 'Show entries with Host matching *' and a 'Find' button. Below the search bar, it indicates 'Showing 1 - 10 of 20 records'. The main table has columns: #, Host, Interface Name, Interface Type, Interface Description, Interface IP Address, Interface IPv6 Address, Encapsulation, and Port Type. The table lists 10 records for host 'ce3', including ATM and Ethernet interfaces. At the bottom, there is a 'Rows per page' dropdown set to 10, a 'Go to page' field set to 1 of 2, and buttons for 'Attributes', 'Edit', and 'Save'.

#	Host	Interface Name	Interface Type	Interface Description	Interface IP Address	Interface IPv6 Address	Encapsulation	Port Type
1.	ce3	ATM1/0	atm					None
2.	ce3	ATM1/1	atm					None
3.	ce3	ATM1/2	atm					None
4.	ce3	Ethernet0/0	ethernet		172.29.146.26/26			None
5.	ce3	Ethernet0/1	ethernet					None
6.	ce3	Ethernet0/2	ethernet					None
7.	ce3	Ethernet0/3	ethernet					None
8.	ce3	Ethernet0/4	ethernet					None
9.	ce3	Serial1/0	serial					None
10.	ce3	Serial1/1	serial					None

The Interfaces Customer window contains the following:

- **Host**—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.
- **Interface 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. Limited to 256 characters.
- **Interface Type**—Specifies the type of interface. It is a display-only field.
- **Interface Description**—Description of the interface. This field is display-only. Field is populated by importing a configuration file.
- **Interface IP Address**—IPv4 address associated with this interface.
- **Interface IPv6 Address**—IPv6 address associated with this interface.
- **Encapsulation**—The Layer 2 Encapsulation for this device. It is a display-only field. Choices include:
 - DEFAULT
 - DOT1Q
 - ETHERNET
 - ISL
 - FRAME_RELAY

- FRAME_RELAY_IETF
 - HDLC
 - PPP
 - ATM
 - AAL5SNAP
 - AAL0
 - AAL5
 - AAL5MUX
 - AAL5NLPID
 - AAL2
 - ENCAP_QinQ
 - GRE
- **Port Type**—Choices include: Access, Trunk, Routed, and None.

Assigning Devices

To assign a device to a provider or customer, follow these steps:

Step 1 Choose **Service Inventory > Inventory and Connection Manager > Inventory Manager**.

Step 2 Click the **Open** button.

The **Open** drop-down list appears, as shown in [Figure 3-37](#).

Figure 3-36 Open Options Window

Inventory Manager

General Attributes - Devices

Show entries with Host matching

Showing 0 of 0 records

#	Host	Device Type	Description	Management IP Address	Device Domain Name	Terminal Session Protocol	Config Access Protocol	Device Groups
Showing 0 of 0 records								

Rows per page:

Go to page: of 1

Open Options Window

- Devices
- Provider
- Customer

Step 3 Select **Devices**.

The Select Device window appears, as shown in [Figure 3-37](#).

Figure 3-37 *Select Devices Window*

Select Device(s) - Cisco Systems, Inc.

Show Devices with matching

Showing 1 - 8 of 8 records

#	☐	Device Name	Management IP Address	Type	Parent Device Name
1.	☐	pe1		Cisco IOS Device	
2.	☐	pe3		Cisco IOS Device	
3.	☐	sw2		Cisco IOS Device	
4.	☐	sw3		Cisco IOS Device	
5.	☐	sw4		Cisco IOS Device	
6.	☐	ce3		Cisco IOS Device	
7.	☐	ce8		Cisco IOS Device	
8.	☐	ce13		Cisco IOS Device	

Rows per page: Go to page: of 1

Step 4 Select a device to open by checking the box to the left of the Device Name. You can select more than one device to open.

Step 5 Click the **Select** button.

The General Attributes Devices window appears containing information on the selected devices, as shown in [Figure 3-38](#).

Figure 3-38 *General Attributes Devices Window*

Inventory Manager

General Attributes - Devices

Show entries with Host matching

Showing 1 - 3 of 3 records

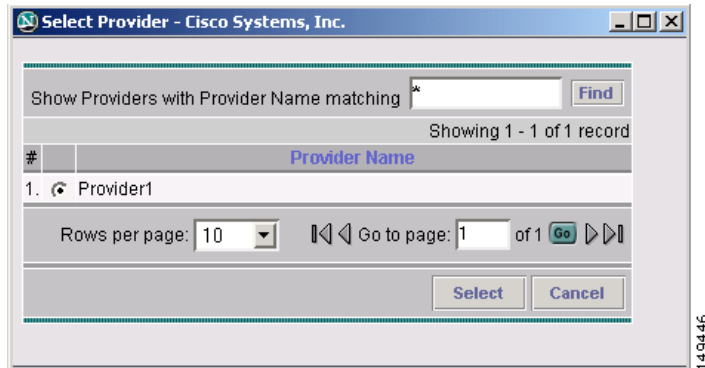
#	☐	Host	Device Type	Description	Management IP Address	Device Domain Name	Terminal Session Protocol	Config Access Protocol	Device Groups
1.	☐	pe1	Cisco IOS Device				Default	Default	Device-Group-1
2.	☐	pe3	Cisco IOS Device				Default	Default	Device-Group-2
3.	☐	sw2	Cisco IOS Device				Default	Default	

Rows per page: Go to page: of 1

Step 6 Click the **Assign CE/PE** button.

Step 7 Select **Customer** or **Provider**.

The corresponding **Select Customer** or **Select Provider** window appears, as shown in [Figure 3-39](#).

Figure 3-39 *Select Provider Window*

- Step 8** Select the customer or provider to which you want to assign the device by checking the box to the left of the Customer or Provider Name.
- Step 9** Click the **Select** button.
- If you assigned the device to a provider, the PE Attributes window appears. If you assigned the device to a customer, the CPE Attributes window appears.
- Step 10** In order to save the assigned devices to the ISC repository, you must specify the Site in the CPE Attributes window or the Region in the PE Attributes window. Do the following:
- Check the one or more boxes to the left of the Device Name.
 - Check the check box above the **Site** or **Region** column.
 - Click the **Edit** button. The **Edit Attributes** window appears.
 - Click **Select**. The **Select Site** or **Select Region** window appears.
 - Select a site or region by checking the box to the left of the Site Name or Region Name.
 - Click Save.
- Step 11** You can choose to edit attributes as desired. Enter any changes you want to make.
- Step 12** Click **Save**.
- The PE or CPE is saved to the ISC repository.

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 3-39](#)
- [Launching Topology Tool, page 3-39](#)
- [Conventions, page 3-41](#)
- [Accessing the Topology Tool for ISC-VPN Topology, page 3-44](#)
- [Types of Views, page 3-46](#)
 - [VPN View, page 3-47](#)

- [Logical View, page 3-52](#)
 - [Physical View, page 3-55](#)
- [Viewing Device and Link Properties, page 3-56](#)
- [Filtering and Searching, page 3-63](#)
 - [Filtering, page 3-63](#)
 - [Searching, page 3-66](#)
- [Using Maps, page 3-67](#)
 - [Loading a map, page 3-68](#)
 - [Layers, page 3-69](#)
 - [Map data, page 3-70](#)
 - [Node locations, page 3-70](#)
 - [Adding new maps, page 3-71](#)

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:

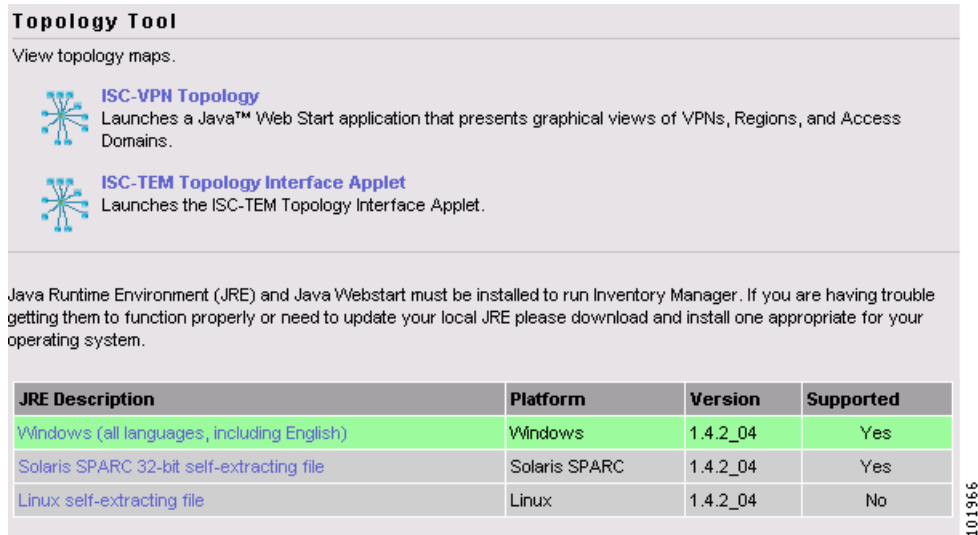
- Filtering and Searching—filter out unnecessary detail in large graphs or jump straight to a particular device using the search tool
- Using Maps—associate maps with the individual views.

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 in to ISC.
Step 2	Choose Service Inventory > Inventory and Connection Manager > Topology Tool and a window appears, as shown in Figure 3-40 , “ Topology Launch Window .” 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 go back to the Topology Tool page.

Figure 3-40 **Topology Launch Window**

- Step 3** Click **ISC-VPN Topology** in [Figure 3-40](#), “Topology Launch Window” to launch the Topology Tool application on the web client. This starts up the Java Web Start application.

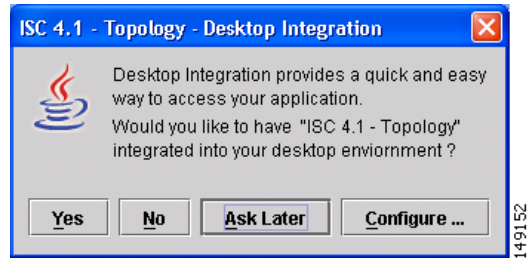
**Note**

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.

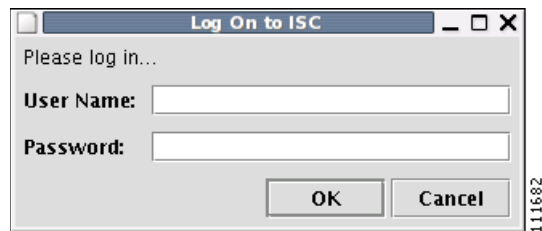
- Step 4** The first time Inventory Manager is activated, the Security Warning window in [Figure 3-41](#) appears. Click **Start** to proceed or **Details** to verify the security certificate.

Figure 3-41 **Security Warning Window**

- Step 5** The Desktop Integration window in [Figure 3-42](#) 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 3-42 *Topology Desktop Integration Window*

The Login window in [Figure 3-43](#), “[Log In to ISC Window](#).” appears whether or not a selection has been made in the Desktop Integration window.

Figure 3-43 *Log In to ISC Window*

- 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 3-3](#).

Table 3-3 **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)
 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
 device-1.domian.com Provider Name Region 1 Name 177.0.0.1 Description of device-1 N-PE 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 N-PE 111688	Blue icon for a router provider device followed by the following information: - Device name - Provider Name - Region Name - Management IP Address - Description - Role

Table 3-3 *Device Role Shapes (continued)*

Shape	Description
	Blue icon for a region followed by the following information: - Region name - Provider Name
	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)
	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 3-4](#):

Table 3-4 *Link Type Color Scheme*

Color	Connection Type
 (green)	End-to-end wire
 (purple)	Attachment circuit
 (brown)	MPLS VPN link

Finally, the four patterns shown in [Table 3-5](#) are used to indicate the service request state:

Table 3-5 *Link State Pattern Scheme*

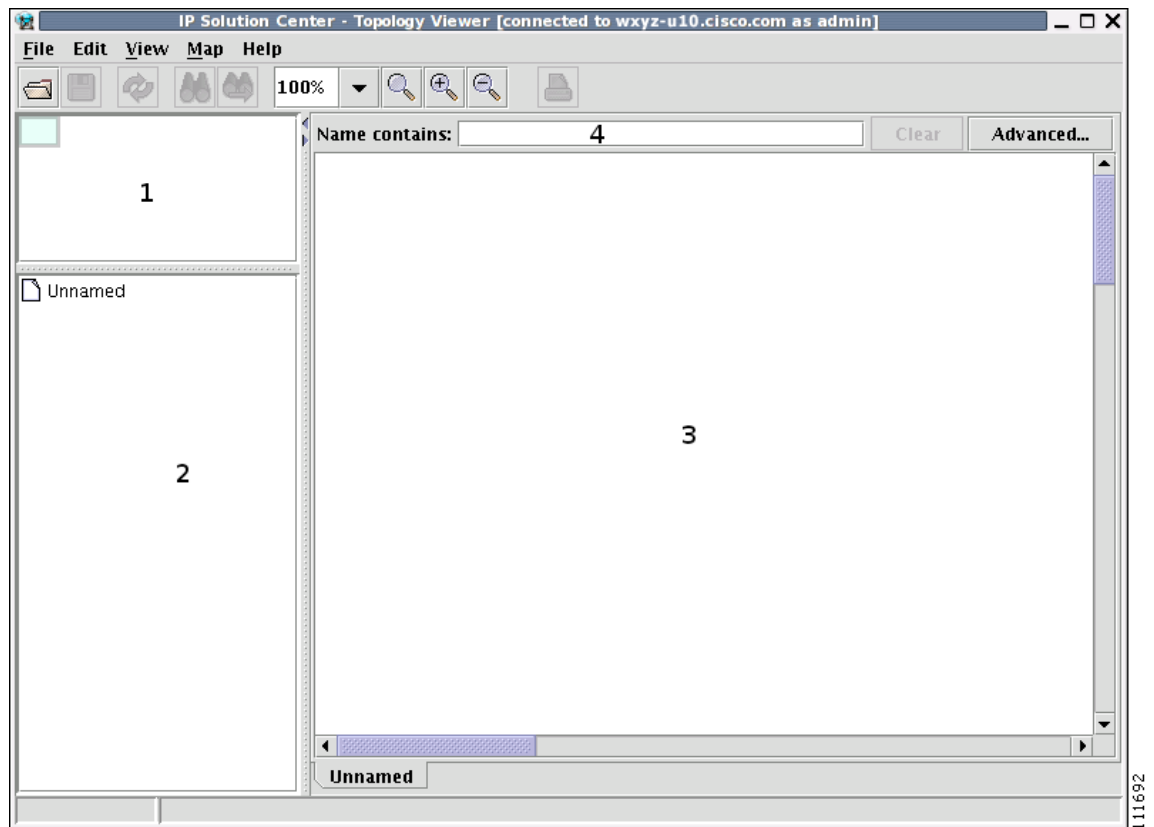
Pattern	Service Request State
	Deployed, functional, pending
	Failed audit, invalid, broken, lost
	Wait deploy, requested, failed deploy
	Closed

Accessing the Topology Tool for ISC-VPN Topology

Launch the Topology Tool as explained in [Figure 3-40](#), “[Topology Launch Window](#),” in the “[Launching Topology Tool](#)” section on [page 3-39](#) and then use the following steps to access the **ISC-VPN Topology** tool.

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

The Topology window shown in [Figure 3-44](#) appears.

Figure 3-44 **Topology Application Window**

The application window is divided into four areas, as shown in [Figure 3-44](#):

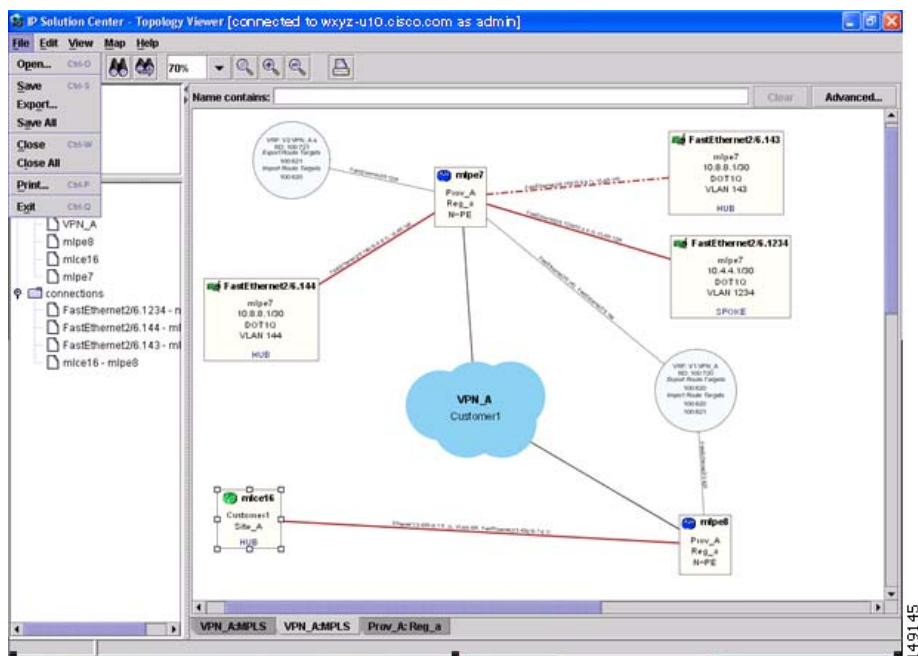
- area (1)—The top left corner shows the Overview area. The colored rectangular panel, called the panner, corresponds to the area currently visible in the main area. Moving the panner around changes the part of the graph showing in the main area. This is particularly useful for large graphs.
- area (2)—The 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 3-66](#) and the “[Filtering](#)” section on [page 3-63](#).



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 3-45](#).

Figure 3-45 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.

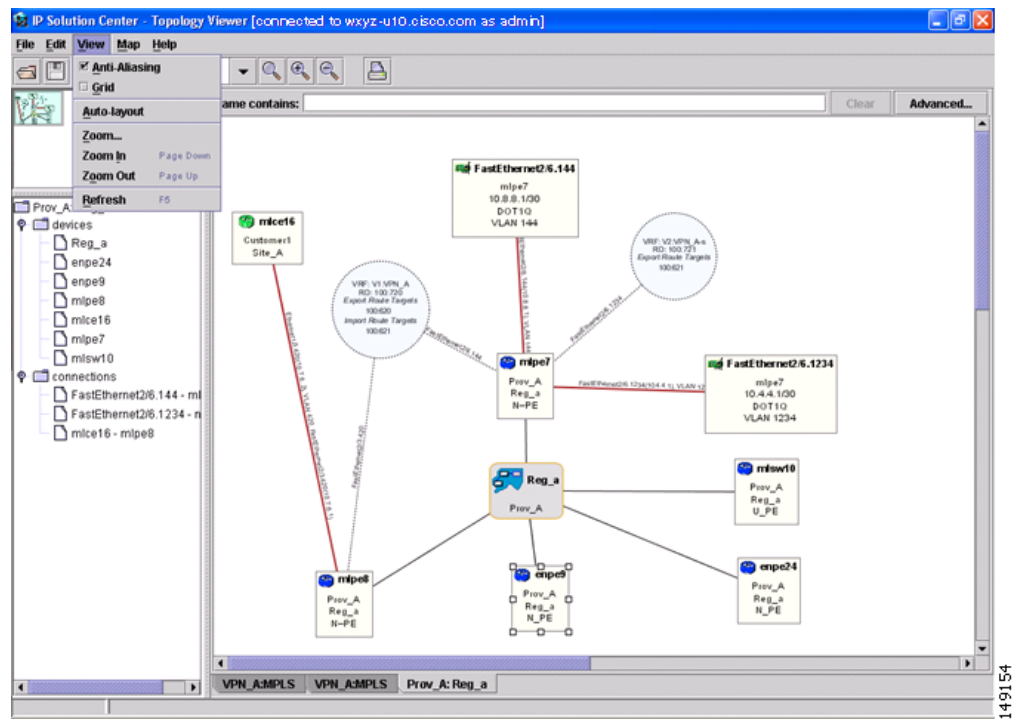
Types of Views

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

- **VPN View**, page 3-47, shows connectivity between devices in a VPN
- **Logical View**, page 3-52, shows connectivity between PEs and CPEs in a region
- **Physical View**, page 3-55, shows physical devices and links for PEs in a region.

The view attributes can be changed using the **View** menu, as shown in Figure 3-46.

Figure 3-46 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

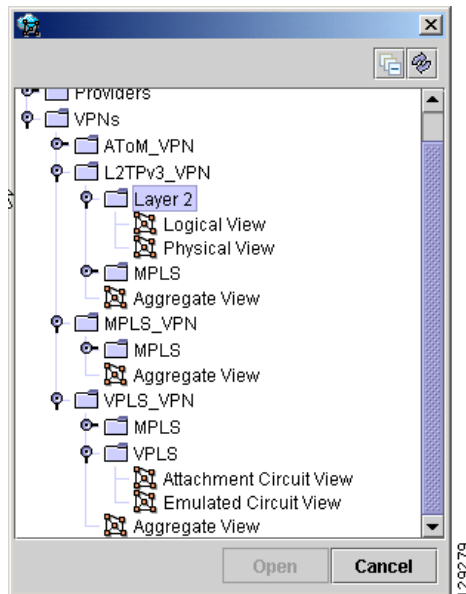
The VPN view shows connectivity between devices forming a given VPN. To activate the VPN view, follow these steps:

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

or

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

The Folder View window in [Figure 3-47](#) appears displaying a directory tree with available VPNs.

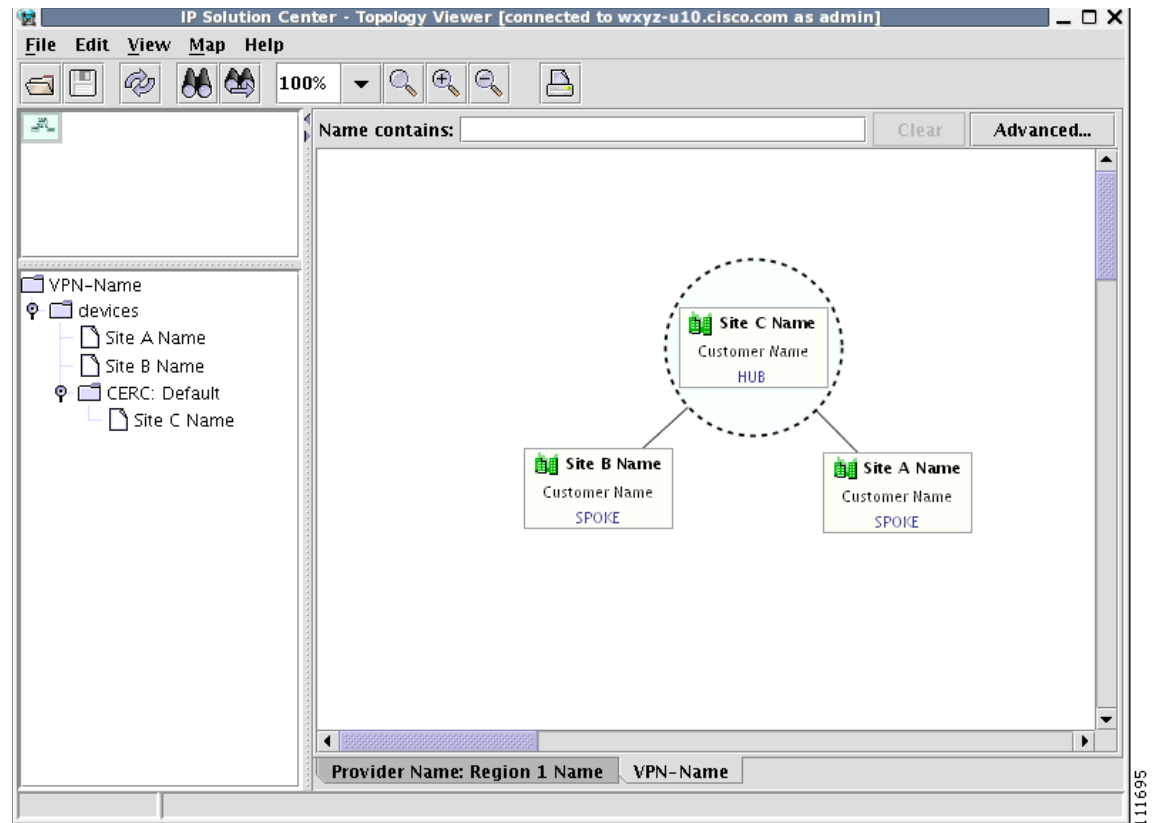
Figure 3-47 Folder View Window

- Step 2** Choose 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 3-48](#), “[Aggregate View](#),” shows connectivity between all customer devices, regardless of the type of technology used to connect them.

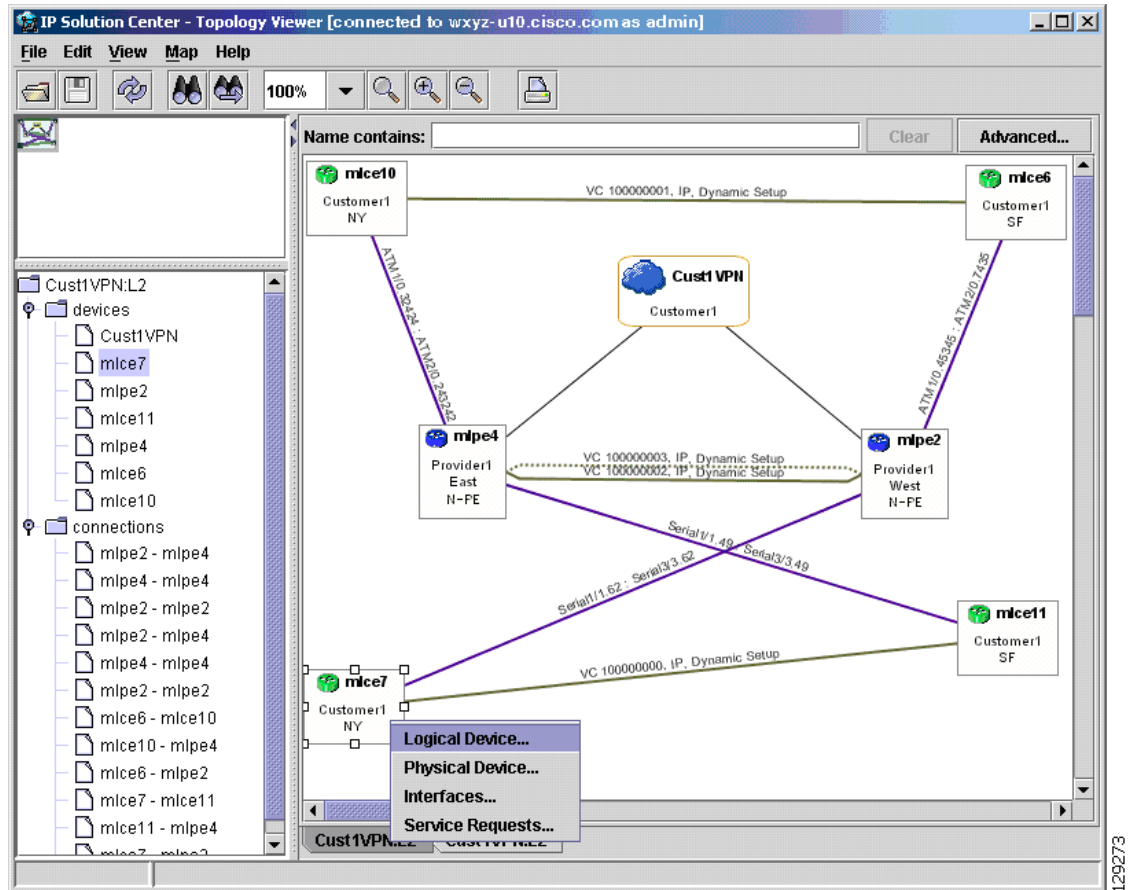
A single view might show a combination of MPLS, Layer 2, and VPLS. For MPLS, only the Customer Premises Equipment devices (CPEs) are shown.

Figure 3-48 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.

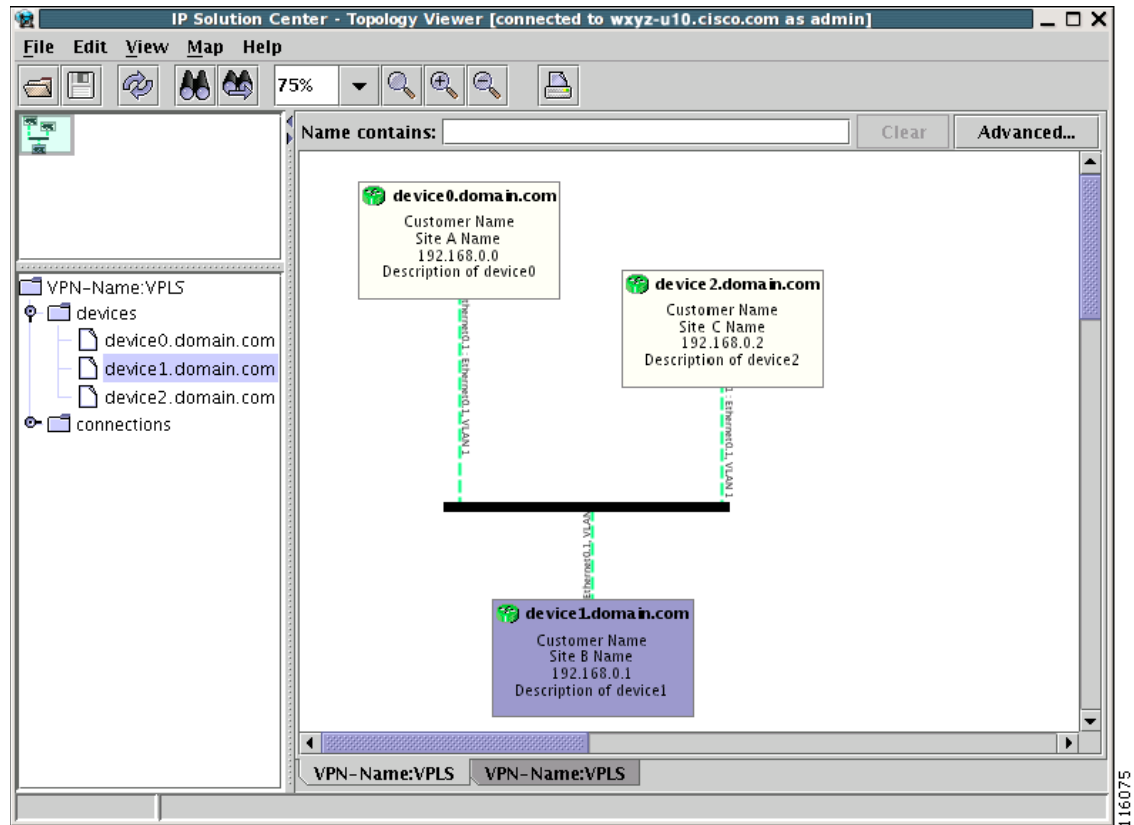
In MPLS Layer 2 VPN, the topology displays Virtual Circuit (VC) with MPLS core (as MPLS string) but with L2TPv3, the topology will display Virtual Circuit (VC) with IP core (as IP string) as shown in [Figure 3-49](#).

Figure 3-49 Virtual Circuit with IP Core



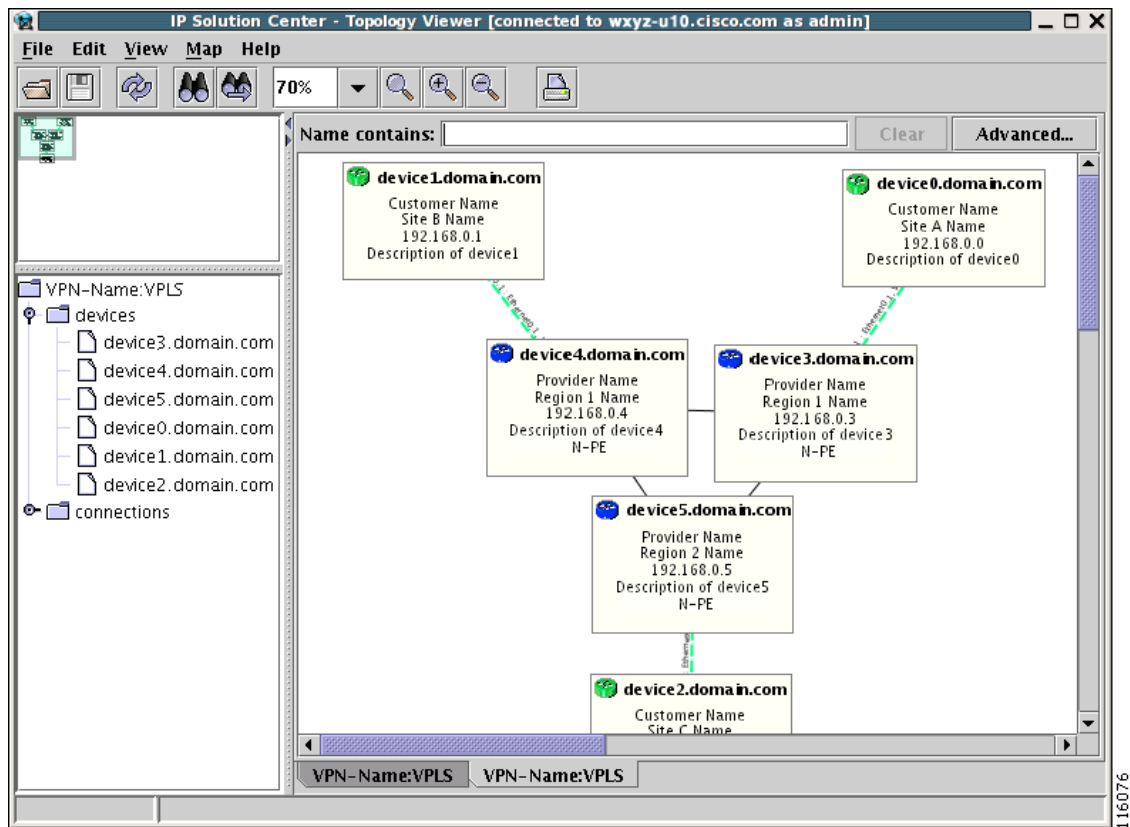
VPLS Topology

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 3-50, “Attachment Circuit View.”

Figure 3-50 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 3-51, “Emulated Circuit View.”](#)

Figure 3-51 Emulated Circuit View

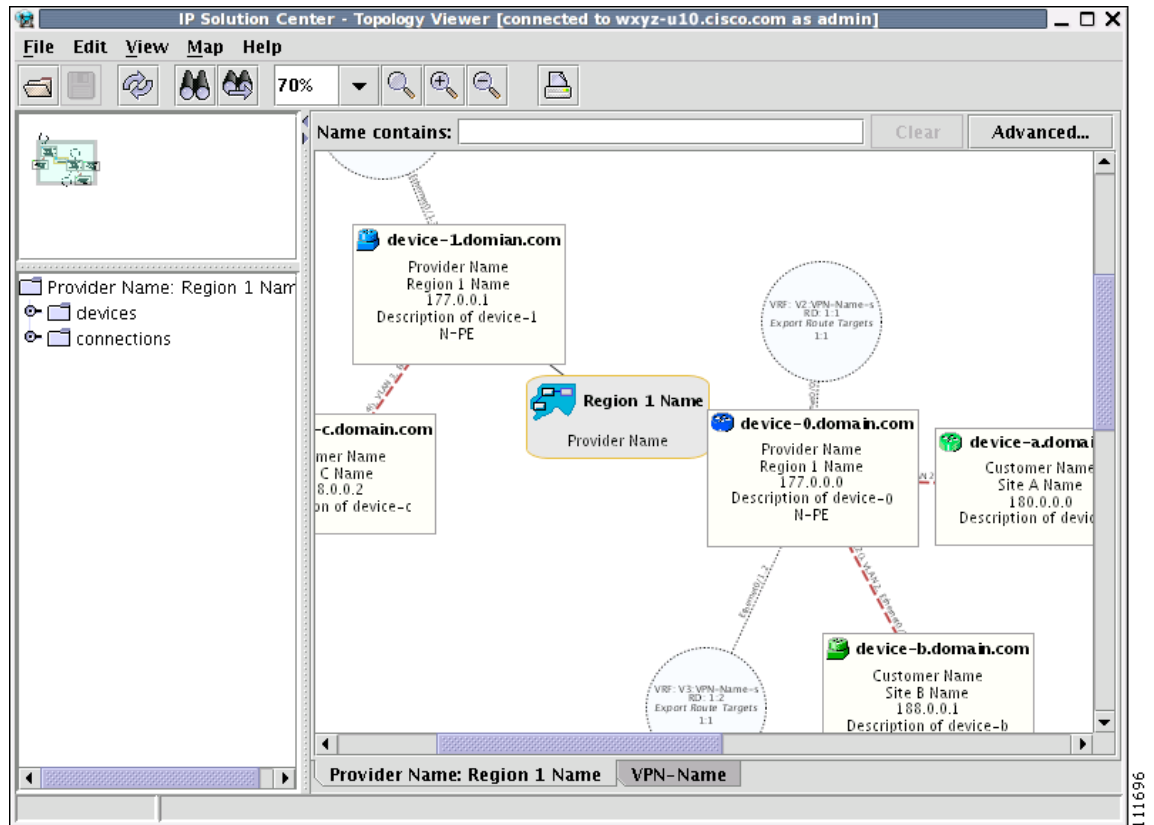


Logical View

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

To activate the logical view, follow these steps:

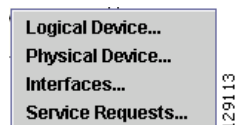
- Step 1** In the menu bar, choose **File > Open**.
or
click the **Open** button in the tool bar.
The Folder View window, as shown in [Figure 3-47](#), appears.
- Step 2** Choose the desired VPN's folder and double-click on the desired folder. Any logical and physical views associated with that VPN are 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 3-52](#).

Figure 3-52 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.

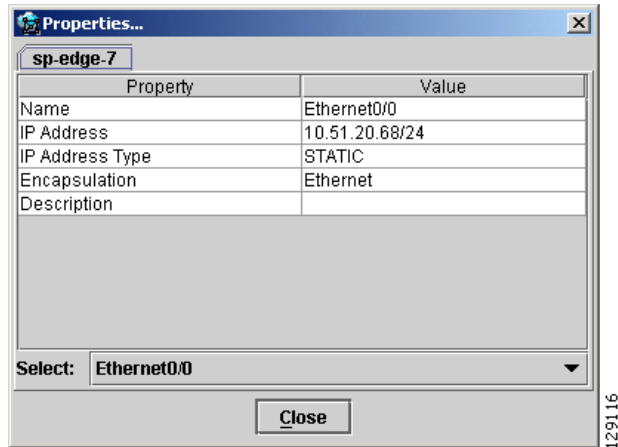
Each node directly connected to the regional node represents a PE. The icon of a node depends on the type and the role of the device it represents (see the “Conventions” section on page 3-41).

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 3-53. For the regional node, details are shown in a tabulated form.

Figure 3-53 Device Properties

The various node and link properties are described in detail in [Viewing Device and Link Properties](#), page 3-56.

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 3-54 appears.

Figure 3-54 *Interface Properties Window*

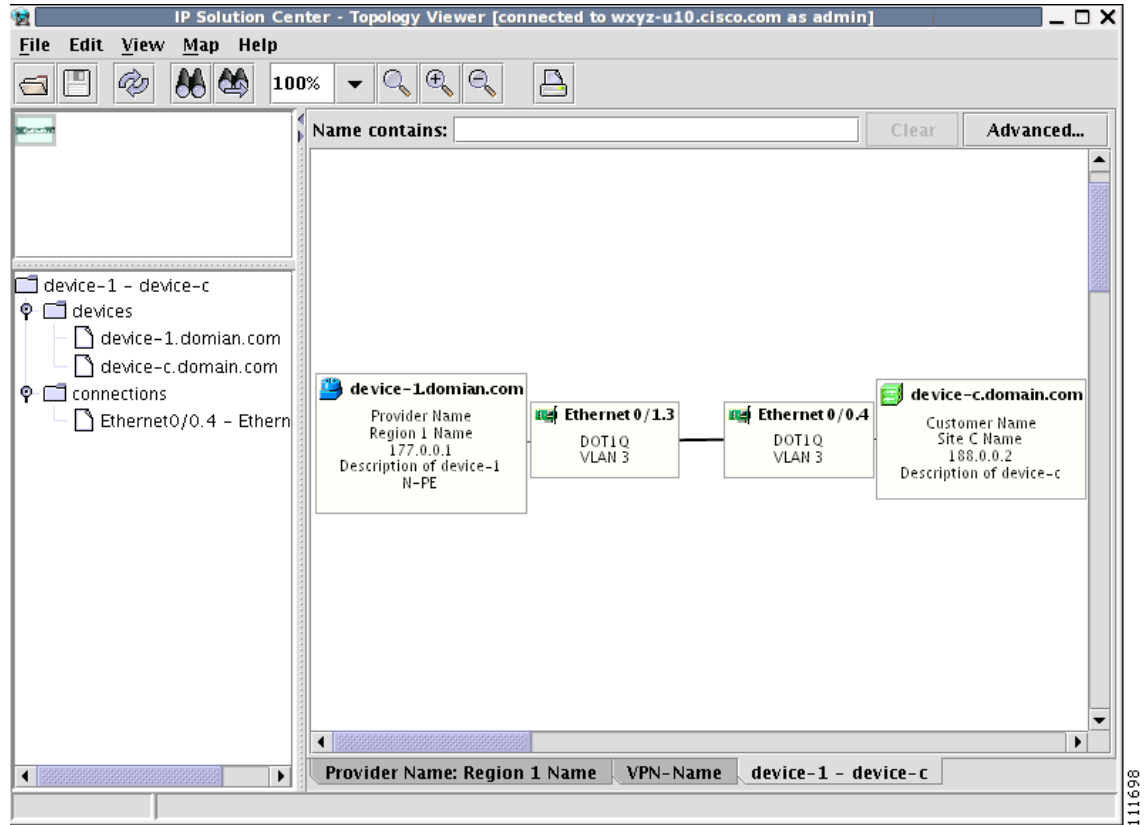
Each PE can be logically connected to one or more CPEs. Such connections are created by either MPLS VPN links or Layer 2 Logical Links. Each such connection is represented by an edge linking the given PE to a CPE. If there are more connections between a particular PE and CPE, all of them are shown. Depending 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 3-4](#) and [Table 3-5](#). 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 3-56.

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 3-55](#).

Figure 3-55 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, follow these steps:

- Step 1** In the menu bar, choose **File > Open**.
or
click the **Open** button in the tool bar.
The Folder View window, as shown in [Figure 3-47](#), appears.
- Step 2** Choose 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:

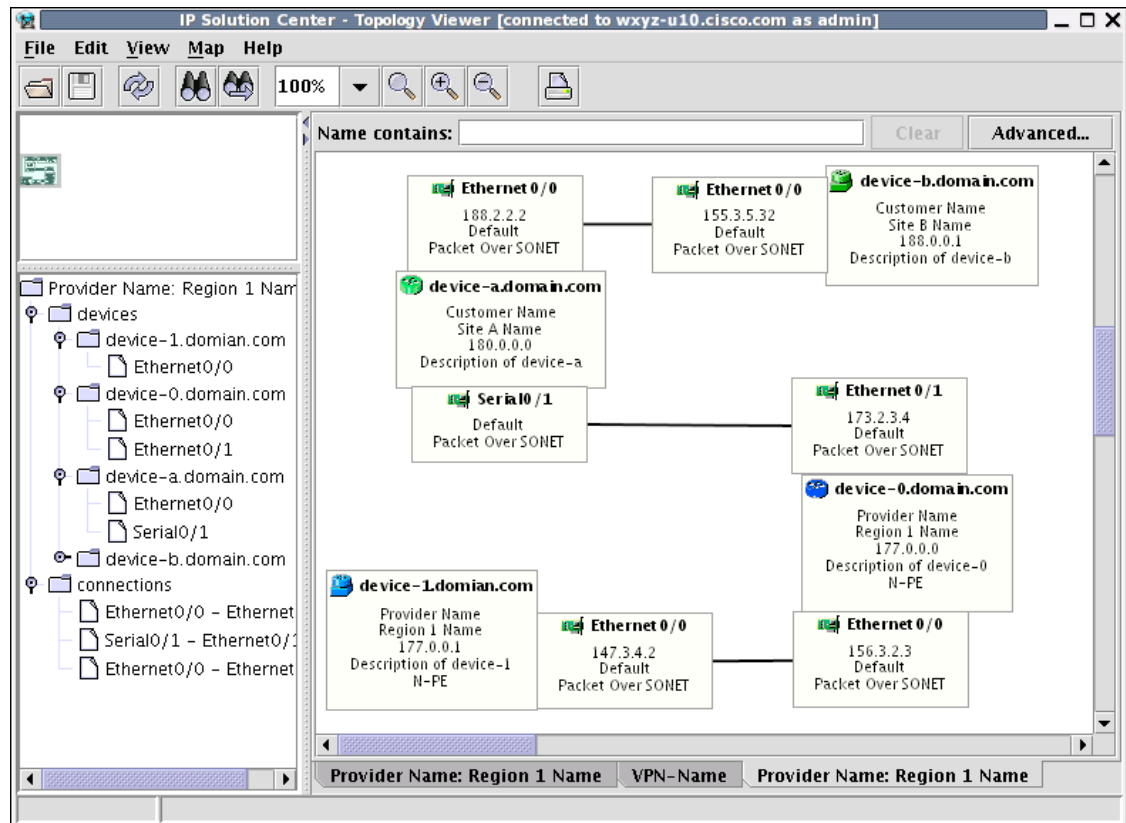
Single-click the **Physical View** icon and click **Open**

or

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

This creates a physical view for the chosen VPN, as shown in [Figure 3-56](#).

Figure 3-56 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 3-57](#) appears.

Figure 3-57 *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.

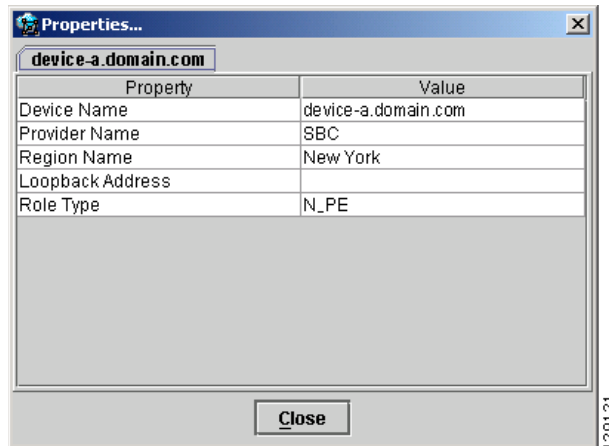
Interfaces...—View interface properties of the device.

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 3-58](#) appears.

Figure 3-58 *Logical Device Properties Window*



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.

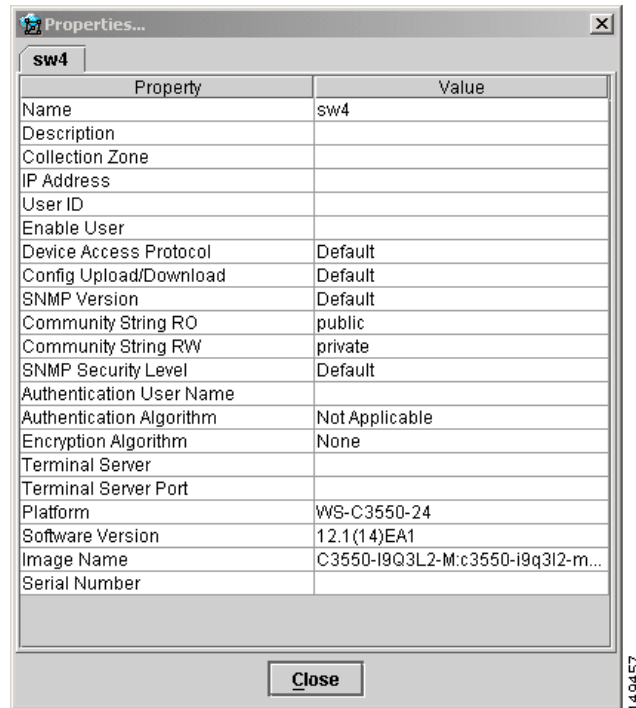
Loopback Address—IP address of the loopback address.

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 3-59](#) appears.

Figure 3-59 *Physical Device Properties Window*



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.

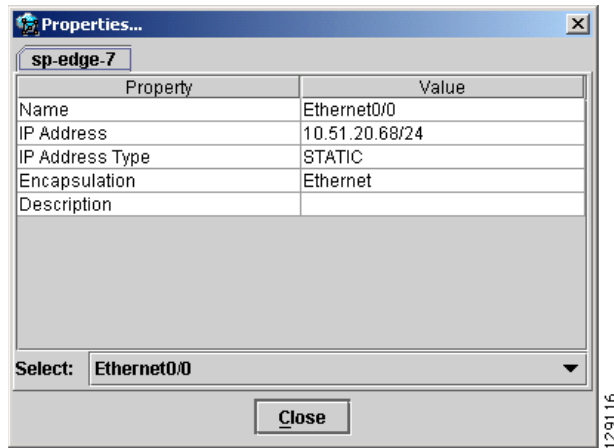
Image Name—Boot image for device initialization.

Serial Number—Serial number of the device.

Interfaces

When right-clicking a device and selecting **Interfaces...**, the interface properties window in [Figure 3-60](#) appears.

Figure 3-60 *Device Interface Properties Window*



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.

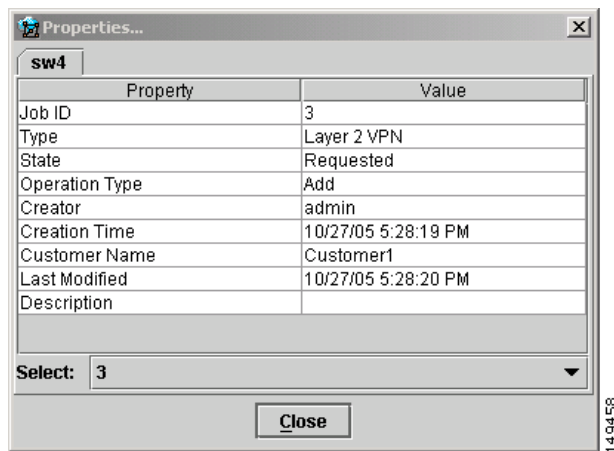
Encapsulation—Encapsulation used on the interface traffic.

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 3-61](#) appears.

Figure 3-61 Service Request Properties Window

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 3-62](#) appears.

Figure 3-62 Link Properties

The following options are available:

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

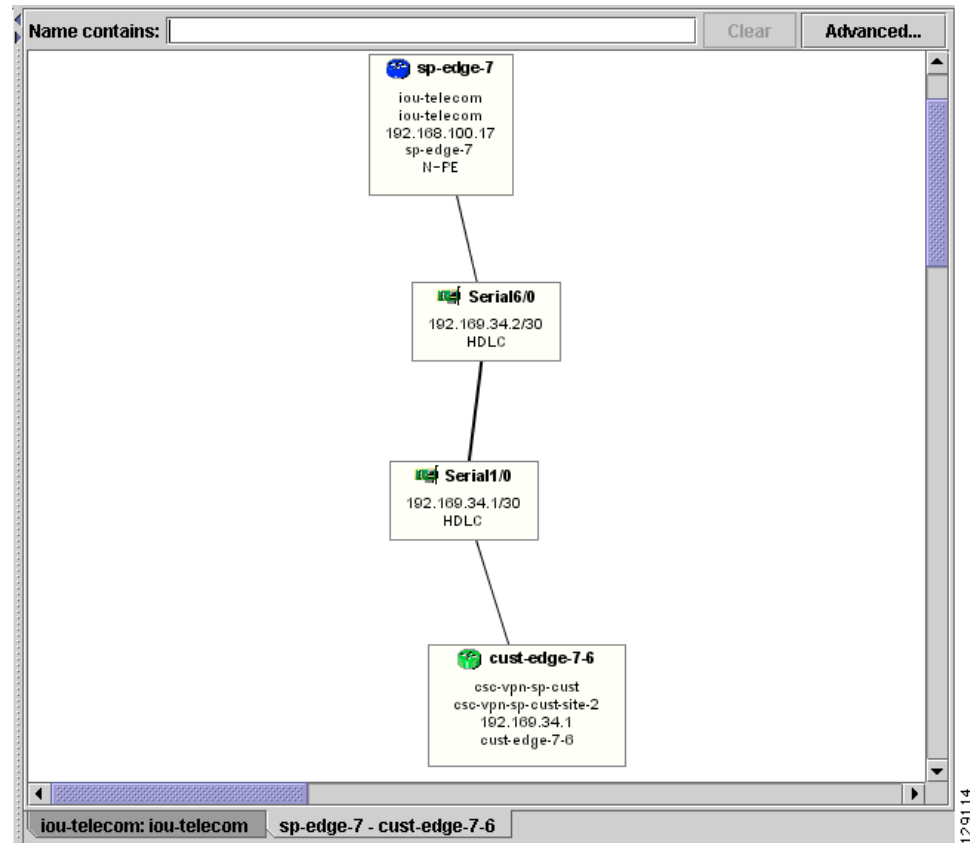
Service Request...—View service request properties associated with the link.

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 3-63](#) will appear.

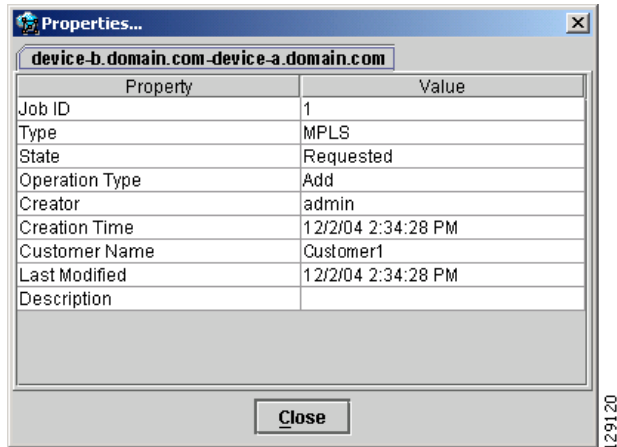
Figure 3-63 Expand Link Window



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 3-64](#) appears.

Figure 3-64 *Link Service Request Properties Window*

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.

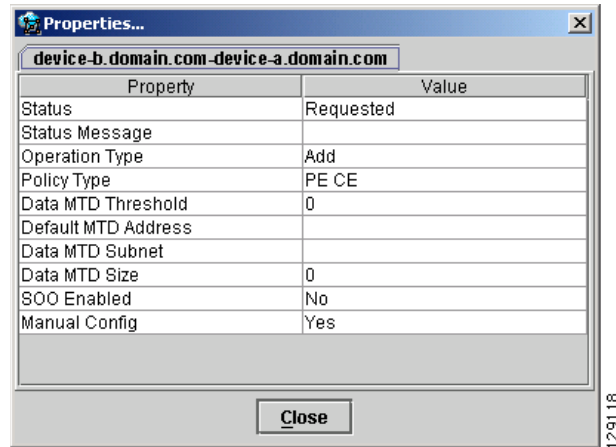
Last Modified—Date and time when the SR was last modified.

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 3-65](#) appears.

Figure 3-65 **Link MPLS VPN Properties Window**

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

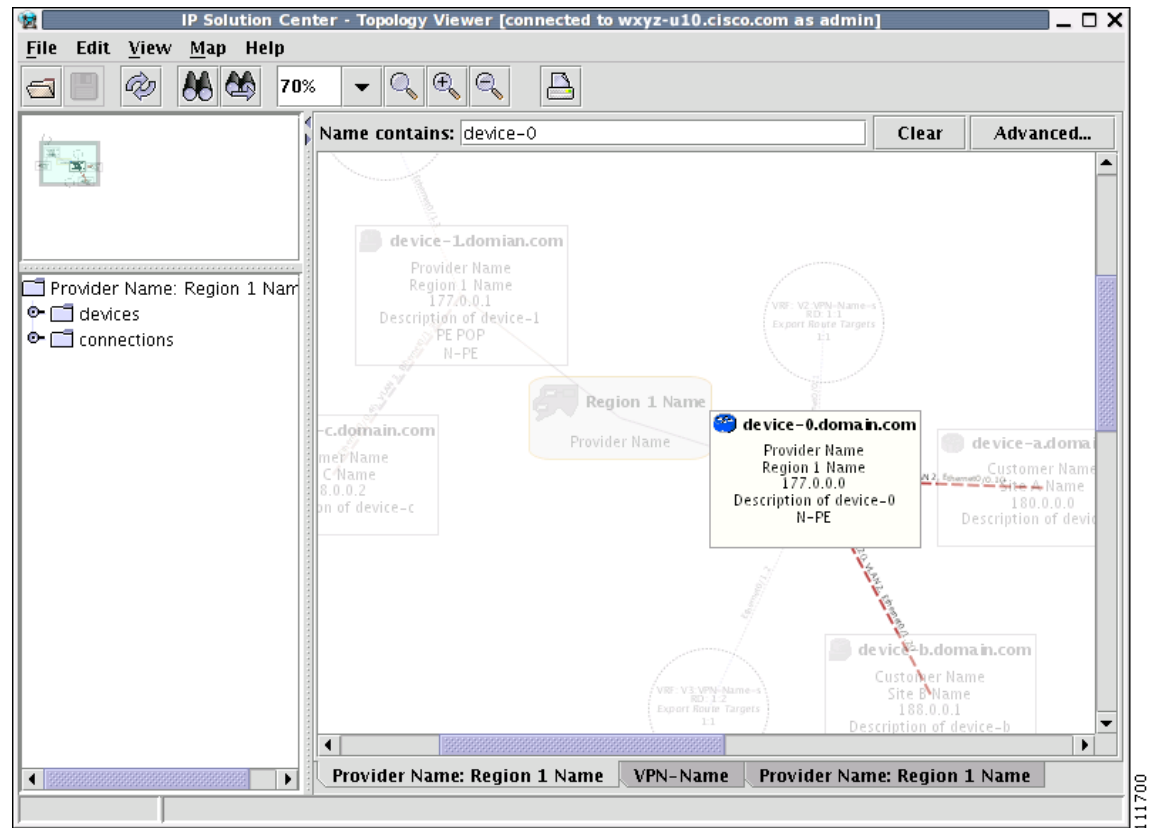
To perform simple filtering of the view, follow these steps:

-
- Step 1** Enter a string in area (4) of the main window, as shown in [Figure 3-44 on page 3-45](#).

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 3-66.

Figure 3-66 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, follow these steps:

Step 1 Open the advanced filtering dialog by clicking the **Advanced...** button. The Advanced Filter dialog appears, as shown in Figure 3-67.

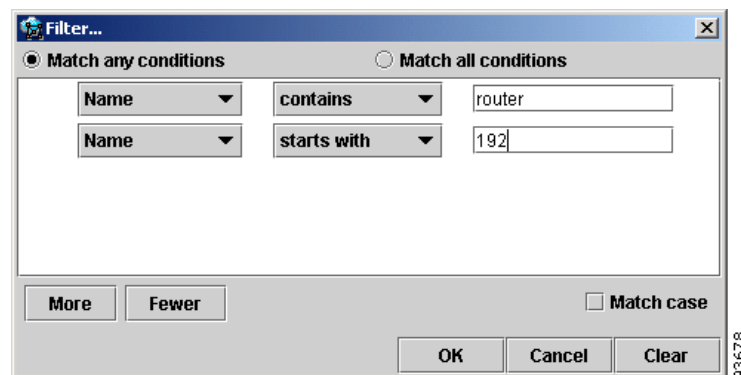
Step 2 Make the desired filtering elections.

The dialog allows you to enter one or more conditions on filtered nodes. The first drop-down list 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 list:

- **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 3-67 **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, check 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 3-44 on page 3-45](#).

Searching

Searching can be conducted by using the menus or the tool bar. To perform a search, follow these steps:

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

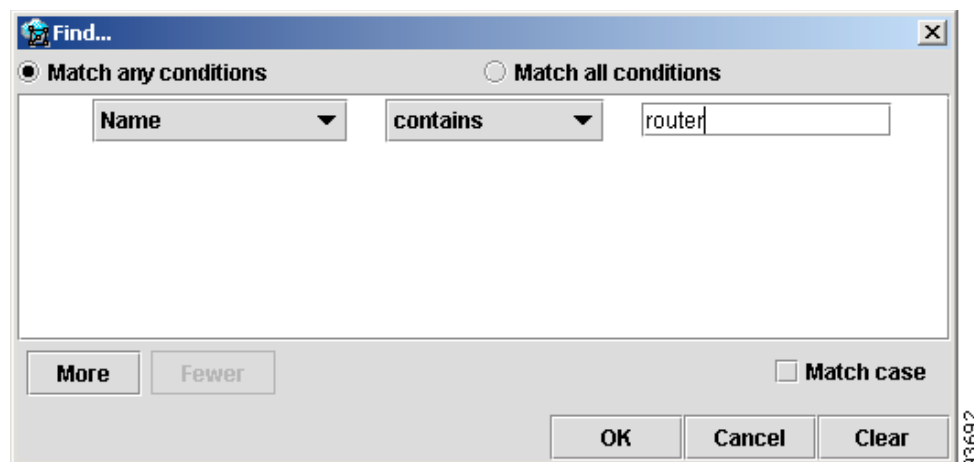
or

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

Both approaches bring up the same dialog box, as shown in [Figure 3-68](#).

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

Figure 3-68 Find Dialog Box



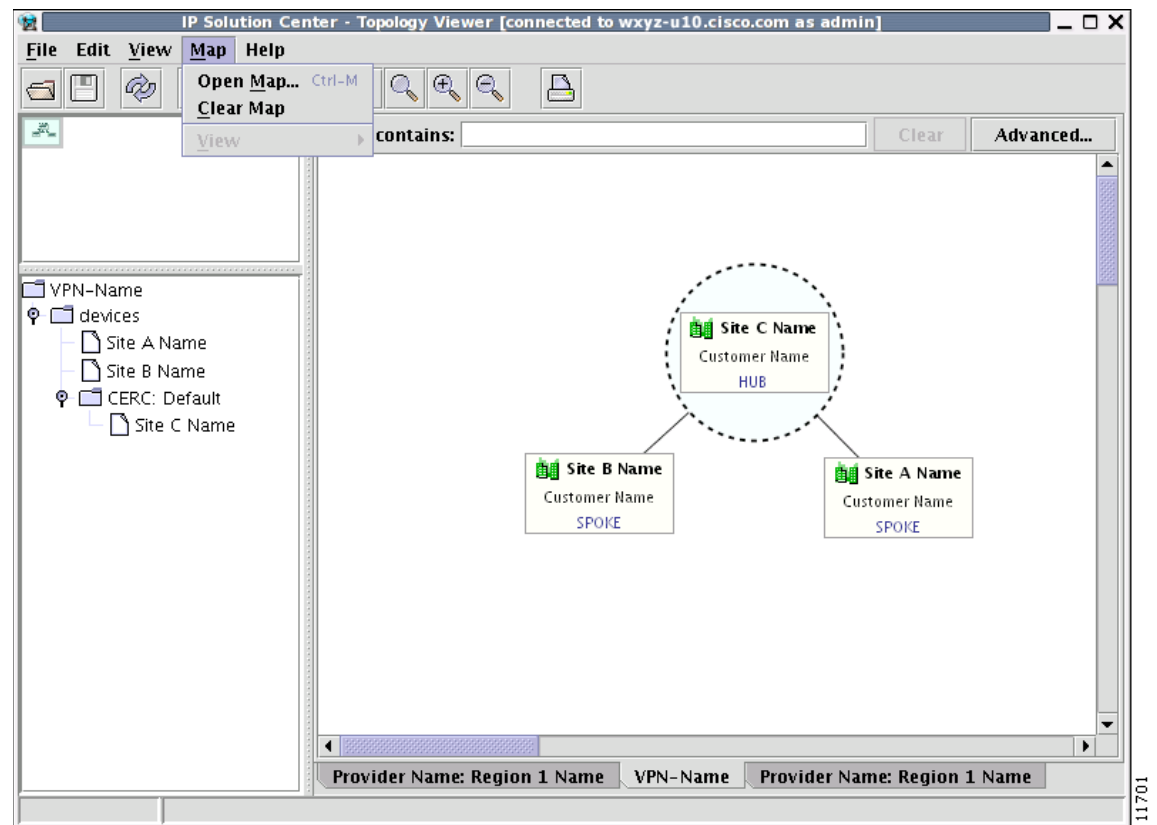
- Step 2** Make the desired filtering selections. Match modes, case check box, and the radio button are used as described under [Advanced Filtering, page 3-64](#), as shown in [Figure 3-67](#).
- Step 3** Click **OK** to start searching for the first node that matches the given criteria. If found, the 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 3-69.

Figure 3-69 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, follow these steps:

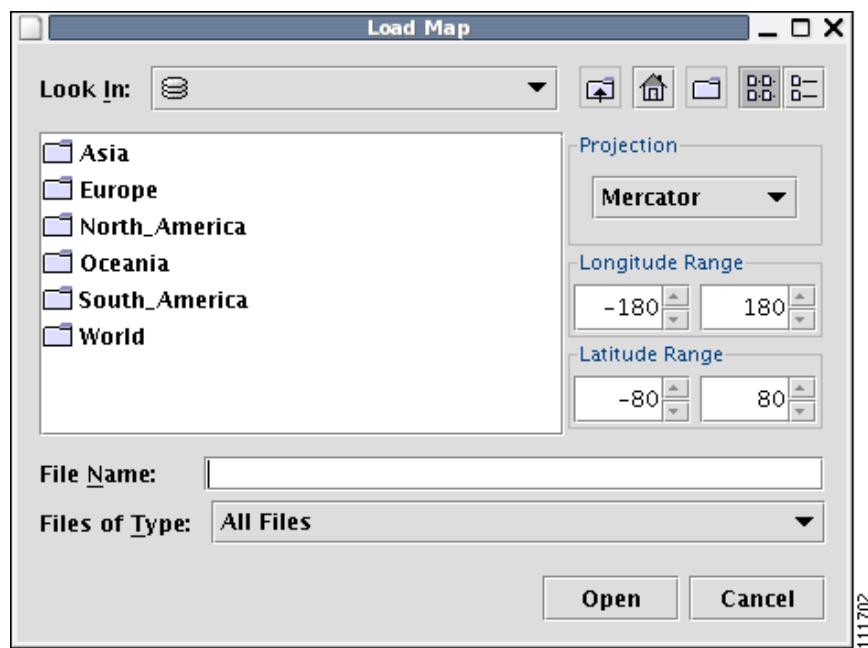
Step 1 In the menu bar, select **Map > Open Map....**

or

Press **Ctrl-M**

Providing the web map server is running and operational, the Load Map window appears, as shown in Figure 3-70.

Figure 3-70 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 Choose the desired folder.

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

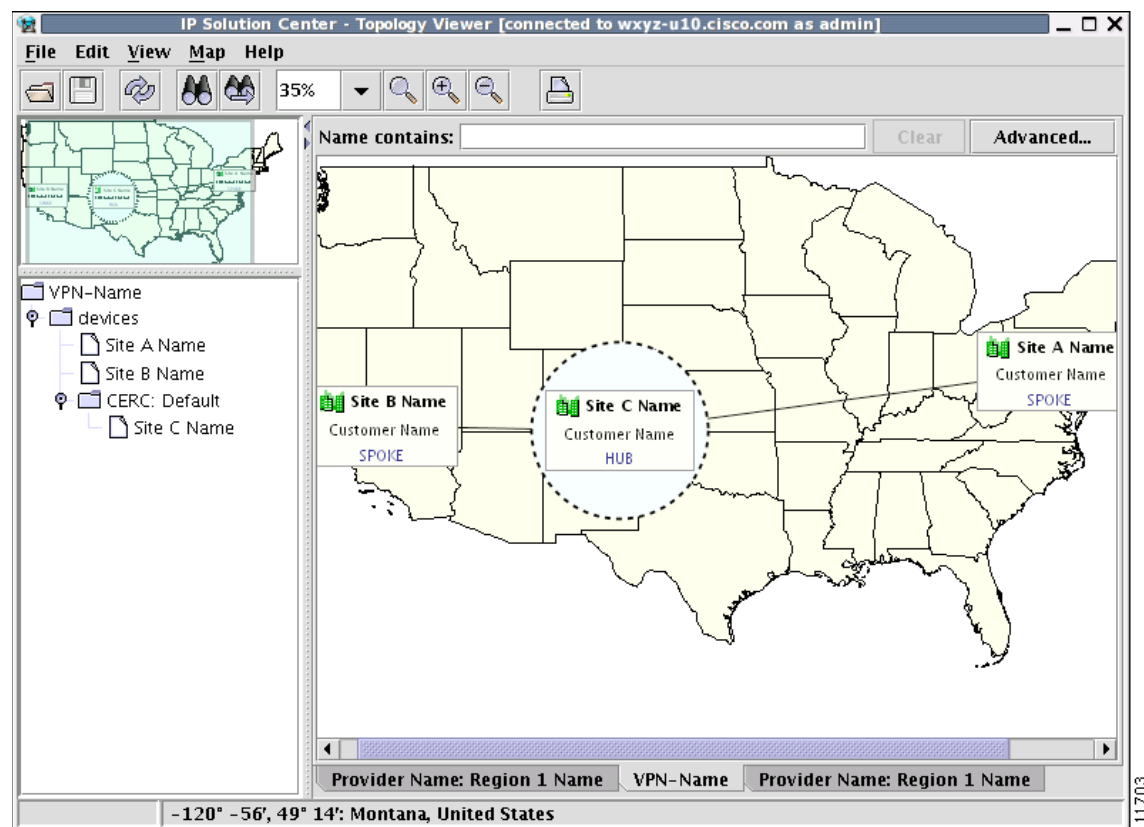
Step 4 Select a map file and click **Open** to load the map.

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 3-71.

Figure 3-71 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 unchecking 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

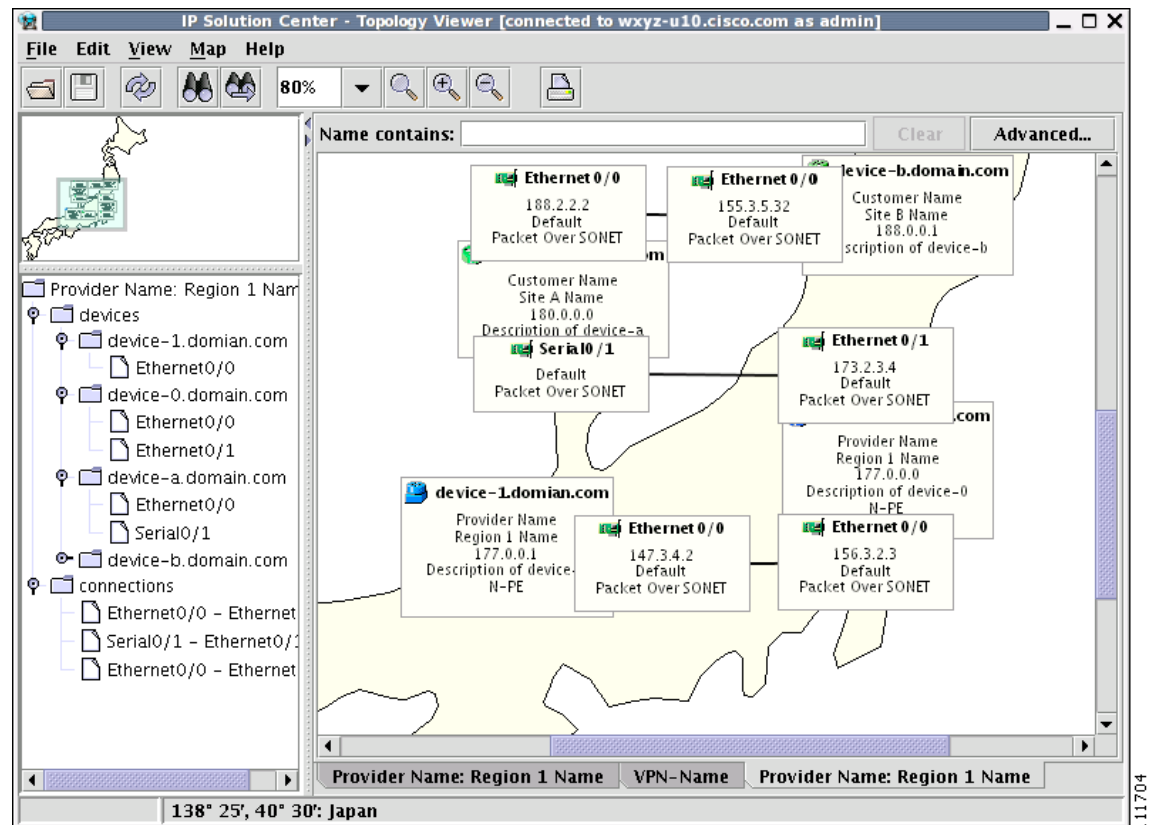
If map data files are successfully loaded with the map, the right field of the Status bar shows the longitude and latitude location of the cursor on the map. If map objects, such as cities, lakes, and so on, have data associated with them, their names are displayed after the longitude and latitude coordinates.

Node locations

After a map is successfully loaded, the view area is adjusted to fully accommodate it, as shown in Figure 3-72. 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 3-72 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 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 or SSHv2, 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 or SSHv2, page 3-72](#)
- [Configuring SSHv1 or SSHv2 on Cisco IOS Routers Using RSA Key Pairs, page 3-73](#)
- [Manually Enabling RTR Responder on Cisco IOS Routers, page 3-77](#)
- [Accessing the Devices Window, page 3-77](#)
- [Creating a Device, page 3-79](#)

- [Editing a Device, page 3-97](#)
- [Deleting Devices, page 3-100](#)
- [Editing a Device Configuration, page 3-101](#)
- [E-mailing a Device's Owner, page 3-103](#)
- [Copying a Device, page 3-104](#)

Configuring SSH or SSHv2

ISC needs a mechanism to securely access and deploy configuration files on devices, which include routers and switches. And, to securely download a configlet and upload a configuration file from a device, Secure Shell (SSH) or SSH version 2(SSHv2) must be enabled.

The following sections describe:

- [Configuring SSH on Cisco IOS Routers Using a Domain Name, page 3-72](#)
- [Configuring SSHv1 or SSHv2 on Cisco IOS Routers Using RSA Key Pairs, page 3-73](#)
- [Configuring SSH or SSHv2 on Cisco IOS XR Routers, page 3-73](#)

Configuring SSH on Cisco IOS Routers Using a Domain Name

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 SSHv1 or SSHv2 on Cisco IOS Routers Using RSA Key Pairs

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 SSHv1 or SSHv2 on a Cisco IOS router is as follows. For more detailed information, go to http://www.cisco.com/en/US/products/ps5845/products_configuration_guide_chapter09186a00806f9ec4.html#wp1027184.

	Command	Description
Step 1	Router# enable	Enables privileged EXEC mode. Enter your password, if prompted.
Step 2	Router# configure terminal	Enters global configuration mode.
Step 3	Router(config)# ip ssh rsa keypair-name <i><keypair-name></i>	Specifies which RSA keypair to use for SSH usage. Note: A Cisco IOS router can have many RSA key pairs.
Step 4	Router(config)# crypto key generate rsa usage-keys label <i><key-label></i> modulus <i><modulus-size></i>	Enables the SSH server for local and remote authentication on the router. For SSH Version 2, the modulus size must be at least 768 bits. Note: To delete the RSA key-pair, use the crypto key zeroize rsa command. After you have deleted the RSA command, you automatically disable the SSH server.
Step 5	Router(config)# ip ssh [timeout <seconds> authentication-retries <integer>]	Configures SSH control variables on your router.
Step 6	Router(config)# ip ssh version [1 2]	Specifies the version of SSH to be run on a router.

Configuring SSH or SSHv2 on Cisco IOS XR Routers

This Cisco IOS XR 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 SSHv2 on a Cisco IOS XR router is as follows. For more detailed information, go to http://www.cisco.com/univercd/cc/td/doc/product/software/ios123/123newft/123t/123t_7/gt_ssh2.htm#wp1027129.

	Command	Description
Step 1	RP/0/RP0/CPU0:router# configure	Enters global configuration mode.
Step 2	RP/0/RP0/CPU0:router(config)# hostname <i><hostname></i>	Configures a hostname for your router.
Step 3	RP/0/RP0/CPU0:router(config)# domain name <i><domain-name></i>	Defines a default domain name that the software uses to complete unqualified host names.
Step 4	RP/0/RP0/CPU0:router(config)# exit	Exits global configuration mode, and returns the router to EXEC mode.
Step 5	RP/0/RP0/CPU0:router(config)# crypto key generate rsa [usage keys general-keys] [<i><keypair-label></i>]	Generates an RSA key pair.

	Command	Description
Step 6	RP/0/RP0/CPU0:router# crypto key generate dsa	Enables the SSH server for local and remote authentication on the router. The recommended minimum modulus size is 1024 bits. Generates a DSA key pair. To delete the DSA key pair, use the crypto key zeroize dsa command. This command is used only for SSHv2.
Step 7	RP/0/RP0/CPU0:router# configure	Enters global configuration mode.
Step 8	RP/0/RP0/CPU0:router# ssh timeout <i><seconds></i>	(Optional) Configures the timeout value for user authentication to authentication, authorization, and accounting (AAA). If the user fails to authenticate itself to AAA within the configured time, the connection is aborted. If no value is configured, the default value of 30 is used for 30 seconds. The range is from 5 to 120.
Step 9	RP/0/RP0/CPU0:router(config)# ssh server or RP/0/RP0/CPU0:router(config)# ssh server v2	Brings up an SSH server. To bring down an SSH server, use the no ssh server command. (Optional) Forces the SSH server to accept only SSHv2 clients if you configure the SSHv2 option by using the ssh server v2 command. If you choose the ssh server v2 command, only the SSH v2 client connections are accepted.
Step 10	RP/0/RP0/CPU0:router(config)# end or RP/0/RP0/CPU0:router(config)# commit	Saves configuration changes. When you issue the end command, the system prompts you to commit changes: Uncommitted changes found, commit them before exiting (yes/no/cancel)? [cancel] Entering yes saves configuration changes to the running configuration file, exits the configuration session, and returns the router to EXEC mode. Entering no exits the configuration session and returns the router to EXEC mode without committing the configuration changes. Entering cancel leaves the router in the current configuration session without exiting or committing the configuration changes. Use the commit command to save the configuration changes to the running configuration file and remain within the configuration session.

	Command	Description
Step 11	RP/0/RP0/CPU0:router# show ssh	(Optional) Displays all of the incoming and outgoing SSHv1 and SSHv2 connections to the router.
Step 12	RP/0/RP0/CPU0:router# show ssh session details	(Optional) Displays a detailed report of the SSHv2 connections to and from the router.

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 3-6](#) identifies the combinations of security models and levels.

Table 3-6 *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> enable Router> <enable_password>	Enters enable mode, then enter the enable password.
Step 2	Router# configure terminal	Enters global configuration mode.
Step 3	Router(config)# snmp-server group [<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: snmp-server group v3auth v3 auth read v1default write v1default
Step 4	Router(config)# snmp-server user <username> [<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: snmp-server user user1 v3auth v3 auth md5 user1Pass
Step 5	Router(config)# Ctrl+Z	Returns to Privileged Exec mode.
Step 6	Router# copy running startup	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> enable Router> <enable_password>	Enters enable mode, and then enters the enable password.
Step 2	Router# configure terminal	Enters the global configuration mode.
Step 3	Router(config)# rtr responder	Enables the SA responder on the target router of SA Agent operations.
Step 4	Router(config)# Ctrl+Z	Returns to Privileged Exec mode.
Step 5	Router# copy running startup	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, follow these steps:

- Step 1** Choose **Service Inventory > Inventory and Connection Manager > Devices** to access the Devices window shown in [Figure 3-73](#).

Figure 3-73 *Devices List Window*

Devices

Show Devices with matching

Showing 1 - 8 of 8 records

#	☐	Device Name	Management IP Address	Type	Parent Device Name
1.	☐	pe1		Cisco IOS Device	
2.	☐	pe3		Cisco IOS Device	
3.	☐	sw2		Cisco IOS Device	
4.	☐	sw3		Cisco IOS Device	
5.	☐	sw4		Cisco IOS Device	
6.	☐	ce3		Cisco IOS Device	
7.	☐	ce8		Cisco IOS Device	
8.	☐	ce13		Cisco IOS Device	

Rows per page:

Go to page: of 1

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, and IE2100.
- **Parent Device Name**

In the Devices window, you can create, edit, delete, or configure devices, e-mail the device owner, or copy 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 checking the corresponding box). Enabled only if a single device is selected.
- **Delete** Click to delete selected device (select device by checking the corresponding box). Enabled only if one or more devices are selected.
- **Config** Click to change the selected device configuration (select device by checking the corresponding box). Enabled only if a single device is selected.

- **E-mail** Click to send e-mail to the owner of the selected device(s) (select device(s) by checking the corresponding box(es)). Enabled only if one or more devices are selected.
- **Copy** Click to copy selected device (select device by checking the corresponding box). Enabled only if a single device is selected.

Creating a Device

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

To create a device, follow these steps:

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

Step 2 Click the **Create** button.

The Create options window appears, as shown in [Figure 3-74](#).

Figure 3-74 Create Options Window

The screenshot shows the 'Devices' window with a search bar at the top. Below the search bar is a table with 8 records. The table has columns for #, Device Name, Management IP Address, Type, and Parent Device Name. The records are as follows:

#	Device Name	Management IP Address	Type	Parent Device Name
1.	pe1		Cisco IOS Device	
2.	pe3		Cisco IOS Device	
3.	sw2		Cisco IOS Device	
4.	sw3		Cisco IOS Device	
5.	sw4		Cisco IOS Device	
6.	ce3		Cisco IOS Device	
7.	ce8	Catalyst Switch	Cisco IOS Device	
8.	ce13	Cisco Device	Cisco IOS Device	

Below the table, there is a 'Rows per page' dropdown set to 10. To the right, there is a 'Go to page' field set to 1 of 1. At the bottom, there is a 'Create' button with a dropdown arrow, and buttons for 'Edit', 'Delete', 'Config', 'E-mail', and 'Copy'.

The **Create** options include the following:

- **Catalyst Switch** A Catalyst device running the Catalyst Operating System.
- **Cisco 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.
- **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 3-80](#)
- [Creating a Cisco Device, page 3-85](#)

- [Creating a Terminal Server, page 3-91](#)
 - [Creating a Cisco CNS IE2100, page 3-96](#)
-

Creating a Catalyst Switch

To create a Catalyst switch, follow these steps:

- Step 1** Choose **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 3-75](#).

Figure 3-75 Create Catalyst Device Window

Create Catalyst Device

General

Device Host Name*:

Device Domain Name:

Description:

Collection Zone:

Management IP Address:

Interfaces:

Associated Groups:

Operating System: ☒ Catalyst OS ☐ Cisco IOS

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:

OS:

SNMP Version:

SNMP v1/v2c

Community String RO:

Community String RW:

Additional Properties:

Note: * - Required Field

149462

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 3-7](#) for a description of the Interfaces fields.

Table 3-7 Create Catalyst Device Interfaces Fields

Field	Description	Additional
Interface Name	Name of this interface.	List can be sorted by this field. Limited to 80 characters.
IPv4 Address	IPv4 address associated with this interface.	
IPv6 Address	IPv6 address associated with this interface.	
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
Port Type		NONE ACCESS TRUNK ROUTED
Description		
IP Address Type		

- **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: Catalyst OS or Cisco IOS. Default: Catalyst OS. When you choose the IOS operating system, VPNSM is available under the heading Catalyst Properties. If you click the **Edit** button for **VPNSM**, you can **Create**, **Edit**, and **Delete** VPN Service Modules (VPNSMs).

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) Not required by ISC. However, collection and upload/download will not function without the Login User and Login Password, because 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) 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) 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) 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), SSH version 2 (SSHv2), 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 **Show**.

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

Figure 3-76 Catalyst Device Additional Properties Window

Additional Properties:		Hide
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 Options		
Terminal Server:	None ▾	
Port:	0	
Device Platform Information		
Platform:		
Software Version:		
Image Name:		
Serial Number:		
Device Owner's Email Address:		
		Save Cancel

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) 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) 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) 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) 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 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.

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 **Save**.

The Devices window reappears with the new Catalyst device listed.

Creating a Cisco Device

To create a Cisco device, follow these steps:

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

Step 2 Click the **Create** button.

Step 3 Select **Cisco Device**.

The Create Cisco Device window appears, as shown in [Figure 3-77](#).

Figure 3-77 Create Cisco Device Window

Create Cisco 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) ▾
OS:	IOS ▾
SNMP Version:	Default (SNMP v1/v2c) ▾
SNMP v1/v2c	
Community String RO:	
Community String RW:	
Additional Properties:	Show
Save Cancel	

Note: * - Required Field

149136

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 3-8](#) for a description of the Interface fields

Table 3-8 Create Cisco Device Interface Fields

Field	Description	Additional
Interface Name	Name of this interface.	List can be sorted by this field. Limited to 80 characters.
IPV4 Address	IP address associated with this IPv4 interface.	
IPV6 Address	IP address associated with this IPv6 interface.	
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

Table 3-8 Create Cisco Device Interface Fields (continued)

Field	Description	Additional
Description		
IP Address Type		

- **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), SSH version 2 (SSHv2), and CNS.
- **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.
- **OS** (optional) The choices are: **IOS** for IOS and **IOX** for IOS XR.
- **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 Device**, click **Show**. The Additional Properties window appears, as shown in [Figure 3-78](#).

Figure 3-78 Additional Properties for the Cisco Device Properties Window

Additional Properties: Hide

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: 1.4

CNS Device Transport: HTTP

Device Platform Information

Platform:

Software Version:

Image Name:

Serial Number:

Device Owner's Email Address:

Save Cancel

Note: * - Required Field

149133

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 checked, 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, 1.4, and 1.5. This is the release version of Cisco CNS Configuration Engine that manages the IOS device. Default: 1.4.

- **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 **Save**.

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

Creating a Terminal Server

To create a Terminal Server device, follow these steps:

Step 1 Choose **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 3-79](#).

Figure 3-79 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:

OS:

SNMP Version:

SNMP v1/v2c

Community String RO:

Community String RW:

Additional Properties:

Note: * - Required Field

149153

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 3-9](#) for a description of the Interfaces fields.

Table 3-9 Create Terminal Server Device Interfaces Fields

Field	Description	Additional
Interface 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
Port Type		NONE ACCESS TRUNK ROUTED
Description		
IP Address Type		

- **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), SSH version 2 (SSHv2), 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 **Show**.

The Additional Properties window appears, as shown in [Figure 3-80](#).

Figure 3-80 Additional Properties for the 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 **Save**.

The Devices window reappears with the new Terminal Server 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 with ISC” in the [Cisco IP Solution Center Installation Guide, 5.0](#). 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 the [Cisco IP Solution Center Installation Guide, 5.0](#).

To create a Cisco CNS IE2100 appliance, follow these steps:

Step 1 Choose **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 3-81](#).

Figure 3-81 Create IE2100 Device Window

Create IE2100 Device

General

Device Host Name *:

Device Domain Name:

Description:

IPv4 Address:

Note: * - Required Field

211158

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.
- **IPv4 Address** (optional) Valid IPv4 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, follow these steps:

- Step 1** Choose **Service Inventory > Inventory and Connection Manager > Devices** to access the Devices window shown in [Figure 3-82](#).

Figure 3-82 *Devices List Window*

Devices

Show Devices with matching

Showing 1 - 8 of 8 records

#	☐		Device Name	Management IP Address	Type	Parent Device Name
1.	☐		pe1		Cisco IOS Device	
2.	☐		pe3		Cisco IOS Device	
3.	☐		sw2		Cisco IOS Device	
4.	☐		sw3		Cisco IOS Device	
5.	☐		sw4		Cisco IOS Device	
6.	☐		ce3		Cisco IOS Device	
7.	☐		ce8		Cisco IOS Device	
8.	☐		ce13		Cisco IOS Device	

Rows per page:

Go to page: of 1

Step 2 Select a single device to edit by checking the box to the left of the Device Name. You can also select a device to edit by clicking on the hyperlink 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 3-83](#).

Figure 3-83 *Editing a Device Window*

Edit Cisco Device

General	
Device Host Name *	ensw3550-1
Device Domain Name:	
Description:	
Collection Zone:	None
Management IP Address:	
Interfaces:	192.168.30.3, 192.168.30.4 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)
OS:	IOS
SNMP Version:	Default (SNMP v1/v2c)
SNMP v1/v2c	
Community String RO:	public
Community String RW:	private
Additional Properties:	Show
Save Cancel	

Note: * - Required Field

149144

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.

Deleting Devices

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

To access the Delete window, follow these steps:

- Step 1** Choose **Service Inventory > Inventory and Connection Manager > Devices** to access the Devices window shown in [Figure 3-84](#).

Figure 3-84 *Devices List Window*

The screenshot shows the 'Devices' window with a search bar at the top. Below the search bar is a table with 8 rows of device information. The table has columns for '#', 'Device Name', 'Management IP Address', 'Type', and 'Parent Device Name'. The devices listed are pe1, pe3, sw2, sw3, sw4, ce3, ce8, and ce13, all of which are Cisco IOS Devices. At the bottom of the window, there are buttons for 'Create', 'Edit', 'Delete', 'Config', 'E-mail', and 'Copy'. The 'Delete' button is highlighted.

#	Device Name	Management IP Address	Type	Parent Device Name
1.	pe1		Cisco IOS Device	
2.	pe3		Cisco IOS Device	
3.	sw2		Cisco IOS Device	
4.	sw3		Cisco IOS Device	
5.	sw4		Cisco IOS Device	
6.	ce3		Cisco IOS Device	
7.	ce8		Cisco IOS Device	
8.	ce13		Cisco IOS Device	

- Step 2** Select one or more devices to delete by checking 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 3-85](#).

Figure 3-85 *Confirm Delete Window*

The screenshot shows the 'Confirm Delete' window. It displays a table with 1 row of device information. The table has columns for '#', 'Device Name', 'Management IP Address', 'Type', and 'Parent Device Name'. The device listed is 1. ensw3550-1.cisco.com, which is a Cisco IOS Device. At the bottom of the window, there are buttons for 'Delete' and 'Cancel'. The 'Delete' button is highlighted.

#	Device Name	Management IP Address	Type	Parent Device Name
1.	ensw3550-1.cisco.com		Cisco IOS Device	

- 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, follow these steps:

- Step 1** Choose **Service Inventory > Inventory and Connection Manager > Devices** to access the Devices window shown in [Figure 3-86](#).

Figure 3-86 *Devices List Window*

Devices

Show Devices with matching

Showing 1 - 8 of 8 records

#	☐	Device Name	Management IP Address	Type	Parent Device Name
1.	☐	pe1		Cisco IOS Device	
2.	☐	pe3		Cisco IOS Device	
3.	☐	sw2		Cisco IOS Device	
4.	☐	sw3		Cisco IOS Device	
5.	☐	sw4		Cisco IOS Device	
6.	☐	ce3		Cisco IOS Device	
7.	☐	ce8		Cisco IOS Device	
8.	☐	ce13		Cisco IOS Device	

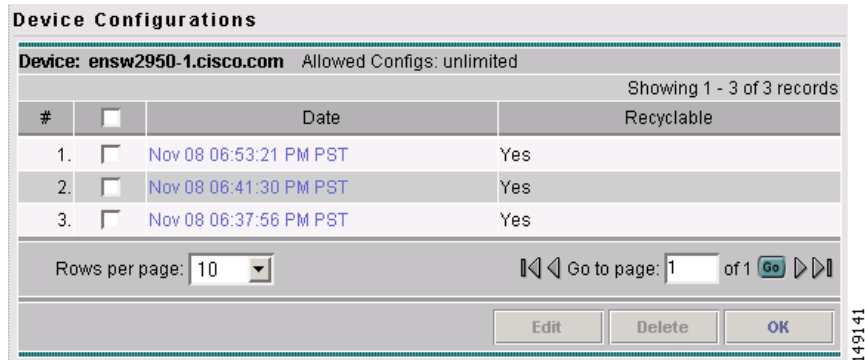
Rows per page:

Go to page: of 1

- Step 2** Select a single device to modify by checking the check box to the left of the Device Name.

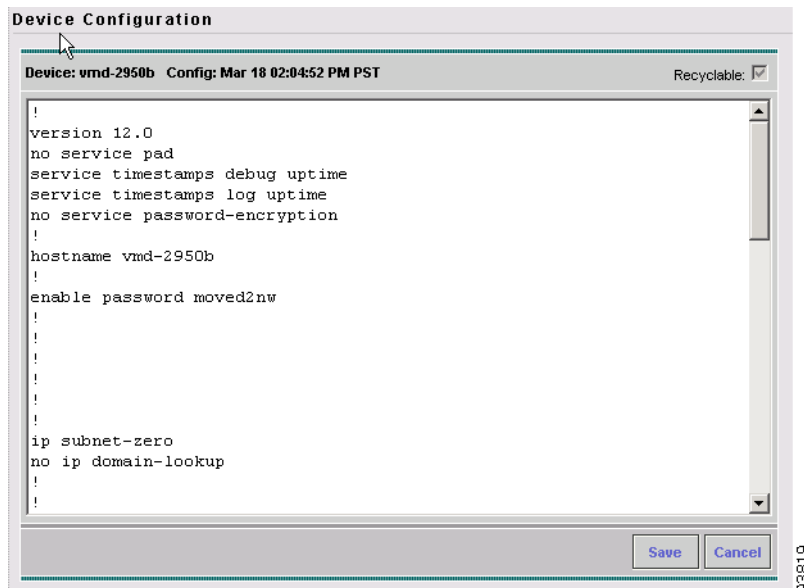
- Step 3** Click the **Config** button.

The Device Configurations window for the selected device appears, as shown in [Figure 3-87](#).

Figure 3-87 *Device Configurations Window*

- Step 4** Check 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 3-88](#).

Figure 3-88 *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, follow these steps:

- Step 1** Choose **Service Inventory > Inventory and Connection Manager > Devices** to access the Devices window shown in [Figure 3-89](#).

Figure 3-89 *Devices List Window*

Devices

Show Devices with matching

Showing 1 - 8 of 8 records

#	☐	Device Name	Management IP Address	Type	Parent Device Name
1.	☐	pe1		Cisco IOS Device	
2.	☐	pe3		Cisco IOS Device	
3.	☐	sw2		Cisco IOS Device	
4.	☐	sw3		Cisco IOS Device	
5.	☐	sw4		Cisco IOS Device	
6.	☐	ce3		Cisco IOS Device	
7.	☐	ce8		Cisco IOS Device	
8.	☐	ce13		Cisco IOS Device	

Rows per page:

Go to page: of 1

- Step 2** Select the devices for which you want to send a device report by checking 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 3-90](#).

Figure 3-90 *Send Mail to Device Owners Window*

Send Mail to Device owners

Please separate E-mail addresses using comma.

To:

CC:

Subject:

Message:

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, follow these steps:

Step 1 Choose **Service Inventory > Inventory and Connection Manager > Devices** to access the Devices window shown in [Figure 3-91](#).

Figure 3-91 **Devices List Window**

Devices

Show Devices with matching

Showing 1 - 8 of 8 records

#	☐	Device Name	Management IP Address	Type	Parent Device Name
1.	☐	pe1		Cisco IOS Device	
2.	☐	pe3		Cisco IOS Device	
3.	☐	sw2		Cisco IOS Device	
4.	☐	sw3		Cisco IOS Device	
5.	☐	sw4		Cisco IOS Device	
6.	☐	ce3		Cisco IOS Device	
7.	☐	ce8		Cisco IOS Device	
8.	☐	ce13		Cisco IOS Device	

Rows per page:

Go to page: of 1

Step 2 Select a single device to copy by checking 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 3-79](#) 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 3-106](#)
- [Creating a Device Group, page 3-106](#)
- [Editing a Device Group, page 3-109](#)
- [Deleting Device Groups, page 3-109](#)
- [E-mailing a Device Group, page 3-110](#)

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, follow these steps:

-
- Step 1** Choose **Service Inventory > Inventory and Connection Manager > Device Groups** to access the Device Groups window shown in [Figure 3-92](#).

Figure 3-92 *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', a text input field containing an asterisk (*), and a 'Find' button. 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 in the first column. The rows are: 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'.

#	Device Group Name	Description
1.	☐ group1	
2.	☐ Device Group 1	
3.	☐ Device Group B	
4.	☐ DeviceC	

Rows per page: 10

Create Edit Delete 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 checking the corresponding box). Enabled only if a single device group is selected.
 - **Delete** Click to delete selected device group(s) (select device group by checking 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 checking 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, follow these steps:

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

Step 2 Click the **Create** button.

The Create Device Group window appears, as shown in [Figure 3-93](#).

Figure 3-93 Create Device Group Window

Create Device Group

Name *

Description:

Devices:

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

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 3-94](#).

Figure 3-94 *Select Group Members Window*

Select Group Members

Members of the Device Group <>>

Show Devices with Name matching * **Find**

Showing 1 - 8 of 8 records

#	☐	Name	Description
1.	☐	pe1	
2.	☐	pe3	
3.	☐	sw2	
4.	☐	sw3	
5.	☐	sw4	
6.	☐	ce3	
7.	☐	ce8	
8.	☐	ce13	

Rows per page: 10

Go to page: 1 of 1

Step 5 Select the devices that you want to be group members by checking 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 3-95](#).

Figure 3-95 *Create Device Group Window*

Create Device Group

Name *: group2

Description:

Devices:

#	Name	Description
1.	pe1	
2.	pe3	

Rows per page: 10

Go to page: 1 of 1

Note: * - Required Field

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, follow these steps:

-
- Step 1** Choose **Service Inventory > Inventory and Connection Manager > Device Groups**.
 - Step 2** Select a single device group to modify by checking 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 3-96](#).

Figure 3-96 *Edit Device Group Window*

Edit Device Group

Name *: group2

Description:

#	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, follow these steps:

-
- Step 1** Choose **Service Inventory > Inventory and Connection Manager > Device Groups**.
 - Step 2** Select one or more device groups to delete by checking 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 3-97](#).

Figure 3-97 *Confirm Delete Window*

Confirm Delete

Showing 1-1 of 1 records

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

Rows per page: 10

Delete **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, follow these steps:

- Step 1** Choose **Service Inventory > Inventory and Connection Manager > Device Groups**.
- Step 2** Select the device groups for which you want to send a device report by checking 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 3-98](#).

Figure 3-98 *Send Mail to Device Owners of Selected Groups Window*

Send Mail to Device owners of selected groups

Please separate E-mail addresses using comma.

To:

CC:

Subject: Device Group Report

Message:

93826

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 3-112](#)
- [Creating a Customer, page 3-112](#)
- [Editing a Customer, page 3-113](#)
- [Deleting Customers, page 3-114](#)
- [Creating Customer Sites, page 3-115](#)
- [CPE Devices, page 3-116](#)

Accessing the Customers Window

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

To access the Customers window, follow these steps:

-
- Step 1** Choose **Service Inventory > Inventory and Connection Manager > Customers** to access the Customers window shown in [Figure 3-99](#).

Figure 3-99 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 a text input field containing an asterisk (*) and a 'Find' button. Below the search bar, it says 'Showing 1-3 of 3 records'. The main area is a table with a header row containing a '#' column, a checkbox column, and a 'Customer Name' column. The table lists three customers: 1. Customer01, 2. Customer1, and 3. Customer2, each with a corresponding checkbox. 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'. A vertical label '95238' is 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 checking the corresponding box). Enabled only if a single customer is selected.
 - **Delete** Click to delete selected customer (select customer by checking 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, follow these steps:

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

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

The Create Customer window appears, as shown in [Figure 3-100](#).

Figure 3-100 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 9 characters.
- **Customer Information** (optional) Any pertinent information about the customer that could be helpful to service provider operators. Limited to 256 characters.
- **Site of Origin Enabled** (optional) This check box appears only when you have MPLS permissions. Check this check box to enable the site of origin.

- Step 3** Enter the name and information for the Customer that you are creating. Check the **Site of Origin Enabled** check box if you want this enabled.
- Step 4** Click **Cancel** if you do not want to save this information, and you will proceed to the previous window. Otherwise, click **Save**. The changes are then saved and the Customers window reappears.

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, follow these steps:

- Step 1** Choose **Service Inventory > Inventory and Connection Manager > Customers**.
- Step 2** Select a single customer to modify by checking 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 3-101](#).

Figure 3-101 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 **Cancel** if you do not want to save this information, and you will proceed to the previous window. Otherwise, click **Save**. The changes are then 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, follow these steps:

- Step 1** Choose **Service Inventory > Inventory and Connection Manager > Customers**.
- Step 2** Select one or more customers to delete by checking 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 3-102](#).

Figure 3-102 Confirm Delete Window

Delete Customer

Confirm Delete

Showing 1-1 of 1 records

#	Name
1.	Customer2

Rows per page: 10

Delete **Cancel**

96241

- Step 4** Click **Cancel** if you do not want to save this information, and you will proceed to the previous window. Otherwise, click **Delete** 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, follow these steps:

- Step 1** Choose **Service Inventory > Inventory and Connection Manager**.
- Step 2** Click on **Customer Sites** listed in the Inventory and Connection Manager tree in the left column under Customers.
- The Customer Sites window appears.

Figure 3-103 Customer Sites Window

Customer Sites

Show Sites with Site Name matching *

Find

Showing 1 - 2 of 2 records

#	☐	Site Name	Customer Name
1.	☐	east	Customer1
2.	☐	west	Customer1

Rows per page: 10

Go to page: 1 of 1 **Go**

Create **Edit** **Delete**

158150

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 checking the corresponding box). Enabled only if a single customer site is selected.
- **Delete** Click to delete selected customer site(s) (select by checking the corresponding box(es)). Enabled only if one or more customer sites are selected.

CPE Devices

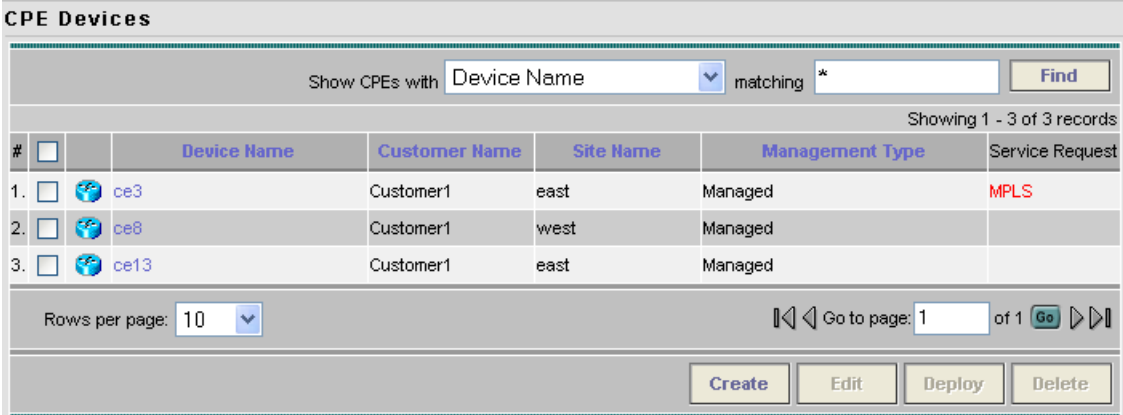
The CPE feature provides a list of CPEs that have been associated with a site through the CPE editor or Inventory Manager. To access the CPE Devices window, follow these steps:

Step 1 Choose **Service Inventory > Inventory and Connection Manager**.

Step 2 Click on **CPE Devices** listed in the Inventory and Connection Manager tree in the left column under Customers.

The CPE Devices window appears.

Figure 3-104 CPE Devices Window



CPE Devices

Show CPEs with matching

Showing 1 - 3 of 3 records

#	☐	Device Name	Customer Name	Site Name	Management Type	Service Request
1.	☐	 ce3	Customer1	east	Managed	MPLS
2.	☐	 ce8	Customer1	west	Managed	
3.	☐	 ce13	Customer1	east	Managed	

Rows per page:

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 (MVRFCE) 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

This section explains how to create a CPE device.

-
- Step 1** Click **Create** to create new CPE devices. Enabled only if no customer site is selected. The resulting window is shown in [Figure 3-105](#), “Create CPE Device Window.”

Figure 3-105 Create CPE Device Window

Create CPE Device

Device Name *		Select
Site Name *		Select
Management Type:	Managed	
		Save Cancel

Note: * - Required Field

116230

- Step 2** Click **Select** for the required **Device Name** and **Site Name**. For each, you receive a list of the devices and sites, respectively, from which you can choose one in each window and then click **Select**. Click **Cancel** if you do not want to save this information, and you will proceed to the previous window.
- Step 3** The drop-down window for **Management Type** allows you choose the management type of the CPE device you are creating.
- Step 4** Click **Cancel** if you do not want to save this information, and you will proceed to the previous window. Otherwise, click **Save**. The changes are saved and the CPE Device window reappears.

Edit CPE Device

Click **Edit** to edit a single CPE device selected in [Figure 3-104](#). The result is a window as shown in the example in [Figure 3-106](#), “[Edit CPE Device Window](#),” for which you can make changes and **Save**.

Figure 3-106 *Edit CPE Device Window*

Edit CPE Device

Device Name: ce3
 Site Name: east
 Customer Name: Customer1
 Management Type: Managed
 Pre-shared Keys:
 IPsec High Availability Options: ☒ None ☐ Normal Failover ☐ Stateful Failover
 IPsec Public IP Address:
 IP Address Ranges:

Show interfaces with Name matching *

#	Interface Name	IPv4 Address	IPv6 Address	IP Address Type	Encapsulation	Description	IPsec	Firewall	NAT	QoS C
1.	ATM1/0			STATIC	UNKNOWN		None	None	None	None
2.	ATM1/1			STATIC	UNKNOWN		None	None	None	None
3.	Ethernet0/1			STATIC	UNKNOWN		None	None	None	None
4.	Ethernet0/2			STATIC	UNKNOWN		None	None	None	None
5.	ATM1/2			STATIC	UNKNOWN		None	None	None	None
6.	Ethernet0/0	172.29.146.26/26		STATIC	UNKNOWN		None	None	None	None
7.	Ethernet0/3			STATIC	UNKNOWN		None	None	None	None
8.	Ethernet0/4			STATIC	UNKNOWN		None	None	None	None
9.	Serial1/0			STATIC	UNKNOWN		None	None	None	None
10.	Serial1/1			STATIC	UNKNOWN		None	None	None	None

Rows per page: 10 Go to page: 1 of 2

Save

211159

Delete CPE Device

Click **Delete** to delete selected CPE device(s) (select by checking the corresponding box). Enabled only if one or more CPE devices are selected. A Confirm Delete window allows you to continue with the deletion or cancel this deletion.

Providers

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

- [Accessing the Providers Window, page 3-120](#)
- [Creating a Provider, page 3-120](#)
- [Editing a Provider, page 3-121](#)
- [Deleting Providers, page 3-122](#)
- [Creating Provider Regions, page 3-123](#)
- [Creating PE Devices, page 3-124](#)
- [Creating Access Domains, page 3-125](#)

Accessing the Providers Window

The Providers feature is used to create and manage providers.

To access the Providers window, follow these steps:

- Step 1** Choose **Service Inventory > Inventory and Connection Manager > Providers** to access the Providers window shown in [Figure 3-107](#).

Figure 3-107 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' followed by an asterisk and a text input field, and a 'Find' button. Below the search bar, it says 'Showing 1 - 1 of 1 record'. The main table has two columns: '# Provider Name' and 'Provider BGP AS'. The first row shows '1. ☐ Provider1' and '99'. At the bottom, there is a 'Rows per page' dropdown set to '10', a 'Go to page: 1 of 1' with a 'Go' button, and 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.
- **Provider BGP AS** The Unique number assigned to each BGP autonomous system. Range: 1 to 65535.

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 a selected provider (check the corresponding box). Enabled only if a single provider is selected.
- **Delete** Click to delete selected provider(s) (check the corresponding box(es)). 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, follow these steps:

- Step 1** Choose **Service Inventory > Inventory and Connection Manager > Providers**.

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

The Create Provider window appears, as shown in [Figure 3-108](#).

Figure 3-108 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, follow these steps:

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

Step 2 Select a single provider to modify by checking 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 3-109](#).

Figure 3-109 *Edit Provider Window*

Edit Provider

Name * : ProviderA

BGP AS * : 100 (1 - 65535)

Contact Info:

Save Cancel

Note: * - Required Field

95244

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, follow these steps:

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

Step 2 Select provider(s) to delete by checking 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 3-110](#).

Figure 3-110 Confirm Delete Window

The screenshot shows a window titled "Delete Provider(s)". Inside, there is a sub-header "Confirm Delete" and a status bar indicating "Showing 1-1 of 1 records". Below this is a table with two columns: "#", which contains the value "1.", and "Name", which contains the value "ProviderA". Under 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".

- 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, follow these steps:

- Step 1** Choose **Service Inventory > Inventory and Connection Manager**.
- Step 2** Click on **Provider Regions** listed in the Inventory and Connection Manager tree in the left column under Providers.
- The Provider Regions window appears.

Figure 3-111 Provider Regions Window

The screenshot shows a window titled "Provider Regions". At the top, there is a search bar with the text "Show Regions with" followed by a dropdown menu set to "PE Region Name", the word "matching", and a text input field containing an asterisk (*). To the right of the input field is a "Find" button. Below the search bar, a status bar indicates "Showing 1 - 1 of 1 record". The main area contains a table with three columns: "#", "PE Region Name", and "Provider Name". The first row has the values "1.", "region_1", and "Provider1". Below the table, there is a "Rows per page:" label with a dropdown menu set to "10". To the right of this is a pagination control with "Go to page:" followed by a text input field containing "1", "of 1", a "Go" button, and navigation arrows. At the bottom right of the window, there are three buttons: "Create", "Edit", and "Delete".

The Provider Regions window contains the following:

- **PE 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 (check the corresponding box). Enabled only if a single provider region is selected.
- **Delete** Click to delete selected provider regions (check the corresponding box(es)). 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, follow these steps:

- Step 1** Choose **Service Inventory > Inventory and Connection Manager**.
- Step 2** Click on **PE Devices** listed in the Inventory and Connection Manager tree in the left column under Providers.

The PE Devices window appears.

Figure 3-112 PE Devices Window

The screenshot shows the 'PE Devices' window. At the top, there is a search bar with the text 'Show PEs with Device Name' and a dropdown menu. To the right of the search bar is a 'Find' button. Below the search bar, it says 'Showing 1 - 5 of 5 records'. The main part of the window is a table with the following columns: #, Device Name, Provider Name, PE Region Name, Role Type, and Service Request. The table contains five rows of data. At the bottom of the window, there is a 'Rows per page' dropdown set to 10, a 'Go to page' field set to 1 of 1, and three buttons: 'Create', 'Edit', and 'Delete'.

#	Device Name	Provider Name	PE Region Name	Role Type	Service Request
1.	pe1	Provider1	region_1	N-PE	QoS MPLS L2VPN
2.	pe3	Provider1	region_1	N-PE	QoS MPLS L2VPN
3.	sw2	Provider1	region_1	U-PE	
4.	sw3	Provider1	region_1	U-PE	L2VPN
5.	sw4	Provider1	region_1	U-PE	L2VPN

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: N-PE, U-PE, P, PE_AGG.

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 (check the corresponding box). Enabled only if a single PE device is selected.



Note Next to the PE Role Type, for both the Create and Edit selections, is a 6VPE check box. During the configuration collect operation, the device is detected as 6VPE if it is feature compatible.

- **Delete** Click to delete selected PE device(s) (check the corresponding box(es)). Enabled only if one or more PE devices are selected.

Creating Access Domains

To access the Access Domains window, follow these steps:

- Step 1** Choose **Service Inventory > Inventory and Connection Manager**.
- Step 2** Click on **Access Domains** listed in the Inventory and Connection Manager tree in the left column under Providers.

The Access Domains window appears.

Figure 3-113 Access Domains Window

The screenshot shows the 'Access Domains' window. At the top, there is a search bar with the text 'Show Access Domains with' followed by a dropdown menu set to 'Access Domain Name', the word 'matching', and a text input field containing an asterisk (*). A 'Find' button is to the right. Below the search bar, it says 'Showing 1 - 2 of 2 records'. The main area contains a table with two columns: '#', 'Access Domain Name', and 'Provider Name'. The first row shows a checkbox, '1.', 'Provider1:pe1', and 'Provider1'. The second row shows a checkbox, '2.', 'Provider1:pe3', and 'Provider1'. Below the table, there is a 'Rows per page' dropdown set to '10'. To the right, there is a 'Go to page:' field with '1' entered, followed by 'of 1' and a 'Go' button. At the bottom right, there are three buttons: 'Create', 'Edit', and 'Delete'. A vertical label '158155' is on the far right edge of the window.

#		Access Domain Name	Provider Name
1.	☐	Provider1:pe1	Provider1
2.	☐	Provider1:pe3	Provider1

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 a selected access domain (check the corresponding box). Enabled only if a single access domain is selected.
- **Delete** Click to delete selected access domain(s) (check the corresponding box(es)). 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 3-127](#)
- [Creating an IP Address Pool, page 3-128](#)
- [Creating a Multicast Pool, page 3-129](#)
- [Creating a Route Distinguisher and Route Target Pool, page 3-130](#)
- [Creating a Site of Origin Pool, page 3-132](#)
- [Creating a VC ID Pool, page 3-134](#)
- [Creating a VLAN Pool, page 3-134](#)
- [Deleting Resource Pools, page 3-136](#)

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, follow these steps:

- Step 1** Choose **Service Inventory > Inventory and Connection Manager > Resource Pools** to access the Resource Pools window shown in [Figure 3-114](#).

Figure 3-114 Resource Pools Window

The screenshot shows the 'Resource Pools' window. At the top, there is a 'Pool Type' dropdown menu set to 'IPv4 Address'. Below this is a search bar with the text 'Show IP Address Pools with Pool Name matching *' and a 'Find' button. A status bar indicates 'Showing 1 - 2 of 2 records'. The main area contains a table with the following data:

#	Start	Pool Mask	Pool Size	Status	Type	Pool Name
1.	10.10.10.0	32	256	Available	Region	Provider1:region_1
2.	11.11.11.0	30	64	Available	Region	Provider1:region_1

Below the table, there is a 'Rows per page' dropdown set to '10' and a 'Go to page: 1 of 1' section with a 'Go' button. At the bottom right, there are 'Create' and 'Delete' buttons.

From the Resource Pools window, you have access to the following buttons:

- **Pool Type** Choices include: IP Address, Multicast, 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 checking the corresponding box(es)). 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, follow these steps:

- Step 1** Choose **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 3-115](#).

Figure 3-115 Create IP Address Pool Window

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**, **VPN**, and **Customer** from the drop-down list. Then you can click the **Select** button to receive all selections for the choice you made in the drop-down list. From this new window, make your selection and click **Select**.



Note If you choose **VPN**, an additional optional field appears, **Pool Name Suffix**, when you return to [Figure 3-115](#). 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, follow these steps:

Step 1 Choose **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 3-116](#).

Figure 3-116 Create Multicast Pool Window

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, follow these steps:

- Step 1** Choose **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 3-117](#).

Figure 3-117 Create Route Distinguisher Pool Window

Create Route Distinguisher Pool

RD Pool Start *	0	(0 - 2147483646)
RD Pool Size *	0	(1 - 2147483647)
Provider *		Select

Save Cancel

Note: * - Required Field

96304

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 3-118](#).

Figure 3-118 Provider for New Resource Pool Window

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, follow these steps:

Step 1 Choose **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 3-119](#).

Figure 3-119 Create Route Target Pool Window

The Create Route Target Pool window contains the following fields:

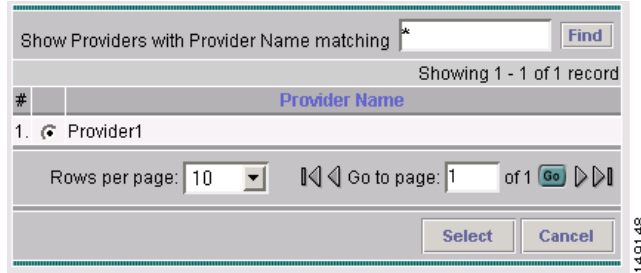
- **RT Pool Start** (required) Range: 0 to 2147483646.
- **RT Pool Size** (required) Range: 1 to 2147483647.
- **Provider** (required)

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 3-120](#).

Figure 3-120 Provider for New Resource Pool Window



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, follow these steps:

- Step 1** Choose **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 3-121](#).

Figure 3-121 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

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 3-122](#).

Figure 3-122 Provider for New Resource Pool Window

Show Providers with Provider Name matching* **Find**

Showing 1 - 1 of 1 record

#	Provider Name
1.	Provider1

Rows per page: 10 **Go**

Select **Cancel**

- 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, follow these steps:

-
- Step 1** Choose **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 3-123](#).

Figure 3-123 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.

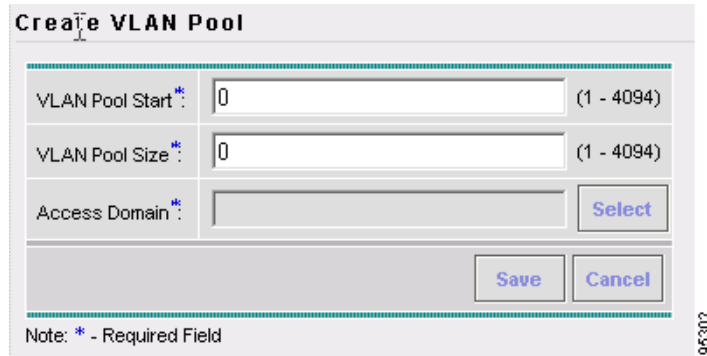
Creating a VLAN Pool

From the Create VLAN Pool window, you can create VLAN pools.

To create a VLAN pool, follow these steps:

-
- Step 1** Choose **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 3-124](#).

Figure 3-124 Create VLAN Pool Window


The 'Create VLAN Pool' window contains the following fields:

- VLAN Pool Start** (required): A text box with '0' entered, with '(1 - 4094)' to its right.
- VLAN Pool Size** (required): A text box with '0' entered, with '(1 - 4094)' to its right.
- Access Domain** (required): A text box with a 'Select' button to its right.

At the bottom right are 'Save' and 'Cancel' buttons. A note at the bottom left states: 'Note: * - Required Field'. A vertical label '96302' is on the right side.

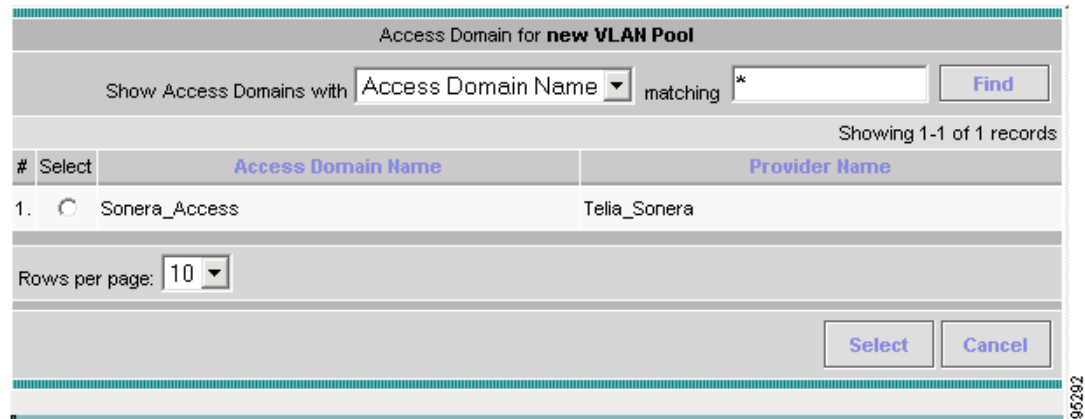
The Create VLAN Pool window contains the following fields:

- **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 3-125](#).

Figure 3-125 Access Domain for new VLAN Pool Window


The 'Access Domain for new VLAN Pool' window shows a search interface. At the top, it says 'Access Domain for new VLAN Pool'. Below that, a search bar contains 'Show Access Domains with' followed by a dropdown menu showing 'Access Domain Name', the word 'matching', and a text box with an asterisk '*'. A 'Find' button is to the right. Below the search bar, it says 'Showing 1-1 of 1 records'. A table lists the results:

#	Select	Access Domain Name	Provider Name
1.	☐	Sonera_Access	Telia_Sonera

Below the table, there is a 'Rows per page:' dropdown menu set to '10'. At the bottom right are 'Select' and 'Cancel' buttons. A vertical label '96292' is on the right side.

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.

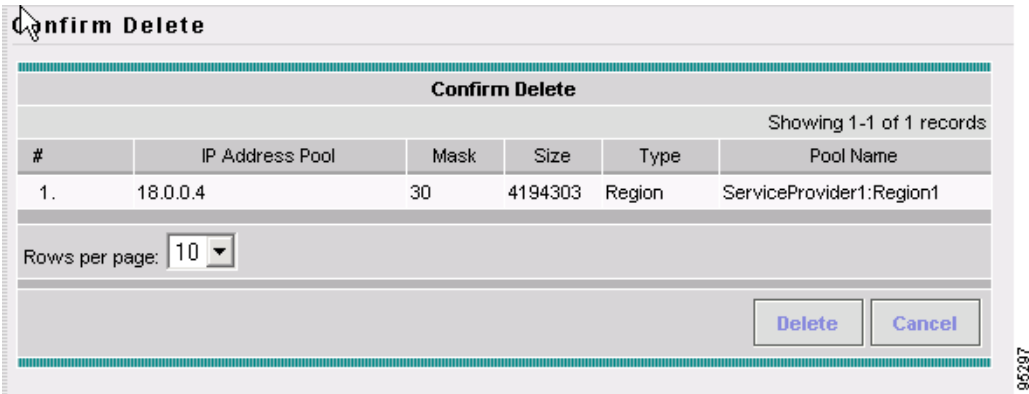
Deleting Resource Pools

From the Resource Pool window, you can delete specific resource pools.
To delete resource pools, follow these steps:

- Step 1** Choose **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 checking the check box(es) to the left of the resource pool(s).
- Step 4** Click the **Delete** button.

The Confirm Delete window appears, as shown in [Figure 3-126](#).

Figure 3-126 Confirm Delete Window



- 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 3-137](#)
- [Creating CE Routing Communities, page 3-138](#)
- [Deleting CE Routing Communities, page 3-139](#)

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, follow these steps:

- Step 1** Choose **Service Inventory > Inventory and Connection Manager > CE Routing Communities** to access the CE Routing Communities window shown in [Figure 3-127](#).

Figure 3-127 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', the word 'matching', an asterisk in a text box, and a 'Find' button. Below this, it says 'Showing 1 - 2 of 2 records'. The main area contains a table with the following data:

#	☐	Name	HRT	SRT	Provider	VPN
1.	☐	Mpls-VPN-1	99:1	99:2	Provider1	Mpls-VPN-1
2.	☐	Mpls-VPN-2	99:3	99:4	Provider1	Mpls-VPN-2

Below the table, there is a 'Rows per page:' dropdown set to '10'. To the right, there is a pagination control with 'Go to page: 1 of 1' and 'Go' and 'Find' buttons. At the bottom right, there are three buttons: 'Create', 'Edit', and 'Delete'.

149436

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 checking the corresponding box). Enabled only if one CE routing community is selected.
- **Delete** Click to delete selected CE routing communities (select by checking 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, follow these steps:

Step 1 Choose **Service Inventory > Inventory and Connection Manager > CE Routing Communities**.

Step 2 Click **Create**.

The Create CE Routing Community window appears, as shown in [Figure 3-128](#).

Figure 3-128 Create CE Routing Community Window

Create CE Routing Community

Provider Name *:

Name *:

CERC Type: ☒ Hub and Spoke ☐ Fully Meshed

Auto-pick route target values: ☒

Route Target 1:

Route Target 2:

Note: * - Required Field

158156

- Step 3** Complete the CERC fields as required for the CE Routing Community:
- Provider Name** (required) To specify the service provider associated with this CERC, click **Select**. The Select Provider dialog box is displayed.
 - From this new window, 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 checked. If you uncheck 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), follow these steps:

- Step 1** Choose **Service Inventory > Inventory and Connection Manager > CE Routing Communities**

- Step 2** Select CERC(s) to delete by checking 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 3-140](#)
- [Creating a VPN, page 3-141](#)
- [Deleting VPNs, page 3-144](#)

Accessing the VPNs Window

The VPN feature is used to create and manage various types of VPNs.

To access the VPN window, follow these steps:

-
- Step 1** Choose **Service Inventory > Inventory and Connection Manager > VPN** to access the VPN window shown in [Figure 3-129](#).

Figure 3-129 VPNs Window

The screenshot shows the 'VPNs' window with a search bar at the top. Below the search bar, it says 'Showing 1 - 6 of 6 records'. The table has two columns: 'VPN Name' and 'Customer Name'. There are six rows of data. At the bottom, there are buttons for 'Create', 'Edit', and 'Delete', and a 'Rows per page' dropdown set to 10.

#	VPN Name	Customer Name
1.	Mpls-VPN-1	Customer1
2.	Mpls-VPN-2	Customer1
3.	Vpn1	Customer1
4.	Vpn2	Customer1
5.	Vpn3	Customer2
6.	Vpn4	Customer2

Rows per page: 10 Go to page: 1 of 1

Create Edit Delete

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 a selected VPN (check the corresponding box). Enabled only if one VPN is selected.
- **Delete** Click to delete selected VPN(s) (check the corresponding box(es)). Enabled only if one or more VPNs is selected.

Creating a VPN

To create a VPN, follow these steps:

- Step 1** Choose **Service Inventory > Inventory and Connection Manager > VPN**.
- Step 2** Click **Create**.

The Create VPN window appears, as shown in [Figure 3-130](#).

Figure 3-130 Create VPN Window

Create VPN

Name *:

Customer *:

MPLS Attributes

Create Default CE Routing Community: ☐

Enable Unique Route Distinguisher: ☐

Enable Multicast: ☐

Enable Auto Pick MDT Addresses: ☒

Default MDT Address *: (a.b.c.d)

Data MDT Subnet: (a.b.c.d)

Data MDT Size:

Data MDT Threshold: (1 - 4294967 kilobits/sec)

Default PIM Mode:

MDT MTU: (576 - 18010)

Enable PIM SSM: ☐

SSM List Name *:

Multicast Route Limit: (1 - 2147483647)

Enable Auto RP Listener: ☐

Configure Static-RP: ☐

PIM Static-RPs *:

Showing 0 of 0 records

#	Static-RP Unicast Address	Multicast-Group List Name	Override
Rows per page: 10 Go of 1 Go			

CE Routing Communities:

VPLS Attributes

Enable VPLS: ☐

VPN ID: (1-2147483646)

Service Type:

Topology:

Note: * - Required Field

211160

- Step 3** Complete the fields as required for the VPN:
- Name** (required) Enter the name of the VPN.
 - Customer** (required) To select the customer associated with this VPN, choose **Select**.
 - From the list of customers, select the appropriate customer, then click **Select**.

- d. **If you want MPLS attributes, complete the fields in the MPLS Attributes section of the window. For VPLS, skip to step u.**
- e. **Create Default CE Routing Community** (optional) To create a default CE routing community, check the **Create Default CE Routing Community** check box and select a provider.
- f. **Enable Unique Route Distinguisher** The BGP Multipath Load Sharing for Both eBGP and iBGP in an MPLS VPN feature is enabled only under the IPv4 VRF address family configuration mode. When enabled, this feature can perform load balancing on eBGP and/or iBGP paths that are imported into the VRF.
- g. **Enable Multicast** To enable multicast VPN routing, check 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.

- h. **Enable Auto Pick MDT Addresses** (optional) To enable auto picking MDT addresses, check the **Enable Auto Pick MDT Addresses** check box.
- i. **Default MDT Address** If **Enable Auto Pick MDT Addresses** is set on, **Default MDT Address** is required.
- j. **Data MDT Subnet** (optional)
- k. **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.

- l. **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.

- m. **Default PIM Mode** (optional)
- n. **Enable PIM SSM** (optional)
- o. **SSM List Name**
- p. **Multicast Route Limit** (optional)
- q. **Enable Auto RP Listener** (optional)
- r. **Configure Static-RP** (optional)
- s. **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.

- t. Check 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.

- u. If you want VPLS attributes, the optional fields for that are in v. to y.
- v. **Enable VPLS** (optional) Check this check box to enable VPLS.
- w. **VPN ID** (optional)
- x. **Service Type** (optional) Click the drop-down list and choose from ERS (Ethernet Relay Service) or EWS (Ethernet Wire Service).
- y. **Topology** (optional) Select the VPLS topology from the drop-down list: 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), follow these steps:

- Step 1** Choose **Service Inventory > Inventory and Connection Manager > VPN**.
 - Step 2** Select VPN(s) to delete by checking the check box(es) 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.
-

Named Physical Circuits

Named physical circuits (NPCs) are named circuits that describe a physical connection between a CPE or U-PE and an N-PE. 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/U-PE and the destination N-PE 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 U-PE and the last device *must* be an N-PE.
- 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 3-145](#)
- [Creating a Named Physical Circuit, page 3-146](#)
- [Deleting Named Physical Circuits, page 3-150](#)
- [Creating NPC Rings, page 3-150](#)
- [Editing NPC Rings, page 3-154](#)
- [Deleting NPC Rings, page 3-154](#)

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, follow these steps:

-
- Step 1** Choose **Service Inventory > Inventory and Connection Manager > Named Physical Circuits** to access the window shown in [Figure 3-131](#), “[Named Physical Circuits Window](#).”

Figure 3-131 Named Physical Circuits Window

Named Physical Circuits

Show NPCs where matching

Showing 1 - 10 of 13 records

#	☐	Source Device	Source Interface	Destination Device	Destination Interface	Name
1.	☐	sw3	GigabitEthernet0/2	pe1	FastEthernet0/0	1-(sw3-GigabitEthernet0/2) <==>(pe1-FastEthernet0/0)
2.	☐	sw2	FastEthernet0/1	pe1	Ethernet4/2	10-(sw2-FastEthernet0/1) <==>(pe1-Ethernet4/2)
3.	☐	sw3	FastEthernet1/1	pe1	Ethernet4/0	11-(sw3-FastEthernet1/1) <==>(pe1-Ethernet4/0)
4.	☐	sw3	GigabitEthernet0/5	pe1	Ethernet4/1	12-(sw3-GigabitEthernet0/5)<==> (pe1-Ethernet4/1)
5.	☐	sw4	FastEthernet0/1	pe1	FastEthernet0/1	13-(sw4-FastEthernet0/1) <==>(pe1-FastEthernet0/1)
6.	☐	ce8	FastEthernet0/1	pe1	FastEthernet0/0	2-(ce8-FastEthernet0/1) <==>(pe1-FastEthernet0/0)
7.	☐	sw4	FastEthernet0/2	pe3	FastEthernet0/0	3-(sw4-FastEthernet0/2) <==>(pe3-FastEthernet0/0)
8.	☐	ce13	Ethernet1	pe3	FastEthernet0/0	4-(ce13-Ethernet1)<==> (pe3-FastEthernet0/0)
9.	☐	ce3	Ethernet0/1	pe1	Ethernet4/3	5-(ce3-Ethernet0/1)<==> (pe1-Ethernet4/3)
10.	☐	ce3	Ethernet0/2	pe1	Ethernet4/4	6-(ce3-Ethernet0/2)<==> (pe1-Ethernet4/4)

Rows per page:

Go to page: of 2

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 NPC(s) (select by checking the corresponding box(es)). Enabled only if one or more NPCs are selected.

Creating a Named Physical Circuit

To add an NPC physical link, follow these steps:

- Step 1** Choose **Service Inventory > Inventory and Connection Manager > Named Physical Circuit**.
- Step 2** Click the **Create** button in Figure 3-131, “Named Physical Circuits Window,” and a window, as shown in Figure 3-132, “Create a Named Physical Circuit Window,” appears.

Figure 3-132 Create a Named Physical Circuit Window

#	Device	Incoming Interface	Outgoing Interface	Ring
Insert Device Insert Ring Add Device Add Ring Delete Save Cancel				

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 3-150.



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 3-133](#), “[Select Device Window](#),” appears.

Figure 3-133 Select Device Window

Show **CPE** devices where **Device Name** matching *

Showing 1 - 3 of 3 records

#	Device Name	Customer Name	Site Name	Management Type
1.	☐ ce13	Customer1	east	MANAGED
2.	☐ ce3	Customer1	east	MANAGED
3.	☐ ce8	Customer1	east	MANAGED

Rows per page: 10 Go to page: 1 of 1

Step 4 Be sure that the drop-down list in **Show** is **CPE** or **PE**. Click a radio button next to a device and then click **Select**.

Step 5 [Figure 3-132](#), “[Create a Named Physical Circuit Window](#),” reappears with the chosen **Device**.

Figure 3-134 Create Named Physical Circuit Window

#	Device	Incoming Interface	Outgoing Interface	Ring
1.	☐ ence21		Select outgoing interface	
2.	☐ mlce203	Select incoming interface		

Buttons: 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 checked in the check box, click the **Add Device** button in [Figure 3-132 on page 3-147](#) 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 checked in the check box, click the **Insert Device** button in [Figure 3-132 on page 3-147](#) 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 3-132](#), “Create a Named Physical Circuit Window,” click **Select outgoing interface** and a window as shown in [Figure 3-135](#), “Select Outgoing Interface Window,” appears with a list of interfaces.

Figure 3-135 Select Outgoing Interface Window

Interfaces for device **ence11**

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 3-132](#), “Create a Named Physical Circuit Window,” reappears with the chosen **Interface**.
- Step 10** In the **Incoming Interface** column in this new version of [Figure 3-132](#), “Create a Named Physical Circuit Window,” click **Select incoming interface** and a window as shown in [Figure 3-136](#), “Select Incoming Interface Window,” appears with a list of interfaces.

Figure 3-136 *Select Incoming Interface Window*

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 11 Click a radio button next to the interface to be the incoming interface for this NPC and then click **Select**.

Step 12 [Figure 3-132](#), “Create a Named Physical Circuit Window,” 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 3-150, you can click **Insert Ring** or **Add Ring** and the ring appears at the beginning or before the item checked in the check box for **Insert Ring** or the ring appears at the end or after the item checked in the check box for **Add Ring**, as shown in [Figure 3-137](#), “Select NPC Ring Window.”

**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 3-137 *Select NPC Ring Window*

ShowNPC rings matching

Showing 1-1 of 1 records

#	Select	Ring Name
1.	☐	1-enpe1-Ethernet2/0

Rows per page:

Step 14 Click a radio button next to the ring you choose and then click **Select**.

Step 15 [Figure 3-132](#), “Create a Named Physical Circuit Window,” reappears with the chosen **Ring**.

- Step 16** Select the missing devices and interfaces as explained in the “[Creating NPC Rings](#)” section on [page 3-150](#).
- Step 17** Click **Cancel** if you do not want to save this information, and you will proceed to the previous window. Otherwise, click **Save**. [Figure 3-132](#), “[Create a Named Physical Circuit Window](#),” reappears with the new NPC listed.

Deleting Named Physical Circuits

To delete NPC(s), follow these steps:

- Step 1** Choose **Service Inventory > Inventory and Connection Manager > Named Physical Circuits** to access the window shown in [Figure 3-131](#), “[Named Physical Circuits Window](#).”
- Step 2** Select one or more NPCs to delete by checking 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 3-131](#), “[Named Physical Circuits Window](#),” reappears with the specified NPCs deleted.

Creating NPC Rings

To create NPC rings, follow these steps:

- Step 1** Choose **Service Inventory > Inventory and Connection Manager > NPC Rings** and a window as shown in [Figure 3-138](#), “[NPC Rings Window](#),” appears.

Figure 3-138 *NPC Rings Window*

- Step 2** Click the **Create** button and a window as shown in [Figure 3-139](#), “**Create Ring Window**,” appears. A ring has a minimum of three physical links that form a ring.

Figure 3-139 Create Ring Window

#	Source Device	Source Interface	Destination Device	Destination Interface
1.	☐ Select source device	Select source interface	Select destination device	Select destination interface
2.	☐ Select source device	Select source interface	Select destination device	Select destination interface
3.	☐ Select source device	Select source interface	Select destination device	Select destination interface

Buttons: [Edit Cross Links](#) [Insert](#) [Delete](#) [Save](#) [Cancel](#)



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 3-140](#), “**Select Source Device — CPE/PE Window**,” appears.



Note The CPE you choose *must* be a Multi-VRF CE.

Figure 3-140 Select Source Device — CPE/PE Window

Show [CPE](#) devices where [Device Name](#) matching [Find](#)

Showing 1 - 3 of 3 records

#	Device Name	Customer Name	Site Name	Management Type
1.	☐ ce13	Customer1	east	MANAGED
2.	☐ ce3	Customer1	east	MANAGED
3.	☐ ce8	Customer1	east	MANAGED

Rows per page: [10](#) Go to page: [1](#) of 1 [Go](#)

Buttons: [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 3-139](#), “**Create Ring Window**,” 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 3-139](#), “**Create Ring Window**,” click **Select source interface** and a window as shown in [Figure 3-141](#), “**Select Source Interface Window**,” appears with a list of interfaces.

Figure 3-141 Select Source Interface Window

Interfaces for device **ce13**

Show Device Interfaces with **Interface Name** matching * **Find**

#	Interface Name	IP Address	Logical Name
1.	☐ Ethernet0	172.29.146.36/26	
2.	☐ Ethernet1		

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

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 3-139, “Create Ring Window,” reappears with the chosen **Source Interface**.
- Step 10** In the **Destination Device** column in this new version of Figure 3-139, “Create Ring Window,” click **Select destination device** and a window as shown in Figure 3-142, “Select Destination Device — CPE/PE Window,” appears.

Figure 3-142 Select Destination Device — CPE/PE Window

Show **PE** devices where **Device Name** matching * **Find**

Showing 1 - 3 of 3 records

#	Device Name	Customer Name	Site Name	Management Type
1.	☐ ce13	Customer1	east	MANAGED
2.	☐ ce3	Customer1	east	MANAGED
3.	☐ ce8	Customer1	east	MANAGED

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

Select **Cancel**

- 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 3-139, “Create Ring Window,” 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 3-139, “Create Ring Window,” click **Select destination interface** and a window as shown in Figure 3-143, “Select Destination Interface Window,” appears with a list of interfaces.

Figure 3-143 Select Destination Interface Window

Interfaces for device **ce3**

Show Device Interfaces with matching

#	Interface Name	IP Address	Logical Name
1.	☐ ATM1/0		
2.	☐ ATM1/1		
3.	☐ ATM1/2		
4.	☐ Ethernet0/0	172.29.146.26/26	
5.	☐ Ethernet0/1		
6.	☐ Ethernet0/2		
7.	☐ Ethernet0/3		
8.	☐ Ethernet0/4		
9.	☐ Serial1/0		
10.	☐ Serial1/1		

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 3-139](#), “[Create Ring Window](#),” 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, check 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, check 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 3-139](#), “[Create Ring Window](#),” and you then view a new window like [Figure 3-139](#) 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 3-139](#) 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.



Note To **Edit Cross Links**, a minimum of four devices is needed to form this ring.

- Step 20** Click **Cancel** if you do not want to save this information, and you will proceed to the previous window. Otherwise, when you have completed setting up your ring click **Save**. The new ring is added in [Figure 3-138](#), “[NPC Rings Window](#),” and a green check for Succeeded appears. The new ring is identified by the source device-source interface.
- Step 21** To create a ring with more than three physical links, check the check box for the link in [Figure 3-139](#) on [page 3-151](#) 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, follow these steps:



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** Choose **Service Inventory > Inventory and Connection Manager > NPC Rings** and a window as shown in [Figure 3-144](#), “NPC Rings Window,” appears.

Figure 3-144 NPC Rings Window

- Step 2** Check the **check box next to the line that represents an NPC ring and then click Edit**. A window as shown in [Figure 3-139](#), “Create Ring Window,” appears with all the data for this ring. Proceed as in the “Creating NPC Rings” section on page 3-150 to make any changes you want.
- Step 3** When you have the ring as you want it, click **Save**.
- Step 4** [Figure 3-138](#), “NPC Rings Window,” appears with the appropriate name (source device-source interface) and a green check for Succeeded appears.

Deleting NPC Rings

To delete NPC rings, follow these steps:



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** Choose **Service Inventory > Inventory and Connection Manager > NPC Rings** and a window as shown in [Figure 3-145](#), “NPC Rings Window,” appears.

Figure 3-145 NPC Rings Window

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** Check 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 3-146](#), “Delete Rings Window,” appears with the chosen ring(s) for deletion.

Figure 3-146 Delete Rings Window

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 3-145](#), “NPC Rings Window,” appears with the remaining ring names and a green check for Succeeded appears.



CHAPTER 4

Service Inventory—Discovery

This chapter describes how to use the Discovery feature to discover devices, connections, and services for the IP Solution Center (ISC) provisioning process. It contains the following sections:

- [Overview of ISC Discovery, page 4-1](#)
- [Technical Notes for ISC Discovery, page 4-5](#)
- [Summary of Tasks for Discovery \(Cisco ISC MPLS VPN Management and L2VPN Management\), page 4-8](#)
- [Summary of ISC Discovery Steps for MPLS Diagnostics Expert, page 4-12](#)
- [Step 1: Perform Preliminary Steps, page 4-15](#)
- [Step 2: Perform Device Discovery, page 4-25](#)
- [Step 3: Perform Discovery Data Collection, page 4-37](#)
- [Step 4: Perform Role Assignment, page 4-37](#)
- [Step 5: Perform NPC Discovery, page 4-50](#)
- [Step 6: Perform MPLS VPN Service Discovery \(Optional\), page 4-57](#)
- [Step 7: Perform L2VPN \(Metro Ethernet\) Service Discovery \(Optional\), page 4-66](#)
- [Step 8: Commit Discovered Devices and Services to ISC Repository, page 4-78](#)
- [Step 9: Create and Run a Collect Config Task for the Discovered Devices, page 4-79](#)
- [Step 10: View and Edit Services, page 4-79](#)

Overview of ISC Discovery

ISC can expedite the process for building a network device inventory by discovering the devices, connections, and services that your MPLS VPN or L2VPN Metro Ethernet network comprises.



Note

Service discovery is a complex operation that can be impacted by many variables within the network. The original network configuration must have been performed in accordance with the same rules that ISC follows when provisioning services. Otherwise, errors might occur during the discovery. As a result of the many possible configurations in a given network, it is strongly recommended that you contact your Cisco account team or Cisco advanced services to provide support, before committing to the service discovery process.

Users who run service discovery should have a thorough understanding of their overall network topology, should be familiar with network terminology, such as: PE, N-PE, U-PE, PE-AGG, and CE, and should understand the definition of NPC and Metro Ethernet/MPLS services in ISC.

ISC supports the discovery process for admin users only.

The ISC Discovery feature can be used to provision three of the applications in the Cisco ISC application suite:

- Cisco IP Solution Center MPLS VPN Management
- Cisco IP Solution Center L2VPN Management
- Cisco IP Solution Center MPLS Diagnostics Expert


Note

Service discovery does not support Secure Shell version 2 (SSHv2) as a terminal session protocol. MPLS and L2VPN service discovery do not support devices running IOS XR.

When a device in ISC only has a hostname, the ISC device has no IP management address or domain name configured. If in Discovery, a device with the same hostname is discovered with an IP management address or is created manually in the Device Editor, the device might fail to commit to the ISC repository. The failure occurs because a match is determined with the existing ISC device, because both devices do not have a configured domain name.

The workaround is to do either 1. or 2., as follows:

1. Edit the device that exists in ISC and add the management IP address before Discovery. Discovery then treats that device as a duplicate and marks it read-only in the Device Editor.

or

2. During Discovery, in the Device Editor, enter a domain name for the discovered device. Discovery then treats this as a new device.

The Cisco IP Solution Center Traffic Engineering Management has its own Discovery interface and process. This is documented in Chapter 2 of the [Cisco IP Solution Center Traffic Engineering Management User Guide, 5.0](#), “TE Network Discovery.”

Multiple service discovery processes are supported and you can restart from any of the previous steps. Support for multiple discovery processes allows you to do incremental discovery of the network. The ability to restart from previous steps helps you roll back the discovery process to a selected previous step. You can then resume discovery from that step instead of needing to restart the entire discovery process from the beginning. Restarting from discovery data collection prompts the user to select devices for which data needs to be collected.

Incremental discovery occurs for existing VPN links. The existing VPNs are not editable in the discovery GUI and the existing VPN links are by-passed during commit.

There is no synchronization in MPLS and L2VPN service discovery. Any modification must be done manually through the ISC user interface. Only new VPNs are discovered. Also, services on existing modified NPCs and conflicting NPCs are not discovered.

The commit to ISC happens only at the end of the discovery phase, not after each step. The Discovery process does not change the state of ISC during discovery workflow. It is only at the end of the workflow that a user can commit the discovered devices and services to ISC.

The Discovery process provides you with several choices on how to discover your network topology.

3. If you are running Discovery to provision Cisco IP Solution Center MPLS VPN Management or Cisco IP Solution Center L2VPN Management, you can choose between three Discovery methods:

- a. CDP Discovery

You can use the Cisco Discovery Protocol (CDP) to discover devices connected to an initial device that has an IP address you provide in a **policy.xml** file.

- b. Device/Topology Based Discovery

You can use a Device/Topology-based method. This method uses XML files that specify device and NPC topology information.

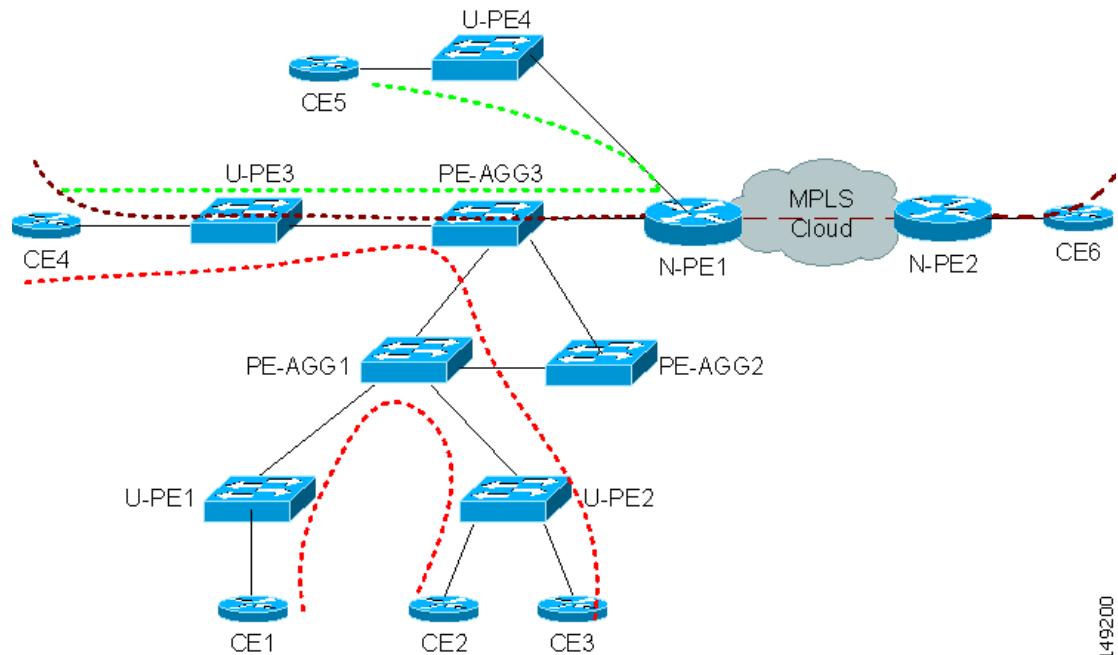
- c. Import Configuration File Based

You can use an Import Configuration Files-based method. This method uses a directory on the server that contains configuration files for the devices to be discovered and an XML file that contains device connectivity information that is used to automatically create NPCs.

4. You can choose the network topology to discover an MPLS VPN topology, an L2VPN (Metro Ethernet) topology, or both.

If you choose L2VPN (Metro Ethernet) Discovery, you can discover either a Metro Ethernet with an MPLS core, a Metro Ethernet with an Ethernet core, or a combination of the two, a mixed core. In a mixed core, the L2VPN services can span across the MPLS core or they can be confined to a local Ethernet domain alone (local switched services). Local switched services that do not traverse N-PE devices across an ethernet domain can also be discovered. [Figure 4-1](#), “Mixed Core,” shows a mixed core.

Figure 4-1 Mixed Core



[Figure 4-2](#) illustrates the phases in the Discovery process.

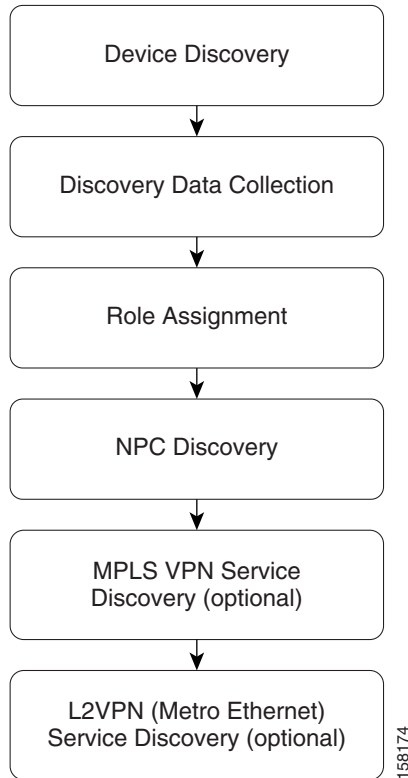
Figure 4-2 *ISC Discovery Steps*

Table 4-1 describes the phases in the Discovery process.

Table 4-1 *Steps in the Discovery Process*

Step	Description
Device Discovery	Discovers devices in the MPLS VPN and/or Metro Ethernet topology.
Discovery Data Collection	Collects the IOS configuration for the devices discovered.
Role Assignment	Does the role assignment for the discovered devices based on rules.xml, and prompts you to edit the device roles as N-PE, U-PE, or CE. Note A sample is found at: \$ISC_HOME/resources/discovery/data/rules.xml, where the rules.xml file must be kept.
NPC Discovery	Displays discovered NPCs and allows addition or removal of NPCs.

Table 4-1 Steps in the Discovery Process (continued)

Step	Description
MPLS VPN Discovery	Discovers the topology for your MPLS VPN network and allows you to change it as required. Note The MPLS VPN Discovery step is not required if you are using ISC Discovery with Cisco IP Solution Center MPLS Diagnostics Expert.
(L2VPN) Metro Ethernet Discovery	Discovers the topology for your Metro Ethernet network and allows you to change it as required. Note The (L2VPN) Metro Ethernet Discovery step is not required if you are using ISC Discovery with Cisco IP Solution Center MPLS Diagnostics Expert.

Technical Notes for ISC Discovery

This section presents technical tips and general information about the ISC Discovery process.

The ISC Discovery feature can be used to provision three of the applications in the Cisco ISC application suite:

- Cisco IP Solution Center MPLS VPN Management
- Cisco IP Solution Center L2VPN Management
- Cisco IP Solution Center MPLS Diagnostics Expert

Although the general steps are similar, there are some differences in the workflow for the various types of Discovery. These are described in the section covering each ISC application:

- [Using ISC Discovery with Cisco IP Solution Center MPLS VPN Management, page 4-6](#)
- [Using ISC Discovery With Cisco IP Solution Center L2VPN Management, page 4-7](#)
- [Using ISC Discovery with Cisco IP Solution Center MPLS Diagnostics Expert, page 4-7](#)
- [Using ISC Discovery With Cisco IP Solution Center Traffic Engineering Management, page 4-8](#)



Note

Cisco IP Solution Center Traffic Engineering Management has its own Discovery interface and process. This is documented in Chapter 2 of the [Cisco IP Solution Center Traffic Engineering Management User Guide, 5.0](#), “TE Network Discovery.”

For technical notes on using ISC Discovery in installations that include both Cisco IP Solution Center Traffic Engineering Management and Cisco IP Solution Center MPLS VPN Management, see [Using ISC Discovery With Cisco IP Solution Center Traffic Engineering Management, page 4-8](#).

General Notes

Note the following points before running ISC Discovery:

- You can use the ISC GUI to create providers, customers, and resource pools before doing Discovery.
- Only one user can control the Discovery workflow interface at a given time.
- The procedures in the chapter show a “generic” procedure. If you do not have licenses for a particular application, you will not see the selections for that application on the start screen for ISC Discovery.
- Perform “manual” device collection after discovery is over.
- After you have started the Discovery process, a **Restart** button appears on the Discovery Workflow window. You can click the **Restart** button, a drop-down list of completed steps pops up and you can select a step and restart from that step.
- Restarting from initialization aborts the current discovery process.
- Discovery using Role Based Access Control (RBAC) is not supported.

Using the Discovery Log Files

A log file is written for each phase of the Discovery process. You can view a log file by clicking the **View** selection in the Log column next to each discovery phase summary on the Discovery Workflow window.

The log file provides useful information in the event a discovery step fails.

Using ISC Discovery with Cisco IP Solution Center MPLS VPN Management

If you are running the Discovery process to discover an MPLS VPN network for use with Cisco IP Solution Center MPLS VPN Management, note the following points:

- You must perform all of the main steps in the Discovery process.
- You can use either CDP Discovery, Device/Topology, or Import Configuration Files-based Discovery. The recommendation is to use either Device/Topology or Import Configuration Files-based Discovery.
- ISC does not support partial mesh VPN topologies. If the Discovery process discovers a Partial Mesh VPN, you must split the partial mesh VPN into smaller units (usually a combination of full mesh VPNs and Hub and Spoke VPNs).
- After completion of the automated Discovery process, you must schedule and run a **Task Manager > Collect Config** task for all discovered devices.



Note

There is no synchronization in MPLS service discovery. Any modification must be done manually through the ISC user interface. Only new VPNs are discovered. Also, services on existing modified NPCs and conflicting NPCs are not discovered.

Using ISC Discovery With Cisco IP Solution Center L2VPN Management

If you are running the Discovery process to discover an L2VPN network that will be provisioned and managed using Cisco IP Solution Center L2VPN Management, note the following points:

- You must perform all of the main steps in the Discovery process.
- You can use either CDP Discovery, Device/Topology, or Import Configuration Files-based Discovery. The recommendation is to use either Device/Topology or Import Configuration Files-based Discovery.
- A new L2VPN service is discovered when any of the following are found compared to the services existing in ISC:
 - A new Virtual LAN Identifier (VLAN ID) in an Ethernet core (Ethernet access domain)
 - A new Virtual Circuit Identifier (VC ID) for virtual private wire service (VPWS) services on an MPLS core.
 - A new VPLS Forwarding Instance Identifier (VFI ID) for virtual private LAN service (VPLS) services on an MPLS core.
- The Discovery process for Cisco IP Solution Center L2VPN Management can discover Metro Ethernet with an MPLS core, an Ethernet core, or both.
- Prior to performing the NPC Discovery step for Cisco IP Solution Center L2VPN Management, you must specify the Access Domain for N-PE devices.
- Any new links that are configured on NPCs marked as Existing Modified or Conflicting are not discovered.
- After completion of the automated Discovery process, you must schedule and run a **Task Manager > Collect Config** task for all discovered devices.

**Note**

There is no synchronization in L2VPN service discovery. Any modification must be done manually through the ISC user interface. Only new VPNs are discovered. Also, services on existing modified NPCs and conflicting NPCs are not discovered.

Using ISC Discovery with Cisco IP Solution Center MPLS Diagnostics Expert

If you are running the Discovery process to discover an MPLS VPN network for use with Cisco MPLS Diagnostics Expert, note the following points.

- You can use either CDP Discovery, Device/Topology, or Import Configuration Files-based Discovery. The recommendation is to use either Device/Topology or Import Configuration Files-based Discovery.
- For Cisco IP Solution Center MPLS Diagnostics Expert, you only need to perform the Device Discovery, Discovery Data Collection, and Role Assignment Steps. You do not need to perform the NPC Discovery step or the Service Discovery step. However, you can let the NPC Discovery process run.

See [Figure 4-5 on page 4-13](#) for a flowchart of the required steps for ISC Discovery with Cisco IP Solution Center MPLS Diagnostics Expert.
- If you are using Cisco IP Solution Center MPLS Diagnostics Expert, then you normally only need to discover P and PE devices. Therefore, when you perform the Role Assignment step for discovered devices, you only need to assign roles to the P and PE devices.



Note If you do discover any CE devices, you must assign them CE roles.

- After completion of the automated Discovery process, you must schedule and run a **Task Manager > Collect Config** task for all discovered devices.

Using ISC Discovery With Cisco IP Solution Center Traffic Engineering Management

Normally you do not have to run the ISC Discovery process if you are using Cisco IP Solution Center Traffic Engineering Management. Cisco IP Solution Center Traffic Engineering Management has its own discovery process. This process is documented in Chapter 2 of the *Cisco IP Solution Center Traffic Engineering Management User Guide, 5.0*, “TE Network Discovery.”

However, if you are running *both* Cisco IP Solution Center Traffic Engineering Management (TEM) and Cisco IP solution Center MPLS VPN Management, you must run the Discovery process for Cisco IP Solution Center MPLS VPN Management.

Note the following points:

- One region (default region) is used for TEM.
- If you are also running ISC Discovery for MPLS VPN Management, make sure you run the Discovery workflow described in this chapter *first*, and then run the Cisco IP Solution Center Traffic Engineering Management process later.

Summary of Tasks for Discovery (Cisco ISC MPLS VPN Management and L2VPN Management)

[Figure 4-3](#) provides a general workflow diagram for the Discovery process used with the Cisco IP Solution Center MPLS VPN Management or Cisco IP Solution Center L2VPN Management application.



Note [Figure 4-5 on page 4-13](#) provides a general workflow diagram for the Discovery process as used with the MPLS Diagnostics Expert application.

Figure 4-3 *Basic Workflow for Discovery with Cisco ISC MPLS VPN Management or Cisco ISC L2VPN Management*

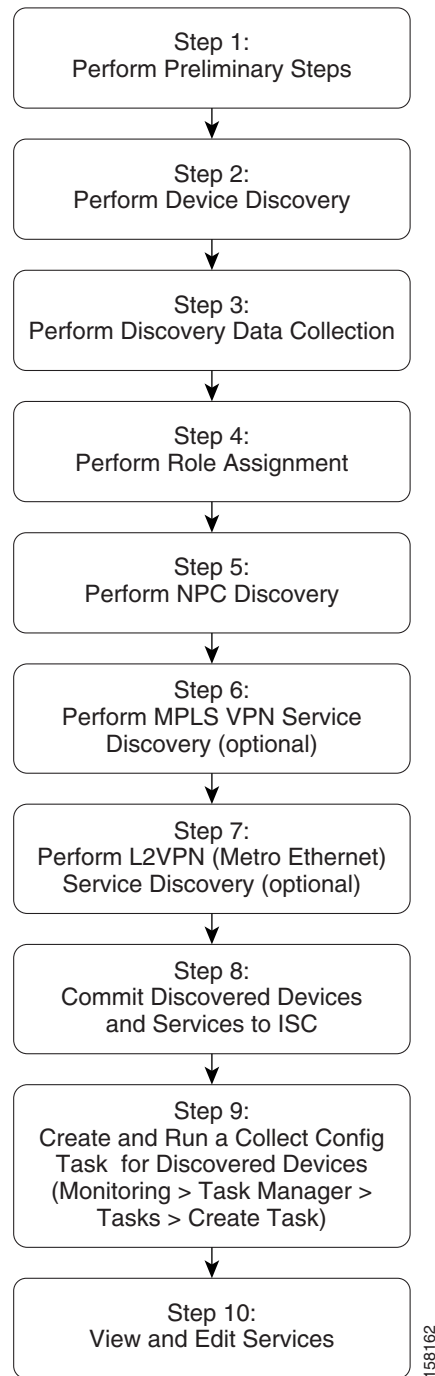


Table 4-2 describes each task in the Discovery workflow for Cisco ISC MPLS VPN Management and Cisco ISC L2VPN Management.

Table 4-2 Description of Discovery Steps for MPLS VPN and L2VPN Management

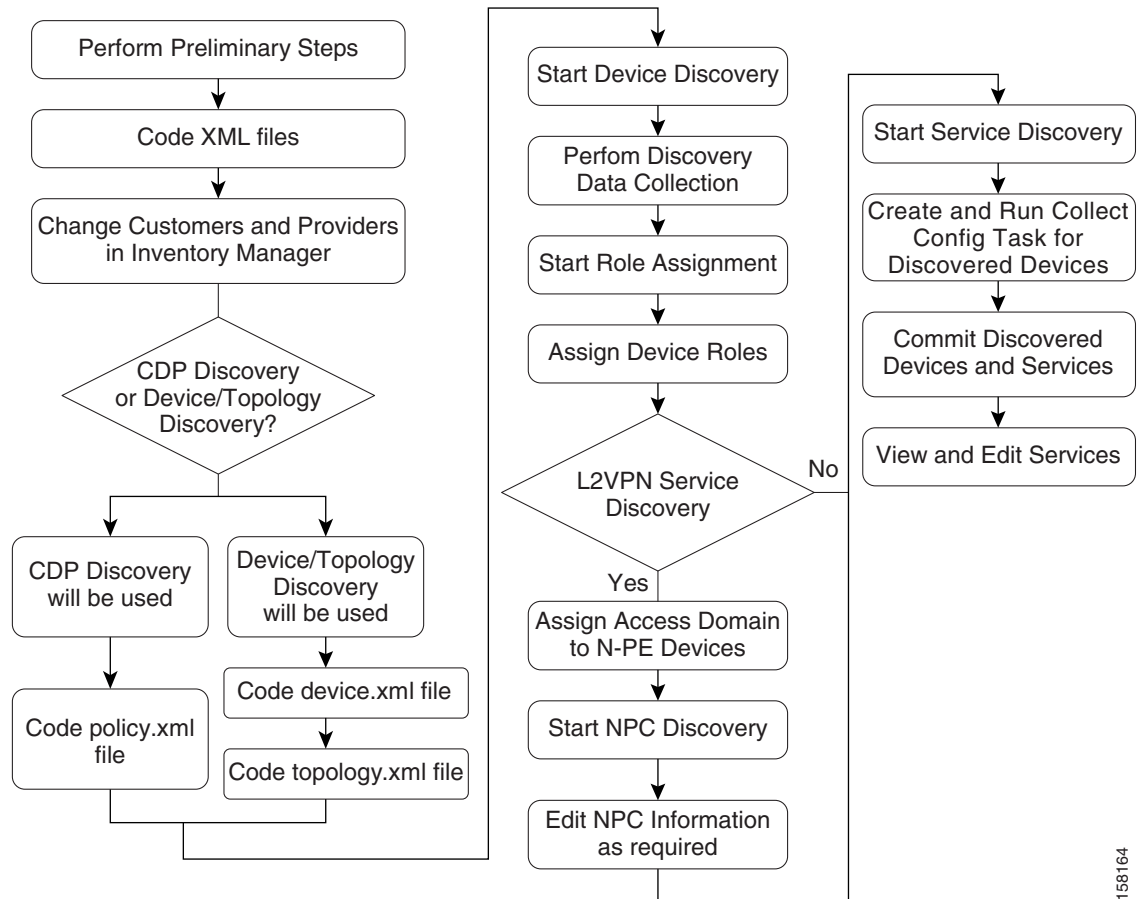
Step	Description
Step 1: Perform Preliminary Steps	Perform preliminary steps that are required for ISC Discovery. See Step 1: Perform Preliminary Steps, page 4-15. - Review System Requirements See Review System Requirements, page 4-16. - Install Licenses See Install Licenses, page 4-17. (CDP Discovery Only) Verify That a Unique TIBCO Port Is Defined See (CDP Discovery Only) Verify That a Unique TIBCO Port Is Defined, page 4-17 (CDP Discovery Only) Verify That CDP Is Running on Devices To Be Discovered See (CDP Discovery Only) Verify That CDP Is Running on Devices To Be Discovered, page 4-18. - Code XML Files Required for Discovery See Code XML Files Required for Discovery, page 4-19.
Step 2: Perform Device Discovery	- Start Device Discovery See Starting Device Discovery, page 4-26. - After Device Discovery is complete, enter device passwords For information on entering device passwords, see Setting Password Attributes (Required Step), page 4-33. - Enter additional device information as required See Setting General Device Attributes, page 4-35 and Setting Cisco CNS Attributes, page 4-36.
Step 3: Perform Discovery Data Collection	Start configuration collection. No input is required for this step. See Step 3: Perform Discovery Data Collection, page 4-37 .
Step 4: Perform Role Assignment	Assign device roles to each device. See Step 4: Perform Role Assignment, page 4-37 .
Step 5: Perform NPC Discovery	If you are discovering a Metro Ethernet Network with an Ethernet Core, perform the required preliminary steps. See Preliminary Steps Before Completing NPC Discovery for Metro Ethernet Networks, page 4-50 - Start NPC Discovery See Step 5: Perform NPC Discovery, page 4-50. - Modify and/or add NPCs as required. See Adding a Device for an NPC, page 4-54, Adding a Ring, page 4-55, Inserting a Device, page 4-56, Inserting a Ring, page 4-56, or Deleting a Device or a Ring, page 4-56.

Table 4-2 Description of Discovery Steps for MPLS VPN and L2VPN Management (continued)

Step	Description
Step 6: Perform MPLS VPN Service Discovery (optional)	Start MPLS VPN Service Discovery. See Step 6: Perform MPLS VPN Service Discovery (Optional), page 4-57. This step is required for the Cisco IP Solution Center MPLS VPN Management application, Note This step is not required for the Cisco IP Solution Center L2VPN Management application or the Cisco IP Solution Center MPLS Diagnostics Expert application.
Step 7: Perform L2VPN Service Discovery (optional)	Start L2VPN Service Discovery. See Step 7: Perform L2VPN (Metro Ethernet) Service Discovery (Optional), page 4-66. This step is required for the Cisco IP Solution Center L2VPN Management application. Note This step is not required for the Cisco IP Solution Center MPLS VPN Management application or the Cisco IP Solution Center MPLS Diagnostics Expert application.
Step 8: Commit Discovered Devices and Services to ISC Repository	Commit the discovered devices and services to the ISC repository. Prior to this step, discovery workflow stores the discovered devices and services in a temporary repository, which gets committed to ISC only at the last step of discovery workflow.
Step 9: Create and Run a Collect Config Task for Discovered Devices	From the ISC Start Page, choose Monitoring > Task Manager. Select the Collect Config task and select all of the devices discovered in the Device Discovery step; then submit the task. See Step 9: Create and Run a Collect Config Task for the Discovered Devices, page 4-79.
Step 10: View and Edit Services	The discovered services will be in Pending state and you need to do a config audit to move them to Deployed state. See Step 10: View and Edit Services, page 4-79.

Within each step, additional tasks must be performed and choices must be made. [Figure 4-4](#) shows a detailed flowchart that illustrates all of the steps in the Discovery workflow.

Figure 4-4 Detailed Diagram of Discovery Steps (Cisco ISC MPLS VPN Management and Cisco ISC L2VPN Management)



158164

Summary of ISC Discovery Steps for MPLS Diagnostics Expert

Figure 4-5 shows the basic Discovery steps for Cisco ISC with the MPLS Diagnostics Expert (MDE) application. For MDE, several of the steps required for Cisco ISC MPLS VPN Management and Cisco ISC L2VPN Management are not required.

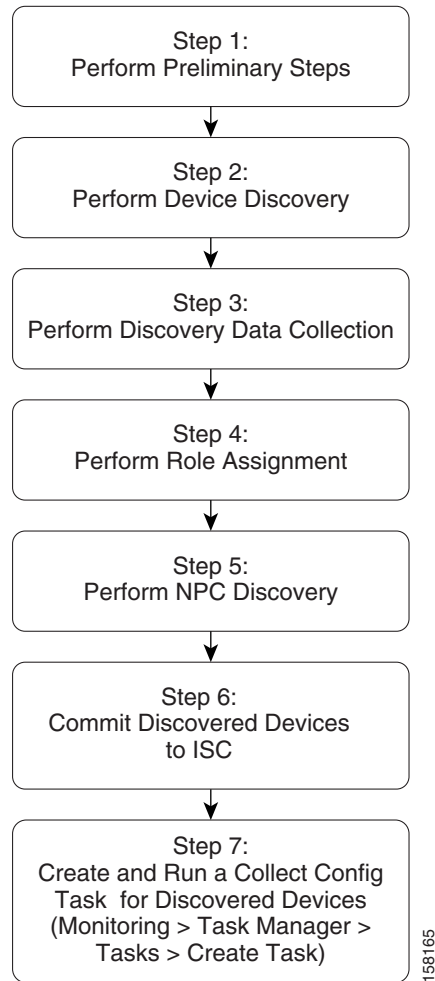
Figure 4-5 *Discovery Workflow for the MPLS Diagnostics Expert Application*

Table 4-3 *Description of Discovery Steps for MPLS Diagnostics Expert*

Step	Description
Step 1: Perform Preliminary Steps	Perform preliminary steps that are required for ISC Discovery. - Review System Requirements See Review System Requirements, page 4-16. - Install Licenses See Install Licenses, page 4-17 - Code XML Files Required for Discovery For specific instructions, see the following section: Code XML Files Required for Discovery, page 4-19.
Step 2: Perform Device Discovery	- Start Device Discovery See Starting Device Discovery, page 4-26. - After Device Discovery is complete, enter device passwords For information on entering device passwords, see Setting Password Attributes (Required Step), page 4-33. - Enter additional device information as required See Setting General Device Attributes, page 4-35 and Setting Cisco CNS Attributes, page 4-36.
Step 3: Perform Discovery Data Collection	Start configuration collection. No input is required for this step. See Step 3: Perform Discovery Data Collection, page 4-37.

Table 4-3 Description of Discovery Steps for MPLS Diagnostics Expert (continued)

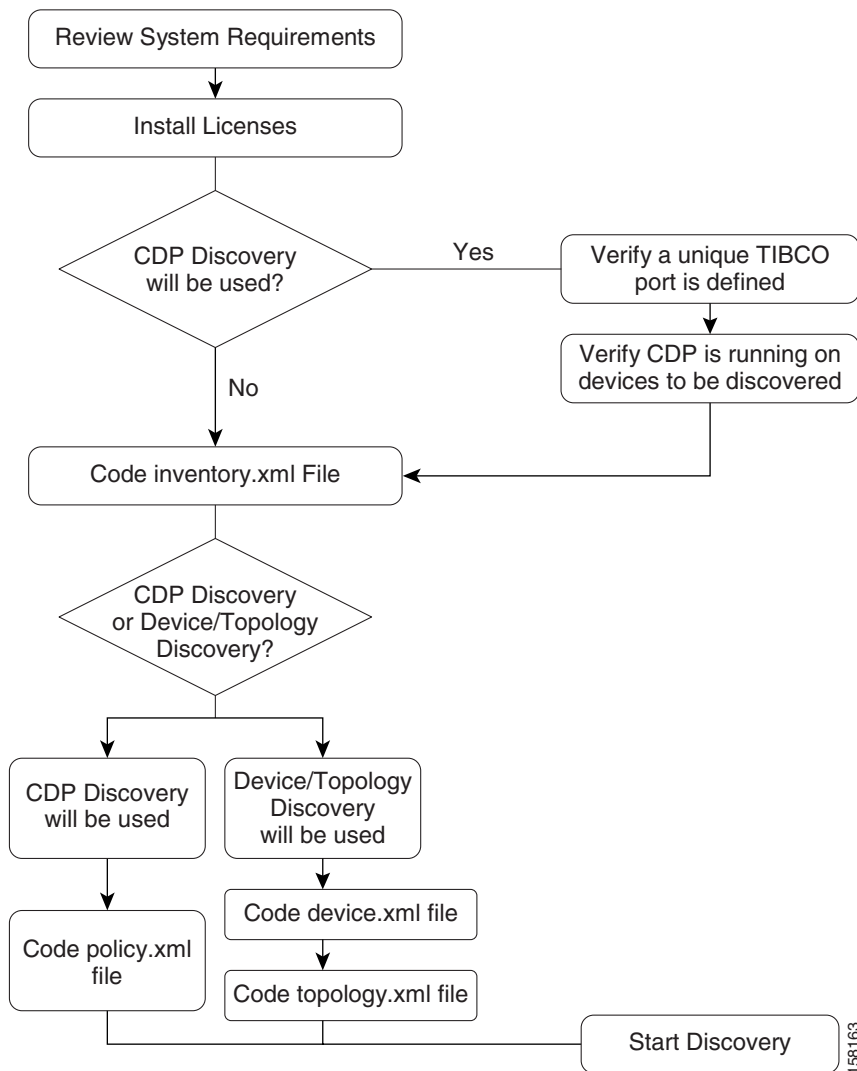
Step	Description
Step 4: Perform Role Assignment	Assign device roles to each device. See Step 4: Perform Role Assignment, page 4-37. For MDE, you normally discover only P and PEs and assign P and PE roles to them. However, if you discover CEs, assign CE roles to the CE devices. Note Although you do not have to edit NPCs for MPLS Diagnostics Expert, after you perform role assignment this step should complete.
Step 5: Create and Run a Collect Config Task for Discovered Devices	From the ISC Start Page, choose Monitoring > Task Manager. Select the Collect Config task and select all of the devices discovered in the Device Discovery step; then submit the task. See Step 8: Commit Discovered Devices and Services to ISC Repository, page 4-78.

Step 1: Perform Preliminary Steps

Before you initiate the ISC Discovery process, complete the following preliminary steps:

- Review System Requirements
- Install Licenses
- Discovery in Large Networks
- (CDP Discovery Only) Verify That a Unique TIBCO Port Is Defined
- (CDP Discovery Only) Verify That CDP is Running on Devices To Be Discovered
- Code XML Files Required for Discovery

[Figure 4-6](#) summarizes the preliminary steps for ISC Discovery.

Figure 4-6 Summary of Preliminary Steps for Discovery

158163

Review System Requirements

Cisco recommends that you thoroughly review the system requirements for ISC before planning your installation, to be sure that you have all the hardware and software that you must successfully install.

The system recommendations and requirements for ISC are listed in Chapter 1, “System Recommendations” of the [Cisco IP Solution Center Installation Guide, 5.0](#) and in the [Release Notes for Cisco IP Solution Center, 5.0.1](#).

Install Licenses

Before starting Discovery, the appropriate licenses (both Activation and VPN licenses) must be installed. Also, each license must be large enough to handle all possible discovered objects. For information on installing licenses, see the “Installing License Keys” section of Chapter 2 of the *Cisco IP Solution Center Installation Guide, 5.0*, “Installing and Logging In to ISC.”

Discovery in Large Networks

To discover large networks with a complex topology, we recommend you reset two DCPL properties, as follows:

-
- Step 1** See [Appendix C, “Property Settings”](#) for an explanation of how to navigate to the Dynamic Component Properties Library (DCPL) properties.
 - Step 2** Navigate to the property `watchdog\server\discovery\heartbeat\timeout` and set this property to **180000 milliseconds** (3 minutes).
 - Step 3** Navigate to the property `watchdog\server\discovery\java\flags` and set this property to **-Xmx3072m -XX:PermSize=256m -XX:MaxPermSize=512m**
 - Step 4** Restart the ISC server.
-

Heap is a block of memory segment for the L2VPN and Metro Ethernet, Layer 3 MPLS VPN, and TEM components. It is allocated for use by the Java virtual machine (JVM) process during runtime. It might need to be increased for large deployments. If the **httpd** process restarts, increase the heap size, as follows:

-
- Step 1** `cd $ISC_HOME/bin`
 - Step 2** `vi tomcat.sh`
 - Step 3** Search for a line with **-Xmx512m**
 - Step 4** Set the heap size to 1GB or 2GB by replacing **-Xmx512m** with **-Xmx1024m** or **-Xmx2048m**, respectively.
 - Step 5** Save the `tomcat.sh` file.
 - Step 6** Enter **stopall** to stop the ISC server.
 - Step 7** Enter **startwd** to start the ISC server.
-

(CDP Discovery Only) Verify That a Unique TIBCO Port Is Defined

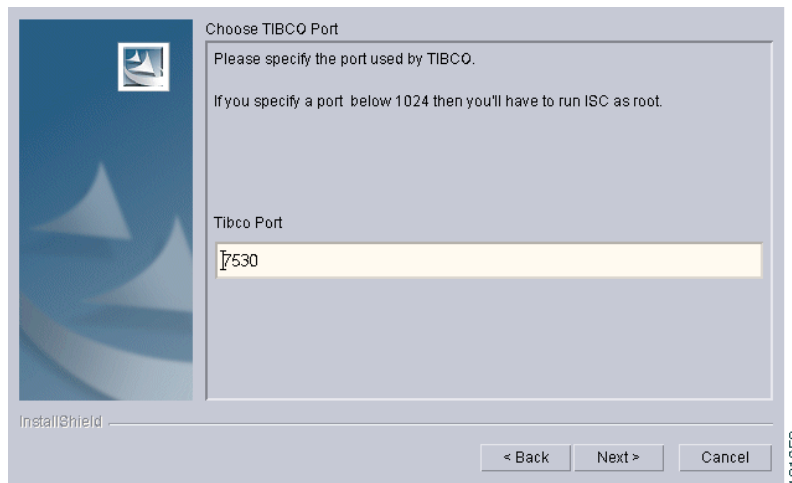
If you are using CDP Discovery to discover the network topology, make sure the TIBCO Port is unique. Otherwise, CDP discovery will fail.

During installation, the TIBCO port can be specified if the “custom” Installation Type is selected at the start of the installation process. Otherwise, the default port installed is 7530. You specify the TIBCO port on the Choose TIBCO Port dialog.

The port number that is specified must be unique throughout the network, and no other ISC installations are allowed with the same port.

Figure 4-7 shows the Choose TIBCO Port dialog.

Figure 4-7 Choose TIBCO Port



The Tibco port can be changed after installation by modifying `vpnsc.properties`.

(CDP Discovery Only) Verify That CDP Is Running on Devices To Be Discovered

If CDP Discovery is going to be used, use the **show cdp** command to ensure that CDP is running on all of the devices intended to be discovered.

For each device, enter the **show cdp** command, as shown in Example 4-1.

Example 4-1 The show cdp Command:

```
Router# show cdp
Global CDP information:
  Sending CDP packets every 120 seconds
  Sending a holdtime value of 180 seconds
  Sending CDPv2 advertisements is enabled
Router#
```



Note

When performing CDP Discovery for devices with more than one IP address configured, it is possible that CDP discovery will find an IP address other than the management IP address. If the IP address found is not accessible from the ISC server, then it will not be possible to discover that device using CDP discovery.

Code XML Files Required for Discovery

Before you can run ISC Discovery, you must code XML files that are required for the Discovery process. A different set of files is required, depending on whether you use CDP Discovery or Device/Topology-based Discovery.

Table 4-4 describes the XML files and indicates which files are required for each type of discovery method.

Table 4-4 XML Files Used with ISC Discovery

XML File	Description	Required for CDP Discovery	Required for Device/Topology Based Discovery
policy.xml	Specifies one or more seed IP addresses that can be reached from the specified seed device and a maximum hop count for the device discovery process.	Yes	No
device.xml	Specifies information used to locate devices, such as device IP addresses and Object IDs (OIDs).	No	Yes
topology.xml	Specifies information used to build NPCs used by MPLS VPN and/or Metro Ethernet topology.	No	Yes



Note

Make sure that the coding in your XML files is accurate. If there are errors in the files, you might need to re-run the Discovery process.

Sample XML Files

The initial installation of ISC provides sample XML files that you can use as a starting point in coding your own XML files. The sample XML files are located in the following directory:

```
<install_directory>/resources/discovery/sample
```

where *install_directory* is the installation directory that you specified when prompted by the ISC installation program.

Coding the policy.xml File

The **policy.xml** file:

- Is required for CDP Discovery.
- Is required for Cisco IP Solution Center MPLS VPN Management, Cisco IP Solution Center Metro Ethernet and L2VPN Management, and Cisco MPLS Diagnostics Expert.
- Is not required for Device/Topology-based Discovery.
- Is not required for Cisco IP Solution Center Traffic Engineering Management.
- Provides a seed IP address that the CDP protocol uses to discover devices near the seed device.

Example 4-2 shows the sample **policy.xml** file that is provided with the ISC installation.

Example 4-2 Sample policy.xml File

```
<?xml version='1.0' encoding='UTF-8'?>
<DISCOVERY_POLICY overwrite_existing_policy="true">
  <DISCOVERY_METHOD>
    <CDP ipaddress="209.168.133.232" hop="1"/>
  </DISCOVERY_METHOD>
  <SNMP_COMMUNITY>
    <RO_COMMUNITY>
      <COMMUNITY community="public"/>
    </RO_COMMUNITY>
    <RW_COMMUNITY>
      <COMMUNITY community="private"/>
    </RW_COMMUNITY>
  </SNMP_COMMUNITY>
</DISCOVERY_POLICY>
```

If there are additional routers that are on the other side of PE routers on the edge of the core segment of the network, you can specify more than one seed IP address in order to discover these devices.

[Example 4-3](#) shows a **policy.xml** file that contains two seed IP addresses.

Example 4-3 Policy.xml File with Two IP Addresses

```
<?xml version='1.0' encoding='UTF-8'?>
<DISCOVERY_POLICY overwrite_existing_policy="true">
  <DISCOVERY_METHOD>
    <CDP ipaddress="209.168.133.241" hop="8"/>
  </DISCOVERY_METHOD>
  <DISCOVERY_METHOD>
    <CDP ipaddress="209.168.133.244" hop="8"/>
  </DISCOVERY_METHOD>
  <SNMP_COMMUNITY>
    <RO_COMMUNITY>
      <COMMUNITY community="public"/>
    </RO_COMMUNITY>
    <RW_COMMUNITY>
      <COMMUNITY community="private"/>
    </RW_COMMUNITY>
  </SNMP_COMMUNITY>
</DISCOVERY_POLICY>
```

[Table 4-5](#) describes the XML tags used in the **policy.xml** file.

Table 4-5 XML Tags and Attributes Used in the policy.xml File

Tag	Description
<DISCOVERY_METHOD>	Starts a <DISCOVERY_METHOD> tag. The <DISCOVERY_METHOD> tag must contain a <CDP> tag.
<CDP>	Starts a <CDP> tag. The <CDP> tag specifies a seed IP address and a hop count. The <CDP> tag must contain the following attributes: • ipaddress • hop

Table 4-5 XML Tags and Attributes Used in the *policy.xml* File (continued)

Tag	Description
ipaddress	Specifies the IP address of a seed device. Required attribute for the <CDP> tag.
hop	Specifies the number of hops from the device identified by the ipaddress attribute to go in discovering devices. Required attribute for the <CDP> tag.

Follow these steps to edit the sample **policy.xml** file:

- Step 1** Edit the sample file and replace the IP address specified with the **ipaddress** XML attribute with an appropriate IP address from your network.

This IP address 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.



Note You can provide more than one IP address. This is useful in situations where one network domain is on the other side of a PE router on the edge of the core segment of the network.

- Step 2** Edit the hop count specified with the **hop** attribute and specify a hop count that will be used when the Discovery process is initialized.

When you choose the seed devices and hop count, 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 hop count 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 3** If you need to add additional IP addresses for seed devices, code additional **<DISCOVERY_METHOD>** tags.

Within the additional **<DISCOVERY_METHOD>** tags, include **<CDP>** tags.

For each **<CDP>** tag, specify an IP address with the **ipaddress** attribute and a hop count with the **hops** attributes.

- Step 4** Save the **policy.xml** file to an appropriate directory on the ISC host.

When you run the Discovery process, the process queries the starting point device for its CDP table. From this table, all of those devices are queried for their CDP information. This process continues until the maximum hop count from the starting point is reached. When you use the CDP-based method, note that only devices running CDP are discovered.

Coding the device.xml File

The **device.xml** file:

- Is required for Device/Topology-based Discovery.
- Is not required for CDP-based Discovery.
- Is required for Cisco IP Solution Center MPLS VPN Management, Cisco IP Solution Center L2VPN Management, and ISC MPLS Diagnostics Expert.
- Is not required for Cisco IP Solution Center Traffic Engineering Management.
- Specifies information used to locate devices, such as device IP addresses and Object IDs (OIDs).

[Example 4-4](#) shows a sample **device.xml** file. Use the sample file as an example and save your edited file in an appropriate directory.

Example 4-4 Sample device.xml file

```
<network>
<device>
<device-name>mlpe8</device-name>
<ip-address>209.168.133.244</ip-address>
<system-object-id>.1.3.6.1.4.1.9.1.509</system-object-id>
<snmp-info>
<ro-community>public</ro-community>
</snmp-info>
</device>

<device>
<device-name>mlsw11</device-name>
<ip-address>209.168.133.170</ip-address>
<system-object-id>.1.3.6.1.4.1.9.1.574</system-object-id>
<snmp-info>
<ro-community>public</ro-community>
</snmp-info>
</device>

<device>
<device-name>mlsw16</device-name>
<ip-address>209.168.133.175</ip-address>
<system-object-id>.1.3.6.1.4.1.9.1.574</system-object-id>
<snmp-info>
<ro-community>public</ro-community>
</snmp-info>
</device>

<device>
<device-name>mlsw17</device-name>
<ip-address>209.168.133.176</ip-address>
<system-object-id>.1.3.6.1.4.1.9.1.574</system-object-id>
<snmp-info>
<ro-community>public</ro-community>
</snmp-info>
</device>

</network>
```

[Table 4-6](#) describes the XML tags used in the **device.xml** file.

Table 4-6 XML Tags Used in the device.xml File

Tag	Description
<device>	Starts a <device> tag. The <device> tag must contain the following tags: • <device-name> • <ip-address> The following tags are optional within the <device> tag: • <system-object-id> • <snmp-info>
<device-name>	Specifies the name of the device. Required within the <device> tag.
<ip-address>	Specifies the IP address of the device. Required within the <device> tag.
<system-object-id>	(optional) Can be included to specify the SNMP Object ID (OID) for the device. If this is provided, it is specified within the <device> tag.
<snmp-info>	Specifies SNMP information for the device. The <snmp-info> tag must contain a <ro-community> tag. Optional within the <device> tag.
<ro-community>	Specifies the level of SNMP access for the device. Normally, this should be “public.” Required within the <snmp-info> tag.

Follow these steps to code the **device.xml** file:

-
- Step 1** Edit the sample **device.xml** file provided with the installation.
- Step 2** For each device that is to be discovered by ISC, code a <device> entry. Each <device> entry should contain the following tags:
- A <device-name> tag specifying the device name.
 - An <ip-address> tag specifying the IP address for the device.
 - A <system-object-id> tag specifying the OID for the device (optional).
 - An <snmp-info> tag specifying <ro-community> information
- Step 3** Save the **device.xml** file to an appropriate directory on the ISC host.
-

Coding the topology.xml File

The **topology.xml** file:

- Is required for Device/Topology-based Discovery.

- Is not required for CDP-based Discovery.
- Is required to perform ISC Discovery for Cisco IP Solution Center MPLS VPN Management, Cisco IP Solution Center L2VPN Management, and Cisco IP Solution Center MPLS Diagnostics Expert.
- Is not required for Cisco IP Solution Center Traffic Engineering Management.
- Specifies information used to locate devices, such as device IP addresses and Object IDs (OIDs).

The **topology.xml** file specifies the discovery protocol that is used in the discovery process, and, for each connection, specifies the starting IP address, the starting interface, the end device, and the end interface

[Example 4-5](#) shows a sample **topology.xml** file. Use the sample file as an example and save your edited file in an appropriate directory.

Example 4-5 Sample topology.xml File

```
<topology>
<connection discovery-protocol="CDP" fromDevice="mlsw19" fromIP="209.168.133.178"
fromInterface="GigabitEthernet1/1/2" toDevice="mlsw21" toIP="209.168.133.220"
toIF="GigabitEthernet1/1/1" >
</connection>

<connection discovery-protocol="CDP" fromDevice="mlsw19" fromIP="209.168.133.178"
fromInterface="FastEthernet1/0/23" toDevice="mlsw21" toIP="209.168.133.220"
toIF="FastEthernet1/0/24" >
</connection>

<connection discovery-protocol="CDP" fromDevice="mlsw19" fromIP="209.168.133.178"
fromInterface="FastEthernet
1/0/24" toDevice="mlsw18" toIP="209.168.133.177" toIF="FastEthernet1/0/23" >
</connection>

<connection discovery-protocol="CDP" fromDevice="mlsw19" fromIP="209.168.133.178"
fromInterface="FastEthernet1/0/22" toDevice="mlsw22" toIP="209.168.133.221"
toIF="FastEthernet1/0/24" >
</connection>

</topology>
```

[Table 4-7](#) describes the XML tags used in the **topology.xml** file.

Table 4-7 XML tags and Attributes Used in the topology.xml File

Tag	Description
<connection>	Starts a <connection> tag. The <connection> tag must specify the following attributes: • discovery-protocol • fromDevice • FromIP • FromInterface • toDevice • toIP • toIF
discovery-protocol	Specifies the Discovery protocol used to discover the network topology. Normally, this is "CDP."

Table 4-7 XML tags and Attributes Used in the topology.xml File (continued)

Tag	Description
fromDevice	Specifies the name of the device from which the Named Physical Circuit starts. Required attribute for the <connection> tag.
FromIP	Specifies the management IP address of the device from which the Named Physical Circuit starts. Required attribute for the <connection> tag.
FromInterface	Specifies the name of the device interface from which the Named Physical Circuit starts. Required attribute for the <connection> tag.
toDevice	Specifies the name of the device to which the Named Physical Circuit connects. Required attribute for the <connection> tag.
toIP	Specifies the management IP address of the device from which the Named Physical Circuit connects. Required attribute for the <connection> tag.
toIF	Specifies the device interface on the device to which the Named Physical Circuit connects. Required attribute for the <connection> tag.

Follow these steps to code the **topology.xml** file:

-
- Step 1** Edit the sample **topology.xml** file provided with the installation.
- Step 2** For each NPC connection that is to be discovered by ISC, code a **<connection>** entry. Each **<connection>** entry must contain the following tags:
- A **discovery-protocol** attribute specifying the CDP protocol.
 - A **fromDevice** attribute specifying the device from which the NPC starts.
 - A **FromIP** attribute specifying the management IP address from which the NPC starts.
 - A **FromInterface** attribute specifying the device interface from which the NPC starts.
 - A **toDevice** attribute specifying the name of the device to which the NPC connects.
 - A **toIP** attribute specifying the management IP address of the device to which the NPC connects.
 - A **toIF** attribute specifying the name of the interface on the device to which the NPC connects.
- Step 3** Save the **topology.xml** file to an appropriate directory on the ISC host.
-

Step 2: Perform Device Discovery

This section describes how to start the device discovery process and edit device configuration.

Starting Device Discovery

To start discovery, follow these steps:

- Step 1** Log in to ISC.
- Step 2** Click the **Service Inventory** tab.
- Step 3** The Service Inventory window appears, as shown in [Figure 4-8](#).

Figure 4-8 Service Inventory Window



- Step 4** Click **Discovery**.

The Discovery window appears, as shown in [Figure 4-9](#).

Initially, the CDP Discovery method is selected and the window displays the required input for this method.

Figure 4-9 Device Discovery—CDP Fields

The screenshot shows the 'Discovery' window in the Cisco IP Solution Center. On the left is a 'Selection' pane with 'Current Request' and 'Previous Requests'. The main area is titled 'Discovery' and contains three sections: 'Identification' with a 'Name' field; 'Device Discovery' with a selected 'CDP' radio button, and three text fields for 'Policy File', 'Output Device File', and 'Output Connection File'; and 'Service Discovery' with checked checkboxes for 'MPLS VPN' and 'L2VPN (Metro Ethernet) Discovery'. A 'Start' button is located at the bottom right. A note at the bottom left states 'Note: * - Required Field'.

The editable **Output Device File** field is optional and defaults to an XML file of the discovered devices. This file can then be an input **Devices File** for rerunning discovery using the **Device/Topology** option, by choosing that radio button.

The editable **Output Connection File** is optional and defaults to an XML file that contains device connectivity information that is written during CDP Device Discovery. This file can then be an input **NPC Topology File** for rerunning discovery using the Device/Topology option, by choosing that radio button.

Step 5 Choose a Discovery method:

- To use the Cisco Discovery Protocol (CDP) method, click the **CDP** radio button, with the resulting window as shown in [Figure 4-9, “Device Discovery—CDP Fields.”](#)
- To use the Device/Topology method, click the **Device/Topology** button, with the resulting window as shown in [Figure 4-10, “Device Discovery—Device/Topology Fields.”](#)
- To use the Import Configuration Files method, click the **Import Configuration Files** button, with the resulting window as shown in [Figure 4-11, “Device Discovery—Import Configuration File Fields.”](#)

Figure 4-10 Device Discovery—Device/Topology Fields

The screenshot shows the 'Discovery' configuration page. On the left is a 'Selection' sidebar with 'Current Request' and 'Previous Requests'. The main area is divided into sections: 'Identification' with a 'Name' field; 'Device Discovery' with radio buttons for 'CDP', 'Device/Topology' (selected), and 'Import Configuration Files'; 'Devices File' with a text box containing '/opt/iscadm/411-196/resources/discovery/data/device.xml'; 'NPC Topology File' with an empty text box; and 'Service Discovery' with checkboxes for 'MPLS VPN' and 'L2VPN (Metro Ethernet) Discovery' (both checked). A 'Start' button is at the bottom right. A note at the bottom left states 'Note: * - Required Field'.

Figure 4-11 Device Discovery—Import Configuration File Fields

This screenshot is similar to Figure 4-10 but shows the 'Import Configuration Files' radio button selected in the 'Device Discovery' section. The 'Devices File' field is replaced by a 'Directory' field with an information icon, and the 'NPC Topology File' field remains. The 'Start' button and the 'Note: * - Required Field' are also present.

The required **Directory** field is the directory on the server that contains configuration files for the devices to be discovered. The format of these files *must* be `<filename>.cfg`.

The **NPC Topology File** field contains an XML file that contains device connectivity information that is used to automatically create NPCs.

**Note**

During service discovery, Providers, Regions, Customers, and Sites are not automatically created, and therefore you must manually create them before running service discovery. If Resource Pools are used for provisioning in ISC, Access Domains and Resource Pools must be manually created before running service discovery.

Step 6 In the Discovery window, specify the settings indicated in [Table 4-8](#).

Table 4-8 **Discovery Settings**

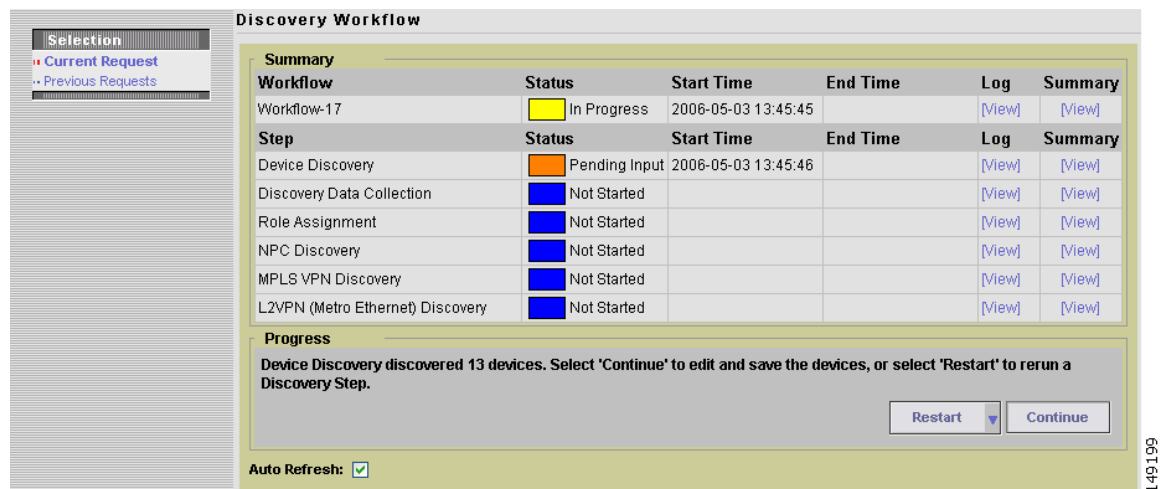
Setting	Description
Name	In this field, enter a unique name of your choice for the Workflow name. If you do not enter a name in this field, the system automatically generates a unique name for you.
CDP	Click this radio button to select Cisco Discovery Protocol (CDP) as the Discovery method.
Policy File	If you click the CDP button, specify the path to your policy.xml file here. This file is an XML file that indicates the IP address of one or more devices used as a starting point for the discovery process. For more information on the policy.xml file, see Coding the policy.xml File, page 4-19.
Output Device File	This editable optional field defaults to an XML file of the discovered devices. This file can then be an input Devices File for rerunning discovery using the Device/Topology option.
Output Connection File	This editable optional field defaults to an XML file that contains device connectivity information that is written during CDP device discovery. This file can then be an input NPC Topology File for rerunning discovery using the Device/Topology option.
Device/Topology	Click this radio button to select Device/Topology as the Discovery method.
Devices File	If you click the Device/Topology button, specify the path to your device.xml file here. This file contains information used to locate the devices in your network, such as IP addresses and OIDs. For more information on the device.xml file, see Coding the device.xml File, page 4-22.
NPC Topology File	If you click this optional Device/Topology button, specify the path to your topology.xml file here. This file contains information used to determine the NPC topology of your network. For more information on the topology.xml file, see Coding the topology.xml File, page 4-23.

Table 4-8 **Discovery Settings (continued)**

Setting	Description
Import Configuration Files	Click this radio button to select Import Configuration Files as the Discovery method.
Directory	This required field is the directory on the server that contains configuration files for the devices to be discovered. The format of these files <i>must</i> be <filename>.cfg.
NPC Topology File	This field contains an XML file that contains device connectivity information that is used to automatically create NPCs.
MPLS VPN	To discover devices used in an MPLS VPN service, click the MPLS VPN radio button.
L2VPN (Metro Ethernet) Discovery	To discover layer 2 devices used in a Metro Ethernet service, click the L2VPN (Metro Ethernet) Discovery radio button.

Step 7 Click the **Start** button.

The discovery process starts and the Discovery Workflow window appears, as shown in [Figure 4-12](#).

Figure 4-12 **Discovery Workflow Window**

The **Workflow** category in the data pane gives the name information about the current discovery request/workflow.

Click the **Restart** button and you receive a drop-down list of completed steps. Select a step and you will restart from that step.

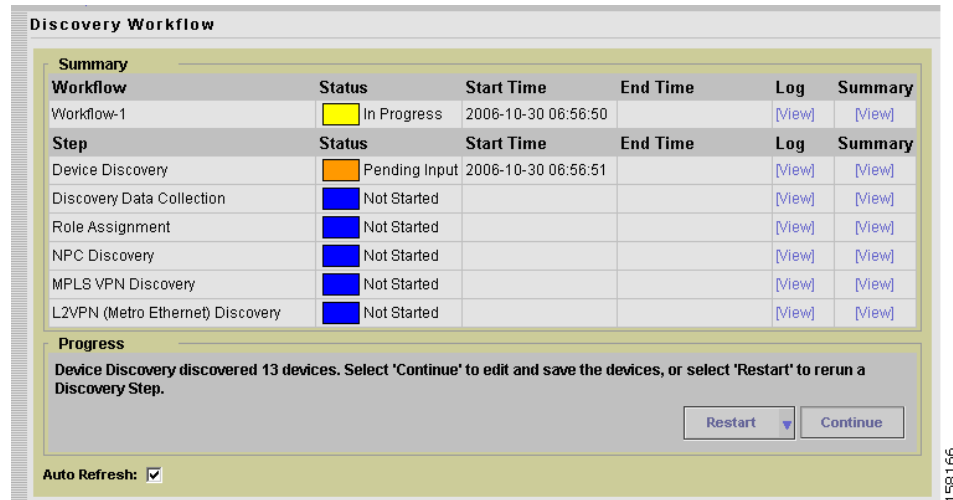
In the left column, **Current Request** gives the discovery request/workflow that is currently running. If there is no currently running discovery request/workflow, an initialization window appears to create a new discovery request/workflow.

In the left column, **Previous Requests** lists all the discovered requests/workflows. You can look at the status and logs for any of these discovery requests/workflows.

Discovery Workflow window indicates the progress of each phase of device discovery:

- When the window first appears, the status indicator is yellow and indicates that the device discovery process is **Initializing**.
- The status indicator then indicates that the process is **In Progress**.
- After the discovery processes has completed, the display indicates how many devices were discovered, and the status indicator changes to orange and indicates that there is **Pending Input**, as shown in [Figure 4-13](#).

Figure 4-13 Discovery Workflow Window with Device Input Pending



The Progress area at the bottom of the window indicates how many devices were discovered.

At the lower right of the window there is a **Restart** button. You can click this button to restart the entire discovery process. However, if you restart the Discovery process, any work that has been done previous to restarting Discovery is lost.



Note

After each phase of the Discovery process, make sure that you check the log file to ensure that there were no errors in the process. For specific instructions, see [Using the Discovery Log Files, page 4-6](#).

Editing Device Configurations

After the initial discovery of devices in your network, you must edit the information that ISC maintains about the devices. This allows the Discovery process to collect configuration information about the devices that are required to determine the network topology and generate service requests.

Editing device configuration includes these steps:

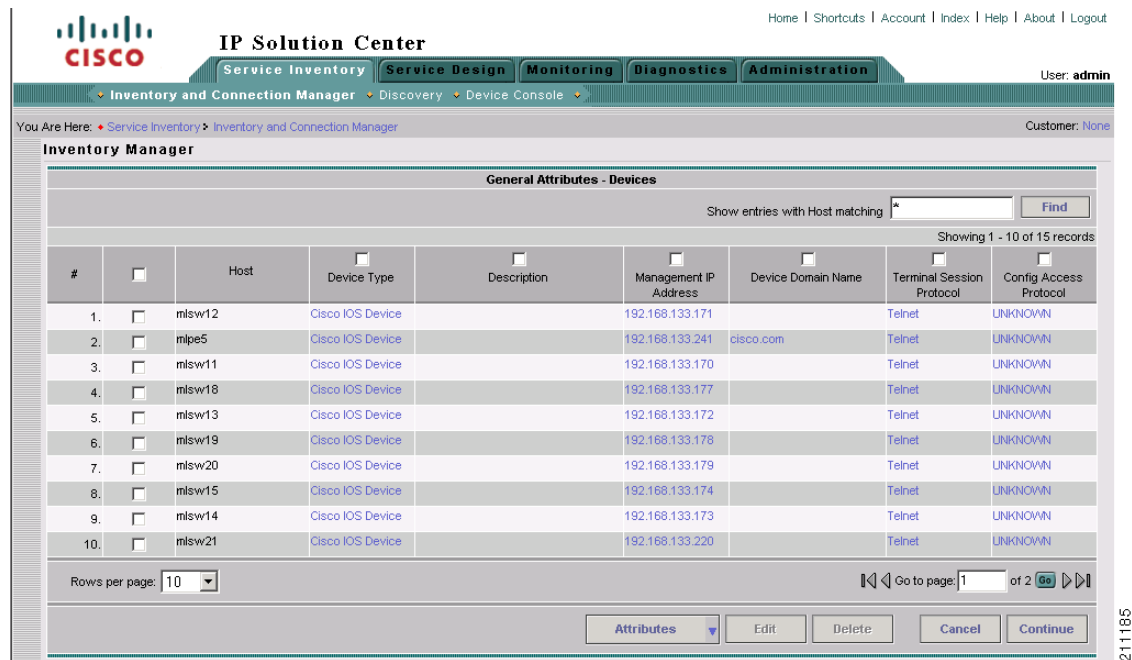
- Setting Password Attributes (a required step)
- Setting General Device Attributes
- Setting Cisco CNS Attributes

Step 2: Perform Device Discovery

Follow these steps to edit device configurations:

- Step 1** When the Discovery Workflow window indicates that the Device Discovery is **Pending Input**, click the **Continue** button.
- Step 2** The General Attributes - Devices window appears, as shown in [Figure 4-14](#).

Figure 4-14 The General Attributes-Devices Window



The General Attributes - Devices window allows you to do the following:

1. Delete devices.

If devices appear in the device list that you do not want to configure, you can delete them, as explained in [Step 5](#).

2. Set the following groups of attributes for each device:

- **General Attributes**—The general attributes include the hostname of the device, the device type, the management IP address, and other settings.

You can accept the default attributes shown in the General Attributes - Devices window or change them as required.

For a list of the general attributes, see [Setting General Device Attributes, page 4-35](#).

- **Password Attributes**—The password attributes include the username and password for the device and the enable username and password for the device. You *must* set these attributes.
- **CNS Attributes**—If the device is a CNS device, set the CNS attributes.

- Step 3** If you want to filter the devices that appear in the window, enter part of the device name for the devices that you want to view, preceded or followed by the asterisk (*) and then click the **Find** button.

If the Find field displays an asterisk, all devices are displayed.

The setting in the Find field applies to all of the attributes windows.

- Step 4** To change the display to show one of the attributes areas, click the **Attributes** button at the bottom of the window and use the pull-down list to select the attributes area to display.
- If you need to change the general attributes for the device, such as the protocol used to configure the device (Config Access Protocol), you can do this in the initial window that appears.
If the General Attributes - Devices window is not the current window, click the **Attributes** button and select **General Attributes** from the pull-down list.
See [Setting Password Attributes \(Required Step\)](#), page 4-33 for instructions on setting the General Attributes.
 - To set the password attributes, click the **Attributes** button and then select Password Attributes from the pull-down list.
For instructions on setting the password attributes, see [Setting Password Attributes \(Required Step\)](#), page 4-33.



Note This is a required step. To enable configuration collection, you *must* set the password attributes.

- If you need to change the CNS attributes, see [Setting Cisco CNS Attributes](#), page 4-36.
- Step 5** If you want to delete one or more devices, follow these steps:
- a. Check the check box next to each device that you want to delete.
If you need to delete more than one device, you can check the check box next to the heading for the list of the devices. This selects all of the devices in the list. You can then uncheck the boxes next to any devices that you do not want to delete.
 - b. To delete the devices, click the **Delete** button.

Setting Password Attributes (Required Step)

In order for the Configuration Collection phase to succeed, you *must* set the password attributes for each device. Follow these steps to set password attributes:

- Step 1** If the Password Attributes window is not the current window, click the **Attributes** button and select **Password Attributes** from the pull-down list.
- Step 2** The Password Attributes window appears, as shown in [Figure 4-15](#).

Figure 4-15 Password Attributes Window

The screenshot shows the Cisco IP Solution Center interface. The top navigation bar includes links for Home, Shortcuts, Account, Index, Help, About, and Logout. The main menu has tabs for Service Inventory, Service Design, Monitoring, Diagnostics, and Administration. The left sidebar shows the breadcrumb path: You Are Here: Service Inventory > Inventory and Connection Manager. The main content area is titled 'Password Attributes' and contains a sub-section 'Password Attributes - Devices'. This section includes a search bar with the text 'Show entries with Host matching' and a 'Find' button. Below the search bar, it says 'Showing 1 - 10 of 15 records'. A table follows with the following columns: #, Device Name, Login User, Login Password, Enable User, and Enable Password. The table lists 10 devices (mlsw12 to mlsw21). At the bottom of the table, there is a 'Rows per page' dropdown set to 10, a 'Go to page' field showing 1 of 2 pages, and buttons for 'Attributes', 'Edit', 'Delete', 'Cancel', and 'Continue'.

#	Device Name	Login User	Login Password	Enable User	Enable Password
1.	mlsw12				
2.	mlpe5				
3.	mlsw11				
4.	mlsw18				
5.	mlsw13				
6.	mlsw19				
7.	mlsw20				
8.	mlsw15				
9.	mlsw14				
10.	mlsw21				

Step 3 Follow these steps to select the devices and password attributes to configure:

- a. Check the check box next to a device that has password attributes you want to configure.

If several devices have the same password attributes, you can check multiple check boxes. If all of the devices have the same password attributes, you can check the box to the left of the heading row to select all of the devices in the list. If this check box is checked, you can uncheck it to deselect all of the devices.

- b. To select the password attributes to configure, check one or more of the check boxes next to the attribute names in the heading row.

Step 4 Click the **Edit** button.

The Edit Attributes window for passwords appears, as shown in [Figure 4-16](#).

Figure 4-16 *Edit Attributes Window for Password Attributes*

- Step 5** Enter the following information for the device:
- **Login Password**—Enter the login password for the device
 - **Login User**—Enter the username for the device
 - **Enable User**—Enter the name of a user with enable privileges
 - **Enable Password**— Enter the enable password for the enable user
- Step 6** Click **Save**.
- The information that you entered appears in the Password Attributes window.

Setting General Device Attributes

After you complete the device discovery process, the General Attributes - Devices window displays the current general attributes settings for each device.

Follow these steps to change the general attributes for a device:

- Step 1** Click on the attribute that you want to change.
- An Edit Attributes dialog box appears for the selected attribute.
- Step 2** In the dialog box, indicate the new setting for the attribute.
- The General Device attributes include the following:
- **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 is the Cisco Router.
 - **Device Description (not editable from this window)**—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.
- **Config Access Protocol**—Administers the access protocol for config upload and download. Choices include: Telnet, Terminal, TFTP, and RCP.

Setting Cisco CNS Attributes

If one of the devices is a Cisco CNS device, follow these steps to set CNS attributes:

- Step 1** If the CNS Attributes window is not the current window, click the **Attributes** button and select **CNS Attributes** from the pull-down list.
- Step 2** The CNS Attributes window appears, as shown in [Figure 4-17](#).

Figure 4-17 CNS Attributes Window

CNS Attributes						
CNS Attributes - Devices						
Show entries with Host matching *						Find
Showing 1 - 10 of 13 records						
#	Device Name	IE2100 Name	Event Identification	CNS Identification	Terminal Server	Port Number
1.	☐ mls12	None	CNS ID		None	0
2.	☐ mlpe5	None	Host Name		None	
3.	☐ mls18	None	Host Name		None	

The **Terminal Server** column specifies the devices that represent the workstations that can be used to provision edge routers, and the **Port Number** column specifies the port numbers used by the terminal server.

- Step 3** Click an existing Event Identification item.
- The Edit Attributes dialog box for Event Identification appears.

- Step 4** From the drop-down list for Event Identification attribute, you can select **Event-Identification**, which indicates whether the CNS Identification field contains a HOST NAME or CNS ID. Default: HOST NAME.

Saving the Device Configuration

After you are finished making device configuration changes, click the **Continue** button.

The Device Discovery indicator turns green and indicates that Device Discovery is **Complete**.

The Discovery Data Collection phase begins automatically.

Step 3: Perform Discovery Data Collection

After you save your device configuration settings, the Discovery Data Collection phase of Device Discovery starts automatically.

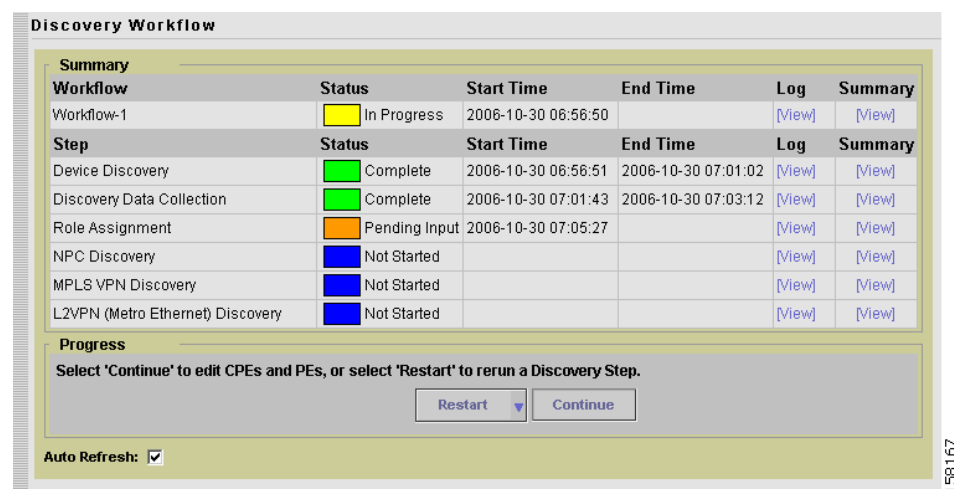
While Cisco IP Solution Center is collecting the device configurations, the Discovery Data Collection indicator is yellow and indicates that the process is **In Progress**.

When the Discovery Data Collection phase is complete, the indicator changes to green and indicates that the process is **Complete**. You are now ready to assign device roles.

Step 4: Perform Role Assignment

After the Discovery Data Collection phase of Device Discovery is complete, the Discovery Workflow window indicates that the Role Assignment phase is **Pending Input**, as shown in [Figure 4-18](#).

Figure 4-18 Discovery Workflow with Role Collection Pending Input



Restarting from Discovery Data Collection prompts you to select the devices for which discovery data collection needs to occur.

Follow these steps to assign device roles:

- Initiate Device Role Assignment
- Change the Device Assignment Display
- Change Device Assignments
- Determine Device Roles
- Assign CE Device Roles
- Assign PE Device Roles

The following sections describe each of these steps.

Initiating Device Role Assignment

Follow these steps to initiate device role assignment:

Step 1 In the Discovery Workflow window, click **Continue**.

The Role Assignment - Un-assigned Devices window appears, as shown in [Figure 4-19](#).

Figure 4-19 Role Assignment - Un-assigned Devices Window

The screenshot shows the 'Role Assignment - Un-assigned Devices' window in the IP Solution Center. The window has a header with the Cisco logo and navigation tabs: Service Inventory, Service Design, Monitoring, Diagnostics, and Administration. The user is logged in as 'admin'. Below the header, there is a breadcrumb trail: 'You Are Here: Service Inventory > Discovery'. The main content area displays a table of unassigned devices. The table has three columns: '#', 'Device Host Name', 'Device Domain Name', and 'Management IP Address'. There are 7 rows of devices, each with a checkbox in the first column. The devices are: 1. lon-3620-ce-e (10.10.0.1), 2. lon-3660-ce-f (10.10.0.3), 3. lon-3660-pe-b (10.10.0.4), 4. nyc-3660-pe-b (10.10.0.6), 5. syd-3620-ce-e (10.10.0.7), 6. syd-3620-ce-f (10.10.0.8), and 7. syd-3660-pe-b (10.10.0.9). Below the table, there is a 'Rows per page' dropdown set to 10 and a 'Go to page' field set to 1 of 1. At the bottom, there are four buttons: 'Un-assigned D', 'Assign as PE(s)', 'Assign as CE(s)', and 'Continue'.

#	Device Host Name	Device Domain Name	Management IP Address
1.	☐ lon-3620-ce-e		10.10.0.1
2.	☐ lon-3660-ce-f		10.10.0.3
3.	☐ lon-3660-pe-b		10.10.0.4
4.	☐ nyc-3660-pe-b		10.10.0.6
5.	☐ syd-3620-ce-e		10.10.0.7
6.	☐ syd-3620-ce-f		10.10.0.8
7.	☐ syd-3660-pe-b		10.10.0.9

On the Role Assignment - Un-assigned Devices window, if you select a single device, you are prompted directly for the device role assignment. However, if you select more than one device, either the Role Assignment - CEs window or the Role Assignment - PEs window appears. On these windows you can specify the desired device roles.

Step 2 If you want to change the way that the devices are displayed, see the following section, [Changing the Device Assignment Display, page 4-39](#).

Changing the Device Assignment Display

You can change the way devices are displayed in the Role Assignment window in the following ways:

- You can change the display to show unassigned devices, PE devices, or CE devices using the pull-down list at the bottom of the Role Assignment window.
- You can change the range of devices that are displayed using the **Show devices with** selection at the top of the window in combination with the **matching** field.

Follow these steps to change the category of devices that is displayed:

-
- Step 1** To change the category of devices that is displayed, select a value from the pull-down list at the bottom of the Role Assignment window:
- To view PE devices, select **PEs**.
 - To view CE devices, select **CEs**.
 - To view unassigned devices, select **Un-assigned Devices**.
- Step 2** To change the range of devices that are displayed, use the **Show devices with** selection at the top of the window in combination with the **matching** field.
- To list devices by hostname, select **Device Host Name** and enter a search value in the matching field, then click **Find**.
 - To list devices by domain name, select **Device Domain Name** name and enter a search value in the matching field, then click **Find**.
 - To list devices by management IP address, select Management IP Address and enter a search value in the matching field, then click **Find**.

The value in the **matching** field specifies a search mask that controls which devices are displayed. An asterisk (*) specifies display of all devices by the selected search criteria. A string followed by an asterisk specifies display of all devices starting with part of a hostname, domain name, or management IP address. And a string preceded by an asterisk specifies display of all devices ending with part of a hostname, domain name, or management IP address.

You can specify more than one wildcard (asterisk) value in a search string. For example, to display all devices that have “ce” in the hostname, enter *ce* in the matching field.

The display changes depending on the selection that you made. For example, if two devices have been assigned the CE role, the Role Assignment - CEs window appears and shows a listing similar to the one in [Figure 4-20](#).

Figure 4-20 Role Assignment - CEs Window

IP Solution Center

Service Inventory | Service Design | Monitoring | Diagnostics | Administration

User: admin

You Are Here: Service Inventory > Discovery

Customer: None

Role Assignment - CEs

Show CEs with CE Device Host Name matching * Find

Showing 1 - 2 of 2 records

#	CE Device Host Name	CE Management Type	CE Site Name	CE Customer Name
1.	☐ lon-3620-ce-e	DIRECT_CONNECTED_REGULAR	lon-3620-ce-e_Customer1_Site	Customer1
2.	☒ lon-3660-pe-b	DIRECT_CONNECTED_REGULAR	lon-3660-pe-b_Customer2_Site	Customer2

Rows per page: 10 Go to page: 1 of 1

CEs Edit Un-assign Assign as PE(s) Continue

Changing Device Assignments

In some instances, the device discovery process assigns the wrong device role to groups of devices. For example, devices that should be PEs can be assigned as CEs.

If this occurs, perform these steps:

- If all the devices you expected would appear as PEs are not listed on the Role Assignment - PEs window, check the Role Assignment - Unassigned Devices window and the Role Assignment - CEs window and assign the devices as PE devices.
 - Go to the Role Assignment - CEs window and select any devices that should be PE devices
 - Click the **Assign as PEs** button

The Role Assignment - PEs window appears and now lists the devices that you assigned as PEs.
- If other devices are not assigned as desired, change their basic device assignment as required.

Assigning Devices Individually or in Bulk

Using the windows provided for Role Assignment, you can assign device roles one device at a time or using bulk assignment (by selecting several devices and assigning them all the same role).

If you assign device roles for a single device, you can also assign the other device attributes, such as Site, Region, etc. However, if you assign device roles in bulk, then you cannot assign the other attributes at this time. You will have to go to the PEs or CEs window later to assign the other attributes.

Determine Device Roles

The purpose of device assignment is to categorize the devices discovered in the provider's network into two general groups:

- Provider-related devices—Provider Edge (PE) devices.

See [Assigning the PE Role, page 4-41](#) for instructions on assigning the PE roles (U-PE, N-PE, P, or PE-AGG).

- Customer-related devices—Customer Edge (CE) devices

See [Assigning the CE Role, page 4-44](#) for instructions on assigning the CE role.

For PE devices, use the following guidelines to determine device roles:

- Assign a device that is at the center of a core domain as a P device.
- Assign any devices that interface with users of the VPN services as U-PE devices. These are devices that are on the customer facing edge of a domain.
- Assign any devices that are on the edge of the MPLS core domain or L2VPN core domain as N-PE devices.
- Assign any devices that are in device rings or which connect to multiple U-PE devices as PE-AGG devices.

For CE devices, see the descriptions of the CE roles in the section on assigning CE roles ([Assigning the CE Role, page 4-44](#)) for specific information.

Assigning the PE Role

Follow these steps to assign a device as a PE device:

-
- Step 1** In the Role Assignment - Un-assigned Devices window, select a device that you want to assign as a PE.
- To select a device, check the check box next to the device name.
 - To deselect a device, uncheck the check box next to the device name.
- Step 2** Click the **Assign as PE(s)** button.
- The Assign as PE window appears, as shown in [Figure 4-21](#).

Figure 4-21 Assign as PE Window

The screenshot shows the 'Assign as PE' window in the IP Solution Center. The window has a header with the Cisco logo and navigation tabs: Service Inventory, Service Design, Monitoring, Diagnostics, and Administration. Below the tabs are links for Inventory and Connection Manager, Discovery, and Device Console. The main content area contains the following fields:

- Device Host Name: syd-3620-ce-f
- PE Region Name: (empty field with a 'Select' button)
- PE Role: N_PE (dropdown menu)

At the bottom of the form are 'OK' and 'Cancel' buttons. A note below the form states: 'Note: * - Required Field'.

Step 3 In the Assign as PE window, assign the required information for the PE.

- a. To assign a PE Region Name, click the **Select** button.

The PE Region Name window appears, as shown in Figure 4-22.

Figure 4-22 PE Region Name Window

The screenshot shows the 'Select Region/Provider' window. It has a search bar at the top with the text 'Show Regions with Region Name matching' and a 'Find' button. Below the search bar, it says 'Showing 1 - 4 of 4 records'. There is a table with the following data:

#	PE Region Name
1.	☐ Cisco HQ
2.	☐ Cisco NYC
3.	☐ Cisco Paris
4.	☐ Cisco SJ

At the bottom of the window are 'Select' and 'Cancel' buttons. A pagination control shows 'Rows per page: 10' and 'Go to page: 1 of 1'.

- b. In the PE Region Name window, click the radio button next to the region name that you want to assign and then click **Select**.

The Assign as PE window appears with the region name in the PE Region field.

- c. To assign a PE role, select a value from the pull-down list for the PE Role field.

The PE role specifies the architectural role that a PE router performs. Assign the PE role based on the network layer to which the device belongs.

You can select the following PE roles:

- **N-PE**—Assign devices that are at the edge of domains (within the Edge layer) as Network Facing Provider Edge (N-PE) devices.
- **U-PE**—Assign devices within the User Facing Provider Edge as U-PE devices.
- **P**—Assign a device that is at the center of a core domain as a Provider Core (P) device.
- **PE-AGG**—Assign devices within the Aggregation Layer as Provider Edge Aggregation (PE-AGG) devices.

d. Click **OK**.

The Role Assignment - PEs window appears with the specified values shown.

Editing the PE Role

After you have assigned one or more devices as PE devices and they appear in the Role Assignment - PEs window, you can edit the PE role. You can edit the PE role even if no values have been assigned in the Assign as PE window.



Note

PE role assignment is not mandatory. However, it is recommended to avoid unexpected behavior.

Follow these steps to edit the Role Assignment values for a PE device:

Step 1

While the Role Assignment phase of Device Discovery is active, choose the Role Assignment - PEs window.

If the Role Assignment - Un-assigned Devices or the Role Assignment - CEs window is active, select **Role-Assignment - PEs** from the pull-down list at the bottom of the window.

The Role Assignment - PEs window appears, as shown in [Figure 4-23](#).

Figure 4-23 *Role Assignment - PEs Window*

IP Solution Center

Service Inventory | Service Design | Monitoring | Diagnostics | Administration

User: admin

You Are Here: Service Inventory > Discovery

Customer: None

Role Assignment - PEs

Show PEs with PE Device Host Name matching * Find

Showing 1 - 3 of 3 records

#	PE Device Host Name	PE Role	PE Provider Name	PE Region Name
1.	☐ nyc-3660-pe-b	UNKNOWN		
2.	☐ syd-3660-pe-b	UNKNOWN		
3.	☐ lon-3660-pe-b	U_PE	Cisco	Cisco Paris

Rows per page: 10

Go to page: 1 of 1 Go

PEs Edit Un-assign Assign as CE(s) Continue

Note that on this window, sorting is disabled for the following columns:

- PE Device Host Name

- PE Provider Name
- PE Region Name.

In the sample window shown in [Figure 4-23](#), one of the PEs has role information assigned. The other two PEs have been assigned as PEs but do not have role information assigned. You can edit any of the information for the PEs, whether information has been entered or not.

Step 2 Select one or more PEs to edit.

- To select a specific PE, check the check box next to the device name.
- To select all the PEs shown in the window, check the check box in the heading row.

Step 3 To edit the PE role, follow these steps:

- Click the **Edit** button at the bottom of the window and choose **PE Role** from the pull-down list. You are prompted to select a PE role.
- Select a value from the pull-down list for the PE Role field.
You can select the following PE roles:
 - **N-PE**—Assign devices within the Edge layer as Network Facing Provider Edge (N-PE) devices.
 - **U-PE**—Assign devices within the User Facing Provider Edge as U-PE devices.
 - **P**—Assign devices within the Core layer as Provider Core (P) devices.
 - **PE-AGG**—Assign devices within the Aggregation Layer as Provider Edge Aggregation (PE-AGG) devices.

The specified PE role appears in the Role Assignment - PEs window.

Step 4 To edit the PE provider name or PE region name, follow these steps:

- Click the **Edit** button at the bottom of the window and choose **Region/Provider** from the pull-down list.
You are prompted for a Region name.
- Click the radio button next to one of the region names listed in the pop-up window and then click the **Select** button.

The specified Region Name and its associated Provider Name appear in the Role Assignment - PEs window.

Assigning the CE Role

Follow these steps to assign a device as a CE device:

Step 1 In the Role Assignment - Un-assigned Devices window, select a device that you want to assign as a CE.

- To select a device, check the check box next to the device name.
- To deselect a device, uncheck the check box next to the device name.

Step 2 Click the **Assign as CE(s)** button.

Step 3 The Assign as CE window appears, as shown in [Figure 4-24](#).

Figure 4-24 Assign as CE Window

The screenshot shows the 'Assign as CE' window in the IP Solution Center. The window has a header with the Cisco logo and navigation tabs: Service Inventory, Service Design, Monitoring, Diagnostics, and Administration. The 'Service Inventory' tab is active, and the 'Discovery' sub-tab is selected. The breadcrumb trail shows 'You Are Here: Service Inventory > Discovery'. The 'Assign as CE' form contains the following fields: 'Device Host Name' with the value 'l0n-3620-ce-e', 'Customer Name' with a 'Select' button, and 'CE Management Type' with a dropdown menu set to 'MANAGED_REGULAR'. There are 'OK' and 'Cancel' buttons at the bottom right. A note at the bottom left states: 'Note: * - Required Field'.

Step 4 In the Assign as CE window, assign the required information for the CE.

- a. To assign a Customer Name (required field), click the **Select** button.

The Customer Name window appears, as shown in [Figure 4-25](#).

Figure 4-25 Customer Name Window

The screenshot shows the 'Select Customer' window. The window title is 'Select Customer - Microsoft Internet Explorer provided by Cisco System...'. It features a search bar with the text 'Show Customers with Customer Name matching *' and a 'Find' button. Below the search bar, it says 'Showing 1 - 2 of 2 records'. There is a table with two columns: '#' and 'Customer Name'. The table contains two rows: '1. Customer1' and '2. Customer2'. At the bottom, there are 'Select' and 'Cancel' buttons. The window also includes a 'Rows per page' dropdown set to '10' and a 'Go to page: 1 of 1' section with a 'Go' button.

- b. To assign a customer name, click the radio button next to the customer name that you want to assign and then click the **Select** button.

The Assign as CE window appears with the specified customer name displayed.

- c. To assign a CE management type, select a value from the pull-down list for the CE Management Type.

The CE Management type specifies the architectural role that a CE router performs. Assign the CE management type based on the network layer to which the device belongs.

You can select the following CE management types:

- **MANAGED-REGULAR**—This is the default CE role assignment. Assign this role to CEs that you want the Provider to manage. The CE must be reachable from an ISC server. When you assign this role, then when you create a router in the Inventory Manager interface, the router configuration is automatically downloaded.
- **UNMANAGED**—Assign this role to a device that you want to manage manually. If this role is assigned, then the device configuration is not assigned automatically when a new device is created and the device must be configured manually. 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-MGMT-LAN**—Specifies that the device management is linked to the PE configuration. The configuration is downloaded automatically when a new device is created. 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-MGMT-LAN**—Specifies that the device management is linked to the PE configuration, but the configuration is not downloaded automatically when a new device is created. 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.
- **DIRECT-CONNECTED-REGULAR**—In most cases, the CE is connected to a PE router. In this case, the CE is connected to a workstation or other device.
- **DIRECT-CONNECTED-MGMT-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**—Specifies that there is a device between the PE and the CE that is a VPN routing/forwarding instance (VRF). A multi-VRF CE (MVRFCE) 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.

d. Click **OK**.

The Role Assignment - CEs window appears with the specified values shown.



Note

The CE Site value is unassigned at this point. To assign this value, you must edit the settings. See [Editing the CE Role, page 4-46](#) for instructions on this task.

Editing the CE Role

After you have assigned one or more devices as CE devices and they appear in the Role Assignment - CEs window, you can edit the CE role. You can edit the CE role even if no values have been assigned in the Assign as CE window.

Follow these steps to edit the Role Assignment values for a CE device:

Step 1 While the Role Assignment phase of Device Discovery is active, choose the Role Assignment - CEs window.

If the Role Assignment - Un-assigned Devices or the Role Assignment - PE window is active, select **Role-Assignment - CEs** from the pull-down list at the bottom of the window.

The Role Assignment - CEs window appears, as shown in Figure 4-26.

Figure 4-26 Role Assignment - CEs Window

The screenshot shows the 'Role Assignment - CEs' window in the IP Solution Center. The window has a search bar at the top with 'CE Device Host Name' selected and a 'Find' button. Below the search bar, it says 'Showing 1 - 4 of 4 records'. The table below has the following data:

#	CE Device Host Name	CE Management Type	CE Site Name	CE Customer Name
1.	☐ lon-3620-ce-e	UNKNOWN		
2.	☐ lon-3660-ce-f	UNKNOWN		
3.	☐ syd-3620-ce-e	MULTI_VRF	syd-3620-ce-e_Customer2_Site	Customer2
4.	☐ syd-3620-ce-f	MULTI_VRF	syd-3620-ce-f_Customer2_Site	Customer2

At the bottom of the window, there is a 'Rows per page' dropdown set to 10, a 'Go to page' field set to 1 of 1, and buttons for 'CEs', 'Edit', 'Un-assign', 'Assign as PE(s)', and 'Continue'.

In the sample Role Assignment - CEs window shown in Figure 4-26, two of the CEs have role assignment information assigned, and two have no information assigned. You can edit any of the information for the CEs, whether information has been entered or not.

Note that on this window, sorting is disabled on the following columns:

- CE Device Host Name
- CE Site Name
- CE Customer Name

Step 2 Select one or more CEs to edit.

- To select a specific CE, check the check box next to the device name.
- To select all the CEs shown in the window, check the check box in the heading row.

Step 3 To edit the Customer name, follow these steps:

- Click the **Edit** button at the bottom of the window and choose **Customer** from the pull-down list. You are prompted to select a customer name.
- To select a customer name, click the radio button next to one of the customer names that is displayed, and then click the **Select** button.

The Role Assignment - CEs window appears with the specified customer name displayed.

Step 4 To edit the CE management type, follow these steps:

- Select one or more CEs to edit.
- Click the **Edit** button at the bottom of the window and choose **CE Management Type** from the pull-down window.

The CE Management type specifies the architectural role that a CE router performs. Assign the CE management type based on the network layer to which the device belongs.

You can select the following CE management types:

- **MANAGED-REGULAR**—This is the default CE role assignment. Assign this role to CEs that you want the Provider to manage. The CE must be reachable from an ISC server. When you assign this role, then when you create a router in the Inventory Manager interface, the router configuration is automatically downloaded.
- **UNMANAGED**—Assign this role to a device that you want to manage manually. If this role is assigned, then the device configuration is not assigned automatically when a new device is created and the device must be configured manually. 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-MGMT-LAN**—Specifies that the device management is linked to the PE configuration. The configuration is downloaded automatically when a new device is created. 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-MGMT-LAN**—Specifies that the device management is linked to the PE configuration, but the configuration is not downloaded automatically when a new device is created. 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.
- **DIRECT-CONNECTED-REGULAR**—In most cases, the CE is connected to a PE router. In this case, the CE is connected to a workstation or other device.
- **DIRECT-CONNECTED-MGMT-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**—Specifies that there is a device between the PE and the CE that is a VPN routing/forwarding instance (VRF). A multi-VRF CE (MVRFCCE) 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.

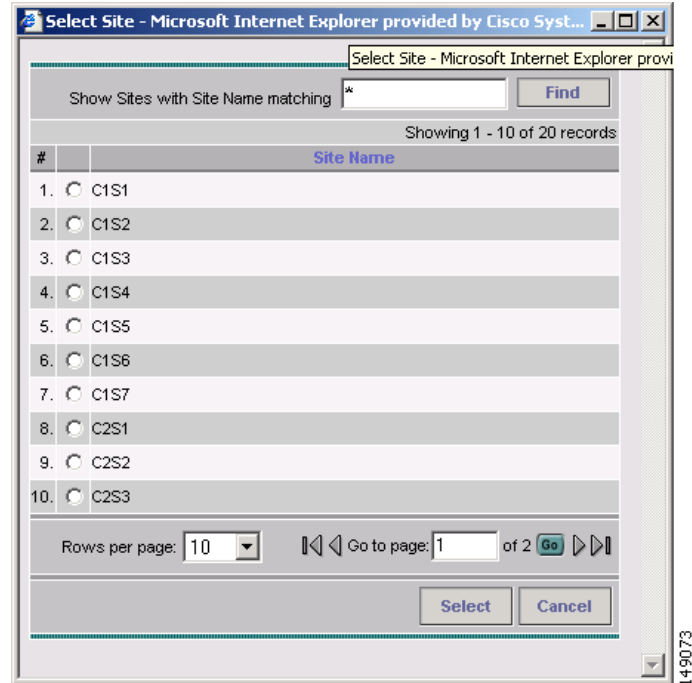
c. Click **Select**.

The Role Assignment - CEs window appears with the specified CE management type displayed.

Step 5 To specify a site name or edit an existing site name, follow these steps:

- a. Select one or more CEs to edit.
- b. Click the **Edit** button at the bottom of the window and choose **Site** from the pull-down window.

The Site Name window appears, as shown in [Figure 4-27](#).

Figure 4-27 Site Name Window

- c. In the Site Name window, click the radio button next to the site name that you want to assign and then click the **Select** button.

The Role Assignment - CEs window appears with the specified site names displayed.

Saving the Role Assignment Information

After you finish assigning roles to the devices, click the **Continue** button.

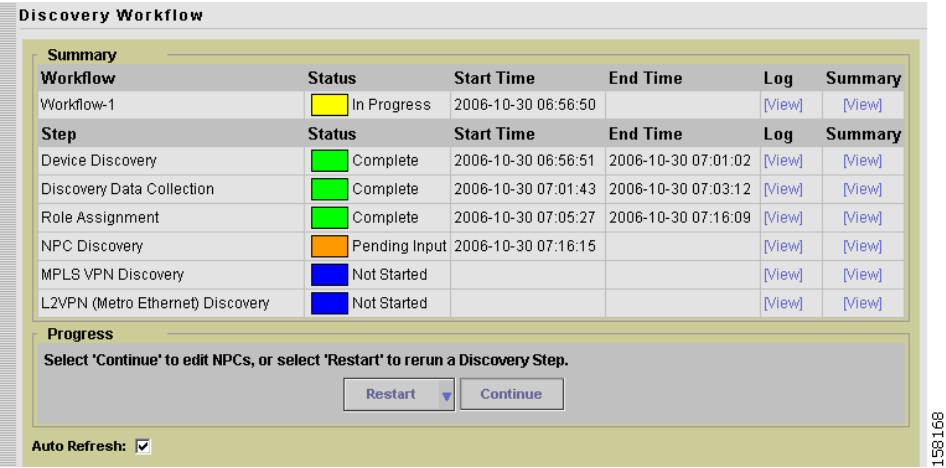
The Role Assignment Discovery indicator turns green and indicates that Role Assignment is **Complete**.

You are now ready to start the NPC Discovery phase of Device Discovery.

Step 5: Perform NPC Discovery

After the Role Assignment phase of Device Discovery is complete, the Discovery Workflow window indicates that the NPC Discovery phase is **Pending Input**, as shown in Figure 4-28.

Figure 4-28 Discovery Workflow with NPC Discovery Pending Input



Follow these general steps to view a list of the NPCs that have been discovered and add or remove NPCs as required:

- If you are discovering a *Metro Ethernet topology with an Ethernet core*, perform the steps described in [Preliminary Steps Before Completing NPC Discovery for Metro Ethernet Networks](#), page 4-50.
- Complete the steps for starting NPC assignment as described in [Starting NPC Assignment](#), page 4-52
- If necessary, complete steps for adding or modifying NPCs as described in [Adding a Device for an NPC](#), page 4-54 and the sections that follow.

Preliminary Steps Before Completing NPC Discovery for Metro Ethernet Networks

Follow these steps if you are discovering a Metro Ethernet topology with an Ethernet core.

- Create one or more Access Domains and assign the devices that were discovered in the Device Discovery phase to the Access Domain(s).
- Create at least one Resource Pool.
- Edit the “inter N-PE interface” for each device.

These steps are performed using the Inventory and Connection Manager in the Service Inventory interface (**Service Inventory > Inventory and Connection Manager**).

Create Access Domains

Follow these steps to create access domains and add discovered devices to the domains:

-
- Step 1** In the ISC start page, select **Service Inventory**.
- Step 2** In the Service Inventory window, select **Inventory and Connection Manager**.
The Inventory and Service manager window appears.
- Step 3** In the left area of the window, select **Access Domains**.
The Access Domains window appears.
- Step 4** Create one or more Access Domains and assign the devices in the L2VPN Metro Ethernet topology to these Access Domains.
For detailed instructions on creating Access Domains, see the [“Creating Access Domains”](#) section on page 3-125.
-

Create Resource Pools

Follow these steps to create a resource pool:

-
- Step 1** In the ISC start page, select **Service Inventory**.
- Step 2** In the Service Inventory window, select **Inventory and Connection Manager**.
The Inventory and Service manager window appears.
- Step 3** In the left area of the window, select **Resource Pools**.
The Resource Pools window appears.
- Step 4** Create a Resource Pools.
- Step 5** For the **Pool Type**, make sure that you select **VLAN**.
- Step 6** For the **Start** value, enter 2.
- Step 7** For the **Pool Size** value, enter a value large enough to accommodate the number of devices in the resource pool, for example, 500.
For detailed instructions on creating Resource Pools, see the [“Resource Pools”](#) section on page 3-126.
-

Edit Inter-N-PE Interfaces

Follow these steps to edit the “Inter N-PE” interfaces for the devices in your Metro Ethernet topology:



Note

These steps are only required if the PE devices already exist in the repository.

-
- Step 1** In the ISC start page, select **Service Inventory**.
- Step 2** In the Service Inventory window, select **Inventory and Connection Manager**.
The Inventory and Service manager window appears.

Step 3 In the left area of the window, select **PE Devices**.

The PE Devices window appears.

Step 4 Select each PE device in your topology and do the following:

a. Click the **Edit** button

The Edit PE window appears.

b. Locate the interface that connects to each device that the device is connected to.

c. For each interface, in the Metro Ethernet column, change **Any** to **None**.

d. Save your changes

Go the following section, [Starting NPC Assignment](#), page 4-52 and follow the steps for starting NPC assignment.

Starting NPC Assignment

Follow these steps to initiate NPC assignment:

Step 1 In the Discovery Workflow window, click **Continue**.

The Named Physical Circuits window appears, as shown in [Figure 4-29](#).

Figure 4-29 *Named Physical Circuits Window*

Named Physical Circuits							
Show NPCs where Name matching * Find							
Showing 1 - 3 of 3 records							
#	☐	Source Device	Source Interface	Destination Device	Destination Interface	Name	State
1.	☐	iscind-3750-7	FastEthernet1/0/11	iscind-7600-2	FastEthernet2/1/0	1-(iscind-3750-7-FastEthernet1/0/11)<==>(iscind-7600-2-FastEthernet2/1/0)	NEW
2.	☐	iscind-3750-2	FastEthernet1/0/14	iscind-7600-2	FastEthernet2/1/4	2-(iscind-3750-2-FastEthernet1/0/14)<==>(iscind-7600-2-FastEthernet2/1/4)	NEW
3.	☐	iscind-3750-1	FastEthernet1/0/23	iscind-7600-2	FastEthernet2/1/9	3-(iscind-3750-1-FastEthernet1/0/23)<==>(iscind-7600-2-FastEthernet2/1/9)	NEW

Rows per page:

The Named Physical Circuits window initially displays any discovered circuits.

At this point, you can create, add, or remove NPCs as required.

The State column has the following categories:

- **New**—No corresponding NPC exists in ISC. Only the New NPCs are committed to ISC.
- **Existing**—The discovered NPC is the same as the NPC in ISC.

- **Existing Modified** —The NPC in ISC has the same source and endpoint but one or more of the intermediate links might not be the same.
- **Conflicting**—The discovered NPC conflicts with the NPC in ISC.

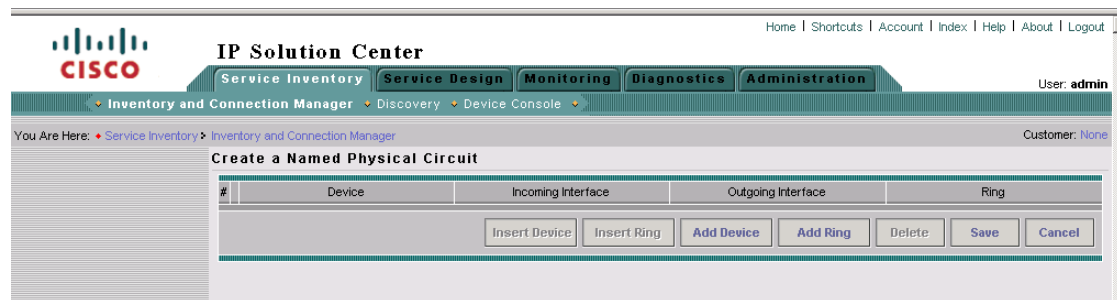
Named physical circuits (NPCs) are named circuits that describe a physical connection between a CPE or U-PE and a N-PE. The intermediate nodes of the NPCs can either be U-PE or PE-AGG. They can be connected in a circular fashion forming a ring of devices, which is represented by an entity known as NPC Rings. NPC Rings represent the circular topology between devices to the Named Physical Circuits. To create an NPC, you must specify how the source CPE/U-PE and the destination N-PE are connected and specify the intermediate nodes.

Step 2 If you need to define an NPC, follow these steps:

- In the Named Physical Circuits window, click **Create**.

The Create a Physical Circuit window appears, as shown in [Figure 4-30](#).

Figure 4-30 Create Physical Circuits Window.

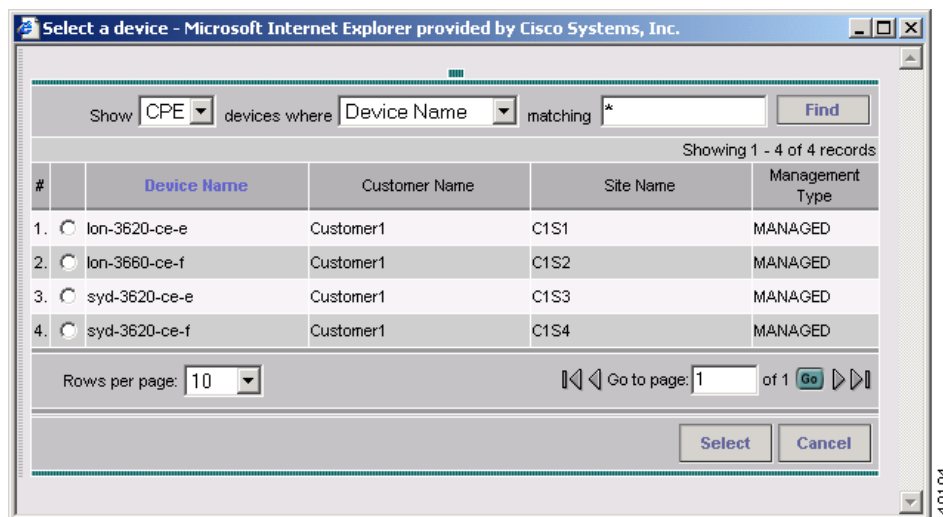


Initially, the list of NPCs is empty.

- Click the **Add Device** button

The Select a Device window appears, as shown in [Figure 4-31](#).

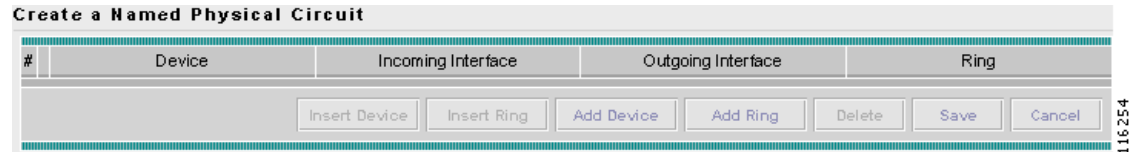
Figure 4-31 Select a Device Window



Step 3 In this window, click the radio button for a device and then click the **Select** button.

The Create a Named Physical Circuit window appears with an initial device added, as shown in [Figure 4-32](#).

Figure 4-32 Create a Named Physical Circuit Window with Initial Device Added



The buttons on the window are now active.

- c. Click a device that appears in the screen and then select one of the following actions:
 - To insert a device, click the **Insert Device** button.
 - To insert a ring, click the **Insert Ring** button.
 - To add a device, click the **Add Device** button.
 - To add a ring, click the **Add Ring** button.
 - To delete an existing device or ring, select a device and then click the **Delete** button.

Step 4 Refer to the following sections for additional information.

Adding a Device for an NPC

- Step 1** To select an incoming interface on the Create a Named Physical Circuit window click on **Select Incoming Interface**.

The Select Device Interface window appears, as shown in [Figure 4-33](#).

Figure 4-33 **Select Device Interface Window**

#	Interface Name	IP Address	Logical Name
1.	☐ GigabitEthernet0/1	192.168.133.160/24	
2.	☐ GigabitEthernet0/10		
3.	☐ GigabitEthernet0/11		
4.	☐ GigabitEthernet0/12		
5.	☐ GigabitEthernet0/2		
6.	☐ GigabitEthernet0/3		
7.	☐ GigabitEthernet0/4		
8.	☐ GigabitEthernet0/5		
9.	☐ GigabitEthernet0/6		
10.	☐ GigabitEthernet0/7		

This window shows the interfaces on the selected device.

- Step 2** Click the radio button next to an interface in the list and then click the **Select** button.
The selected interface now appears in the Create a Named Physical Circuit window.
- Step 3** To select an outgoing interface, click on **Select Outgoing Interface**.
A list of interfaces configured on the device appears
- Step 4** Click the radio button next to an interface in the list and then click the **Select** button.
The outgoing interface now appears in the Create a Named Physical Circuit window.
- Step 5** Select additional devices as required and specify incoming and/or outgoing interfaces.
- Step 6** After you are finished, click the **Save** button in the Create a Named Physical Circuit window.

Adding a Ring

Follow these steps to add a ring before the currently selected device:



Note

Incremental service discovery of rings is not supported.

- Step 1** In the Create a Named Physical Circuit window, click **Add Ring**.
The Select NPC Rings window appears. This window shows any rings that exist in the network topology.

- Step 2** Click the radio button next to a ring listed in the window and then click the **Select** button.
The selected ring now appears in the Create a Named Physical Circuit window.
-

Inserting a Device

To insert a device after the last device in the topology, follow these steps:

-
- Step 1** In the Create a Named Physical Circuit window, click the **Insert Device** button.
The Select a Device window appears, as shown in [Figure 4-31](#).
- Step 2** Check the check box next to a device that you want to insert and then click the **Select** button.
The device now appears on the Create a Named Physical Circuit window.
- Step 3** Click **select incoming interface**.
A list of interfaces on the selected device appears.
- Step 4** Check the check box next to the interface that you want to choose and then click **Select**.
The selected interface now appears on the list of interfaces.
-

Inserting a Ring

To insert a ring after the last device in the topology, follow these steps:

-
- Step 1** In the Create a Named Physical Circuit window, click the **Insert Ring** button.
A list of the currently existing rings appears.
- Step 2** In the list of rings, check the check box next to the ring that you want to insert and then click **Select**.
The selected ring now appears on the Create a Named Physical Circuit window.
-

Deleting a Device or a Ring

Follow these steps to delete a device or a ring:

-
- Step 1** In the Create a Named Physical Circuit window, select a device or ring and then click the **Delete** button.
The create NPC window appears with the device deleted.
-

Saving the NPC Configuration

After you have selected two devices and have configured the connection between them, follow these steps to save the NPC configuration:

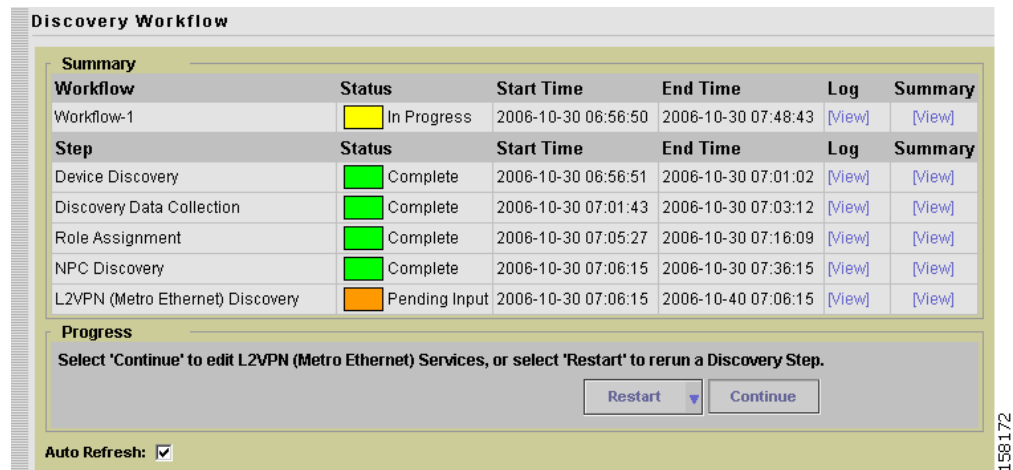
Step 1 In the Create a Named Physical Circuit window, click **Save**.

The NPC process validates the NPC configuration.

Step 2 Click **Continue** to continue.

The workflow window appears with NPC discovery marked as completed, as shown in Figure 4-34.

Figure 4-34 NPC Complete Window



Step 6: Perform MPLS VPN Service Discovery (Optional)

After you have completed the NPC Discovery phase of Device discovery, if you selected **MPLS VPN Discovery** when you initiated the Discovery process, the NPC Discovery phase is marked as complete, and the MPLS VPN Discovery step is marked as **Pending Input**.

You are now ready to initiate configuration of the discovered MPLS VPN using the MPLS VPN Discovery user interface. Follow these steps to configure MPLS VPN services:



Note

MPLS service discovery does not support devices running IOS XR.

Step 1 In the Discovery Workflow window, click **Continue**.

The MPLS VPNs window appears and lists the MPLS VPNs that were discovered. The status of the discovered MPLS VPNs is indicated as follows:

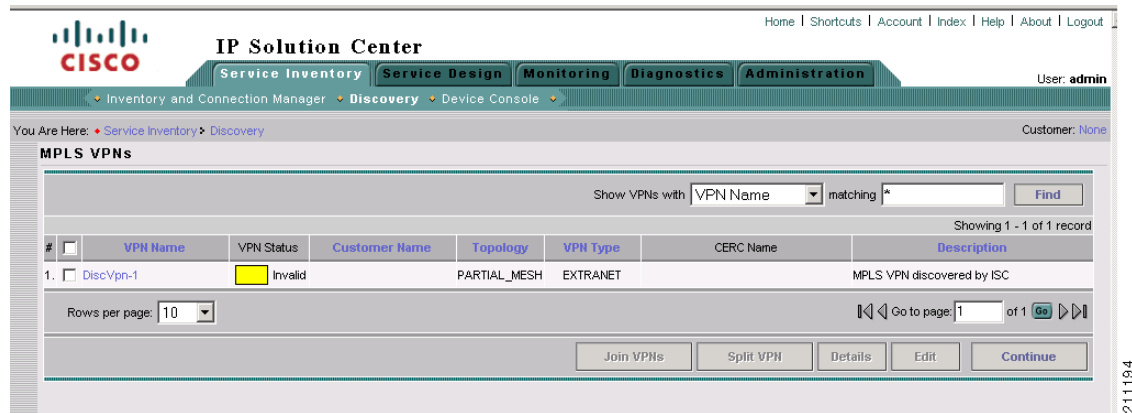
- If the MPLS VPN topology for a discovered MPLS is valid and ready to save in the ISC Repository, then the VPN Status indicates a **Valid** VPN and the status indicator is green.

Step 6: Perform MPLS VPN Service Discovery (Optional)

- If the MPLS VPN topology for a discovered MPLS is invalid (the topology is Partial Mesh), is missing a Customer assignment, or includes an invalid CERC, then the VPN Status indicates an **Invalid** VPN and the status indicator is yellow. Partial Mesh topology VPNs are not supported by Cisco ISC, and must be broken into Full Mesh and/or Hub and Spoke components.

The MPLS VPN window shown in [Figure 4-35](#) shows an invalid MPLS VPN (the topology is Partial Mesh and the Customer Name is blank).

Figure 4-35 MPLS VPNs Window with Invalid MPLS VPN

**Note**

If the MPLS VPN Discovery process discovers an MPLS VPN with a Partial Mesh topology, you must split the VPN into two or more separate VPNs that have a supported topology (Hub and Spoke or Full Mesh).

Step 2 Do one of the following:

- If you want to change the view in the MPLS VPNs window, select another view option.
For a description of the MPLS VPN view options, see [Filtering the MPLS VPN View, page 4-59](#).
- If the MPLS VPNs are valid and you do not need to make any changes to the MPLS VPN topology at this time, click **Continue** to create MPLS VPN services based on the discovered topology.
- If one or more of the discovered MPLS VPNs are invalid, you must complete the following steps:
 - **Split the VPN**—Select an invalid VPN and then click the **Split VPN** button.
See [Splitting a VPN, page 4-59](#) for instructions.
 - **Create New VPNs and add CERCs**—You must create new VPNs containing the devices in the VPN that you have split, and add CERCs to each new VPN.
See [Creating a VPN, page 4-62](#) for instructions.

Filtering the MPLS VPN View

Follow these steps to change the view in the MPLS VPNs window:

-
- Step 1** Pull down the menu next to the **Show VPNs with** field.
- You can filter the list of VPNs by VPN Name, Customer Name, Topology, VPN Type, or Description.
- Step 2** To limit which VPNs are displayed within the selected category, enter a value in the **Matching** field.
- The value in the **matching** field specifies a search mask that controls which sites are displayed. An asterisk (*) specifies display of all sites by the selected search criteria. A string followed by an asterisk specifies display of all sites starting with part of the element specified in the **Show VPNs with** field.
- You can specify more than one wildcard (asterisk) value in a search string. For example, to display all VPNs that have “cisco” as part of the Customer Name, enter *cisco* in the matching field.
- The display changes to display the VPNs with the selected criteria.
-

Splitting a VPN

In some situations, you might need to split an existing MPLS VPN before you complete the MPLS VPN Discovery process and actually create the MPLS VPN services.

For example:

- If the MPLS Service Discovery process discovers an invalid MPLS VPN (an MPLS VPN with a Partial Mesh topology), you must split the VPN into two or more CERCs that have a supported topology (Hub and Spoke or Full Mesh).
- You might also choose to split MPLS VPNs to change your topology, depending on your processing needs. Only one VPN can be split at a time.

Follow these steps to split a VPN:

-
- Step 1** In the MPLS VPNs window, check the check box next to a VPN that you want to split.
- Step 2** Click the **Split VPN** button.

The Split VPN window appears, as shown in [Figure 4-36](#) and [Figure 4-37](#).

Step 6: Perform MPLS VPN Service Discovery (Optional)

Figure 4-36 Split VPN Window (Left Portion)

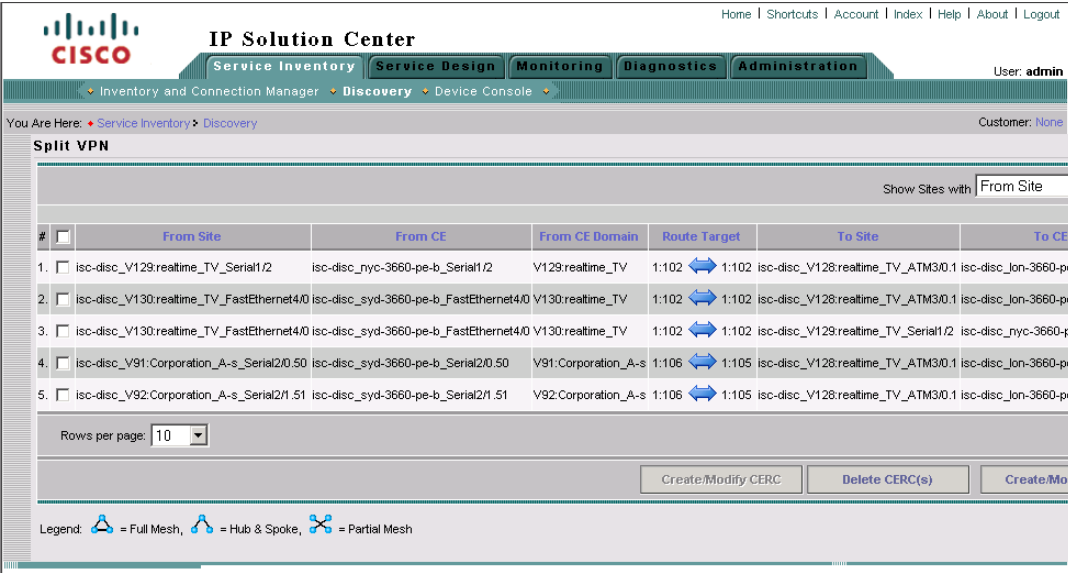
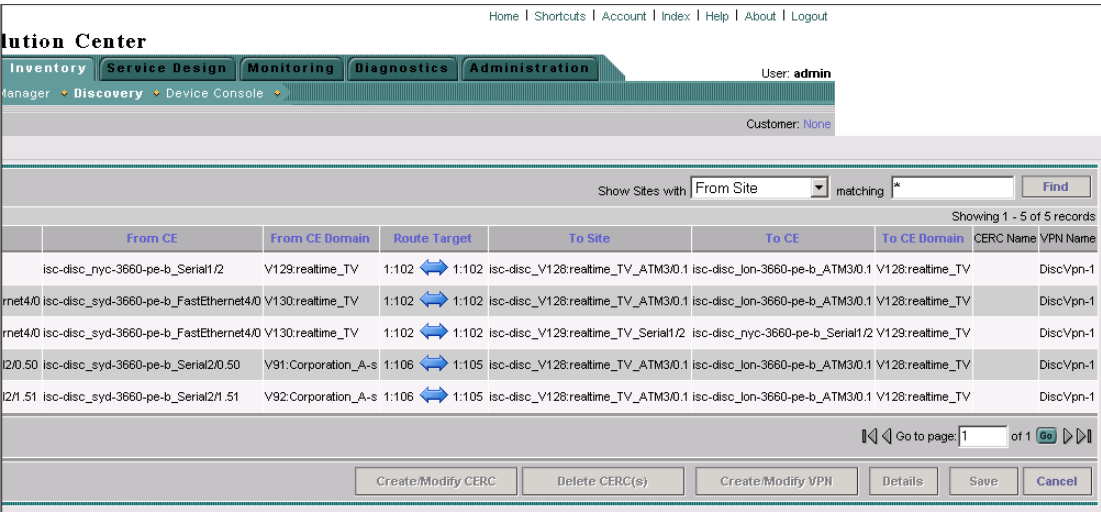


Figure 4-37 Split VPN Window (Right Portion)



Step 3 In the Split VPN window, select several of the links.

In the example shown in [Figure 4-37](#), select the links that would comprise either a Hub and Spoke or Full Mesh topology.

For example, in the Split VPN window shown in [Figure 4-36](#) and [Figure 4-37](#), the first three links all have Route Targets of **1:102** and together form a Full Mesh topology.

The remaining two links have Route Targets of **1:106** and **1:105**. These links together form a Hub and Spoke topology.

To split this VPN, the first three links need to be associated with one CERC, and the two remaining links need to be associated with another CERC. Then we can split this VPN into two separate VPNs following the ISC best practice convention of one CERC per VPN.

Step 4 Click the **Create/Modify CERC** button.

You are prompted for a CERC name.

Step 5 Enter the new CERC name and then click the **Save** button.

Step 6 Repeat these steps for the rest of the devices that are included in invalid VPNs.

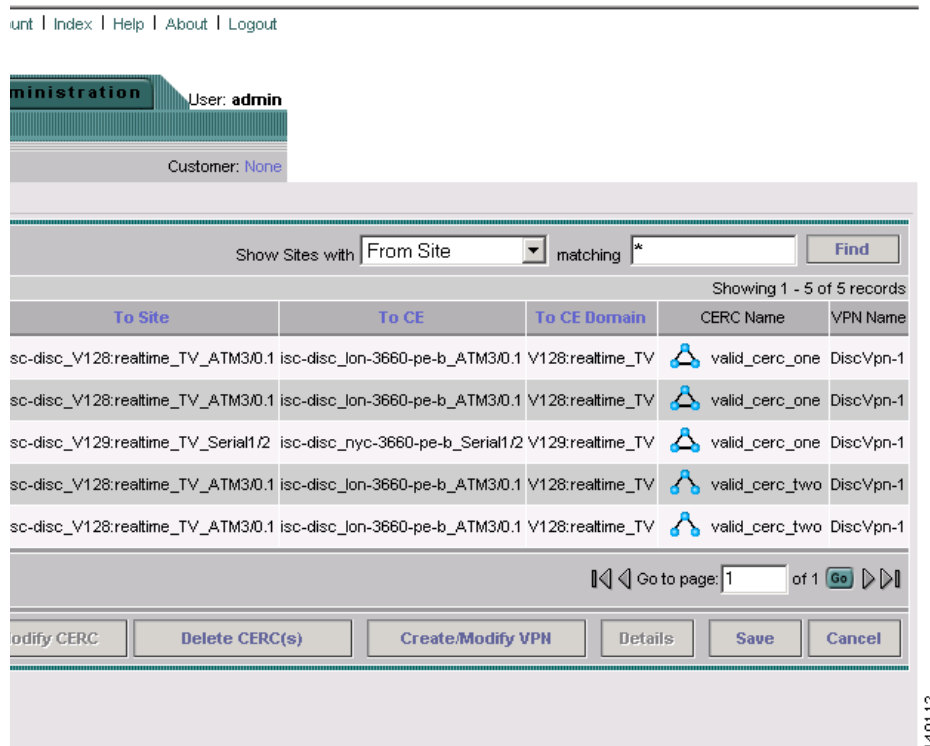
For example, in the topology shown [Figure 4-36](#) and [Figure 4-37](#), select the devices that have the route target **1:106 to 1:105**.

Step 7 Click the **Create/Modify CERC** button.

Step 8 When you are prompted for a CERC name, enter the new CERC name and then click the **Save** button. The Split VPNs window appears again, and the right portion of the window shows the new CERCs that have been created.

[Figure 4-38](#) shows an example.

Figure 4-38 Split VPNs Window After Creation of a Valid CERC Topology



Notice that in the example in [Figure 4-38](#), the two new CERCs that have been created (**valid_cerc_one** and **valid_cerc_two**), have valid topologies. The first CERC, **valid_cerc_one**, has a Full Mesh topology and the second CERC, **valid_cerc_two**, has a Hub and Spoke topology.

Step 9 Click the **Save** button.

You are now ready to continue to the next step, creating VPNs and adding CERCs to the VPNs.

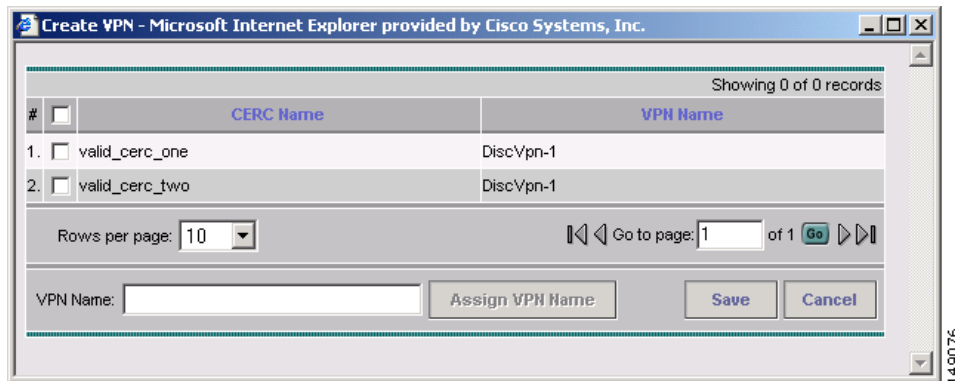
Creating a VPN

After you have created a CERC, you must create a VPN and then add the CERC to it.

Follow these steps to create a VPN:

- Step 1** In the Split VPN window, select **Create/Modify VPN**.
The Create VPN window appears, as shown in [Figure 4-39](#).

Figure 4-39 Create VPN Window



- Step 2** Select the CERCs that you want to assign to the VPN.
In the example shown in [Figure 4-39](#), select **valid_cerc_one**.
- Step 3** In the VPN Name field, enter a name for the VPN.
For this example, enter **vpn_one**.
- Step 4** Click the **Assign VPN Name** button.
- Step 5** Click **Save**.
The VPN is created and appears in the Split VPN window in the VPN Name field.
- Step 6** Create any additional VPNs as needed.
Continuing with the CERCs shown in the sample windows in [Splitting a VPN, page 4-59](#), a VPN must be created and have a CERC assigned to it. To do this:
- In the Split VPN window, click **Create/Modify VPN**.
 - In the Create VPN window, create a second VPN and assign a CERC to it.
In the example screen, you could select the second CERC (**valid_cerc_two**) to the newly created VPN to it.
- Step 7** After you are finished creating VPNs, click the **Save** button in the Split VPN window.
The MPLS VPNs window appears, as shown in [Figure 4-40](#).

Figure 4-40 MPLS VPNs Window with Valid VPN and Invalid VPN

The screenshot shows the IP Solution Center interface. The top navigation bar includes links for Home, Shortcuts, Account, Index, Help, About, and Logout. The main menu has tabs for Service Inventory, Service Design, Monitoring, Diagnostics, and Administration. The left sidebar shows a breadcrumb trail: You Are Here: Service Inventory > Discovery. The main content area is titled 'MPLS VPNs' and contains a search bar with a dropdown for 'VPN Name' and a 'Find' button. Below the search bar, it says 'Showing 1 - 2 of 2 records'. A table lists the VPNs:

#	VPN Name	VPN Status	Customer Name	Topology	VPN Type	CERC Name	Description
1.	vpn_one	Invalid	Customer1	HUB_AND_SPOKE	EXTRANET	valid_cerc_two	MPLS VPN discovered by ISC
2.	vpn_two	Valid	Customer2	FULL_MESH	INTRANET	valid_cerc_one	MPLS VPN discovered by ISC

Below the table, there is a 'Rows per page' dropdown set to 10, and a pagination control showing 'Go to page: 1 of 1'. At the bottom of the table, there are buttons for 'Join VPNs', 'Split VPN', 'Details', 'Edit', and 'Continue'. In the bottom left corner, a 'Status' box shows 'Operation: Edit VPN' and 'Status: Succeeded' with a green checkmark icon.

**Note**

In the example shown in [Figure 4-40](#), one of the VPNs is marked as **Valid** and has a green status indicator. However, the other VPN shown in the window is marked as **Invalid** and has a yellow indicator.

This occurs because in some instances, the MPLS Discovery process cannot completely validate the data. In this situation, you can still continue with the Service Discovery process and create MPLS VPN services. However, the process will skip the invalid VPN, and you must configure the VPN service manually using the ISC provisioning commands.

Step 8 Follow these steps to assign a Customer to each VPN:

- a. Select a VPN entry in the MPLS VPNs window and then click the **Edit** button.

The Edit VPN window appears, as shown in [Figure 4-41](#).

Figure 4-41 Edit VPN Window

The screenshot shows the 'Edit VPN' window in the Cisco IP Solution Center. The window has a header with the Cisco logo and 'IP Solution Center'. Below the header is a navigation bar with tabs for 'Service Inventory', 'Service Design', 'Monitoring', 'Diagnostics', and 'Administration'. The 'Service Inventory' tab is selected. Below the navigation bar is a breadcrumb trail: 'You Are Here: Service Inventory > Discovery'. The main content area is titled 'Edit VPN' and contains several fields: 'VPN Name' with the value 'vpn_one', 'Customer Name' with the value 'Customer2' and a 'Select' button, 'CE Routing Communities' with the value 'valid_cerc_one' and a 'Rename' button, and 'Description' with the value 'MPLS VPN discovered by ISC'. At the bottom of the form are 'Save' and 'Cancel' buttons. A note at the bottom left states: 'Note: * - Required Field'. The top right of the window shows the user 'admin' and a 'Logout' link. The bottom right corner of the window has a vertical text '211197'.

- b. Click the **Select** button next to the Customer Name field.
A list of customer names appears.
- c. Click the radio button next to customer name and then **Select**.
- d. If you want to rename the CERC, click **Rename** and then rename it.
- e. Click **Save**.

The Customer name now appears in the MPLS VPNs window.



Note

In some cases, an apparently valid VPN will be marked as invalid. This VPN will be skipped in the processing. You will then have to configure it manually using the ISC provisioning commands.

- Step 9** After you are finished editing VPNs, click the **Continue** button to initiate the MPLS VPN service creation process.

Viewing VPN Link Details

Follow these steps to view details of VPNs that were discovered:

- Step 1** In the MPLS VPNs window, select a VPN that has details you want to view and then click the **Details** button.
The MPLS VPN Link window appears, as shown in [Figure 4-42](#).

Figure 4-42 MPLS VPN Links Window

IP Solution Center

Service Inventory | Service Design | Monitoring | Diagnostics | Administration

User: admin

Are Here: Service Inventory > Discovery

Customer: None

MPLS VPN Links - Hub and Spoke

VPN Name: vpn_one

CERC Name(s): valid_cerc_two

Show Sites with: From Site matching: * Find

Showing 1 - 2 of 2 records

#	From Site	From CE	From CE Domain	Route Target	To Site	To CE	To CE Domain
1.	isc-disc_V91:Corporation_A-s_Serial2/0.50	isc-disc_synd-3660-pe-b_Serial2/0.50	V91:Corporation_A-s	1:106	isc-disc_V128:realtime_TV_ATM3/0.1	isc-disc_Ion-3660-pe-b_ATM3/0.1	V128:realtime_TV
2.	isc-disc_V92:Corporation_A-s_Serial2/1.51	isc-disc_synd-3660-pe-b_Serial2/1.51	V92:Corporation_A-s	1:106	isc-disc_V128:realtime_TV_ATM3/0.1	isc-disc_Ion-3660-pe-b_ATM3/0.1	V128:realtime_TV

Rows per page: 10

Go to page: 1 of 1

Details Close

Legend: = Hub Site

Step 2 To filter the MPLS VPN links that are displayed, select a value from the pull-down list in the **Show Sites with** field.

You can filter the list of VPNs by From Site, From CE, From CE Domain, Route Target, To Site, To CE, or to CE Domain.

The value in the **matching** field specifies a search mask that controls which sites are displayed. An asterisk (*) specifies display of all sites by the selected search criteria. A string followed by an asterisk specifies display of all sites starting with part of the element specified in the **Show Sites with** field.

You can specify more than one wildcard (asterisk) value in a search string. For example, to display all sites that have “realtime” in the From CE Name, select **From CE Name** in the **Show Sites with** field and then name, enter *realtime* in the matching field.

The display changes to show only the specified links.

Saving the MPLS VPNs and Initiating MPLS VPN Service Creation

After you are finished editing the data for the discovered MPLS VPNs in the MPLS VPNs window, click the **Continue** button.

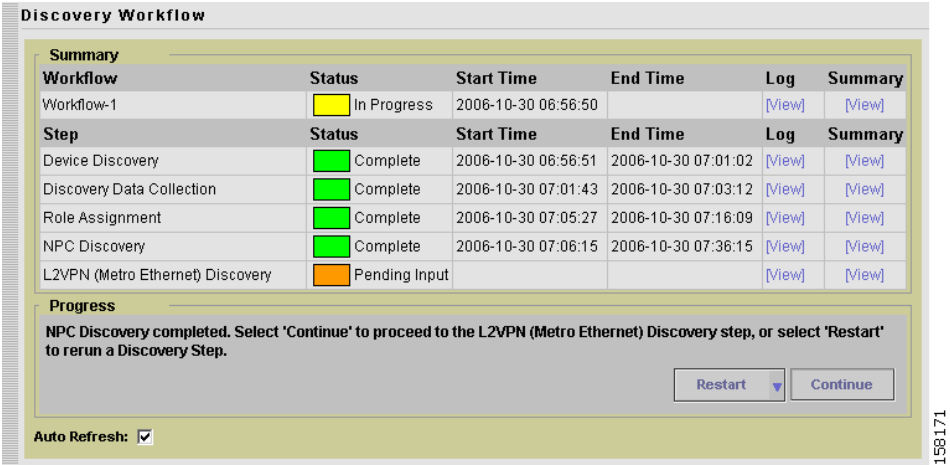
The Discovery process creates VPN services. After the process is complete, the Discovery Workflow window indicates that the MPLS VPN Discovery process is **COMPLETE** and the status indicator is green.

If you also selected **L2VPN (Metro Ethernet) Discovery** in the Discovery window before starting the Discovery process, you can now proceed to Metro Ethernet service discovery.

Step 7: Perform L2VPN (Metro Ethernet) Service Discovery (Optional)

If you selected **L2VPN (Metro Ethernet) Discovery** in the Discovery window before starting the Discovery process, then after the previous steps are complete, the Discovery Workflow window shows the L2VPN (Metro Ethernet) Discovery as **Pending Input**, as shown in [Figure 4-43](#).

Figure 4-43 Discovery Workflow Window with MPLS Ethernet Discovery Pending Input



Follow these steps to initiate Metro Ethernet Service Discovery:



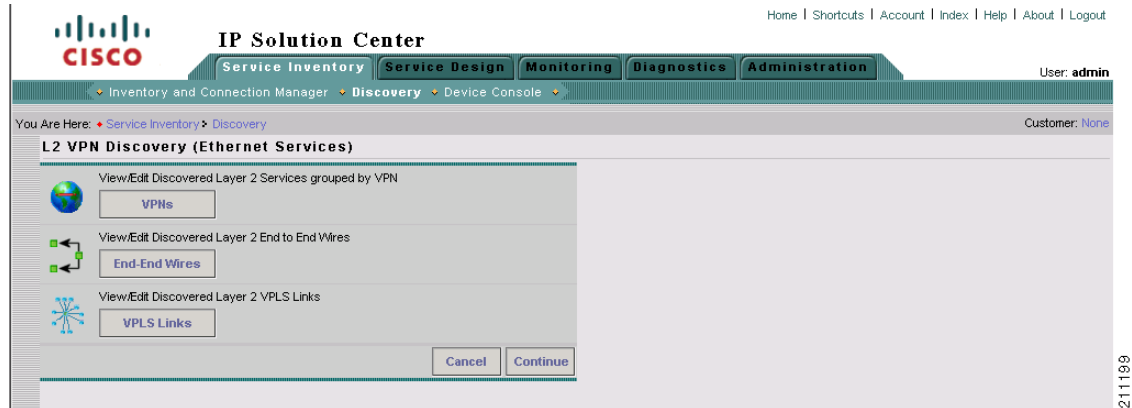
L2VPN service discovery does not support devices running IOS XR.

- Step 1** Before you initiate Metro Ethernet Service Discovery, follow these steps:
- Choose **Service Inventory > Inventory and Connection Manager**.
 - In the task pane at the left of the Inventory and Connection Manager window, select **Access Domains**.
 - Create access domains for any N-PE devices in the Metro Ethernet topology.
For detailed instructions, see the [“Creating Access Domains” section on page 3-125](#).
 - Choose **Service Inventory > Inventory and Connection Manager**.
 - In the task pane at the left of the Inventory and Connection Manager window, select **Resource Pools**.
 - Create resource pools for each of the access domains that you created.
For detailed instructions, see the [“Resource Pools” section on page 3-126](#).
 - Choose **Service Inventory > Discovery**.

The Discovery Workflow window shows the L2VPN (Metro Ethernet) Discovery process as **Pending Input**.

- Step 2** Click **Continue**.

The L2VPN Discovery (Ethernet Services) window appears, as shown in [Figure 4-44](#).

Figure 4-44 L2VPN Discovery (Ethernet Services) Window

Step 3 Select one of the following actions:

- **View/Edit Discovered Layer 2 Services grouped by VPN**—Allows you to view the discovered L2VPN services and edit them as required.
- **View/Edit Discovered Layer 2 End to End Wires**—Allows you to view the discovered Layer 2 End to End wires and edit them as required.
- **View/Edit Discovered Layer 2 VPLS Links**—Allows you to view the discovered Layer 2 Virtual Private LAN Service (VPLS) links and edit them as required.

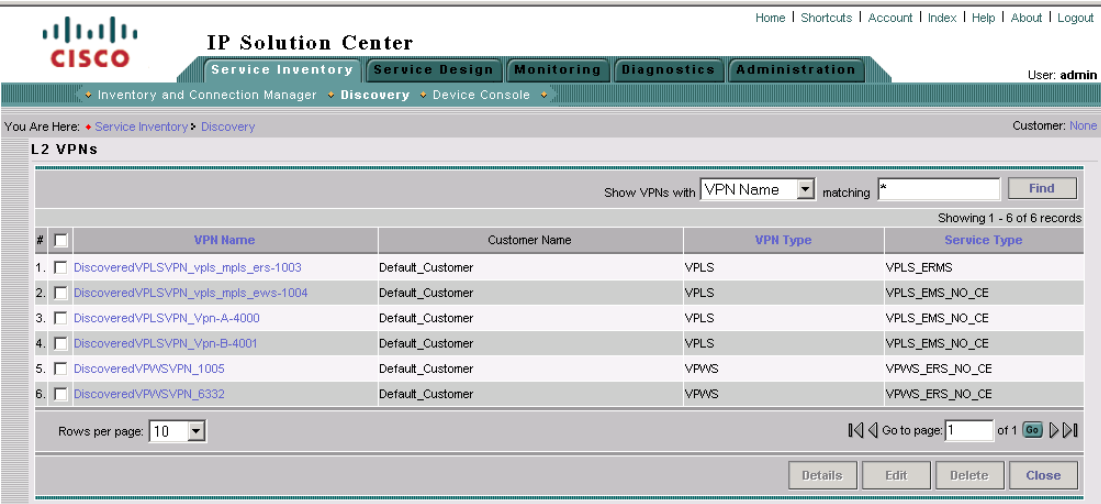
The following sections of this chapter describe each of these actions.

Viewing Discovered Layer 2 Services Grouped by VPN

Follow these steps to view discovered Layer 2 services grouped by VPN:

- Step 1** In the L2VPN Discovery (Ethernet Services) window, click the **VPNs** button. The L2VPNs window appears, as shown in [Figure 4-45](#).

Figure 4-45 L2VPNs Window



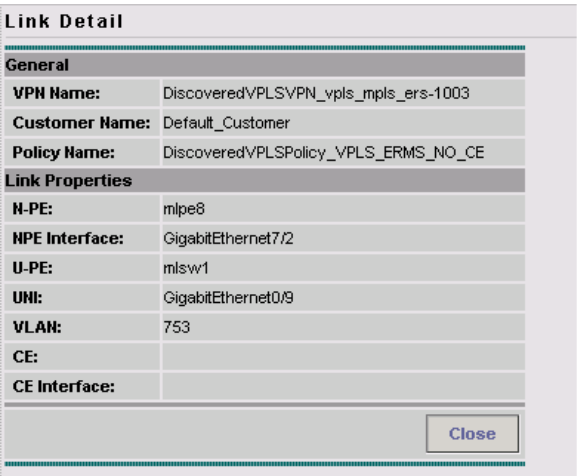
The L2VPNs window allows you to perform the following tasks:

- View detailed information about a Layer 2 VPN.
This task is explained in the following steps of this procedure.
- Display a window that allows you to edit the configuration information for an existing Layer 2 VPN.
See [Editing Discovered Layer 2 Services Grouped by VPN](#), page 4-69 for detailed instructions.
- Delete an existing Layer 2 VPN.
See [Deleting Discovered Layer 2 Services Grouped by VPN](#), page 4-70 for instructions on this task.

Step 2 To view detailed information about a Layer 2 service, check the check box next to a VPN that has details you want to view, and then click the **Details** button.

The Link Details window appears, as shown in [Figure 4-46](#).

Figure 4-46 Link Details Window



The Link Details window shows the details about the discovered VPN, such as the User-Network Interface (UNI), in a table format.

Step 3 When you are finished viewing the link details, click the **Close** button.

Editing Discovered Layer 2 Services Grouped by VPN

You can edit a discovered Layer 2 VPN service to change the policy that is applied to the service. Follow these steps to edit a Layer 2 VPN service:

Step 1 In the L2VPNs window, check the check box next to a VPN that you want to edit, and then click the **Edit** button.

The Edit Link Policy window appears, as shown in [Figure 4-47](#).

Figure 4-47 Edit Link Policy Window

IP Solution Center

Service Inventory | Service Design | Monitoring | Diagnostics | Administration

You Are Here: Service Inventory > Discovery

Edit Link Policy

Policy Name:

Selected Links:

Showing 1 - 1 of 1 record

#	UNI	U-PE	N-PE	Policy Name
1.	GigabitEthernet0/9	mls-w1	m1pe8	DiscoveredVPLSPolicy_VPLS_ERMS_NO_CE

Rows per page: 10

Note: * - Required Field

Step 2 To change the link policy for the service, follow these steps:

- a. Click the **Policy** button next to the Policy Name field.

A list of policies appears.

You can change the list of policies by choosing a filter from the pull-down list in the **Show VPN policies with** field and/or entering a search mask in the **Matching** field.

You can filter the policy list by Policy Name, Customer Name, Provider Name, or Global policy name. And you can limit the lists of policies displayed in the selected category by entering a value in the Matching field.

Step 3 Click the radio button next to a policy that you want to apply to the service and then click **Select**.

Step 4 Do one of the following:

- Click **Save** to save your changes.
- Click **Cancel** to cancel the changes.

Deleting Discovered Layer 2 Services Grouped by VPN

Follow these steps to delete a Layer 2 service:

- Step 1

In the L2VPNs window, check the check box next to a VPN that you want to delete, and then click the **Delete** button.

The following message appears:

Links/End to End wires associated with all selected VPNs will be deleted as a result of this operation. Do you really want to Delete?
- Step 2

If you are sure that you want to delete the VPN, click **OK**; otherwise, click **Cancel**.

If you click **OK**, the VPN and associated links and end-to-end wires are deleted.

Viewing Discovered Layer 2 End to End Wires

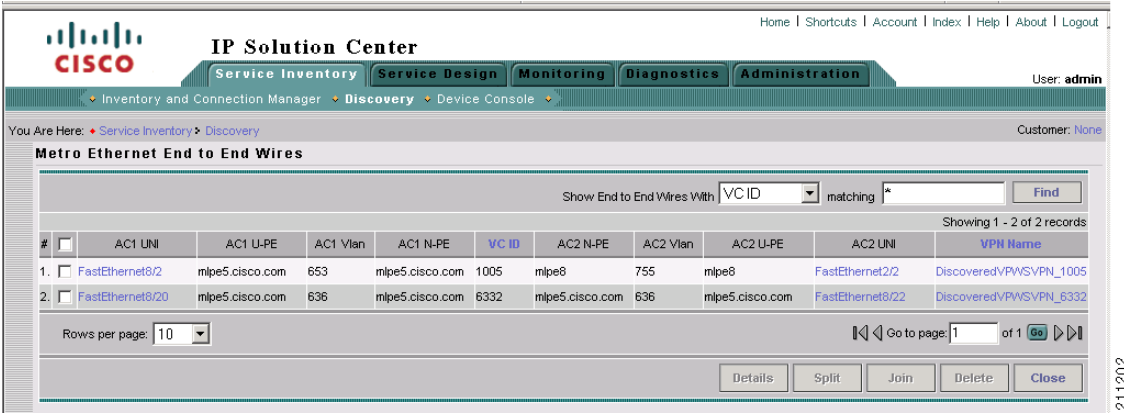
Follow these steps to view discovered Layer 2 end-to-end wires:

- Step 1

In the L2VPN Discovery (Ethernet Services) window, click the **End-End Wires** button.

The Metro Ethernet End to End Wires window appears, as shown in [Figure 4-48](#).

Figure 4-48 Metro Ethernet End to End Wires Window



- The Metro Ethernet End to End Wires window allows you to perform the following tasks:
- View detailed information about a Metro Ethernet end-to-end wire.

This task is explained in the following steps of this procedure.
 - Edit the VPN associated with the end-to-end wire.

See [Editing the VPN Associated with an End to End Wire](#), page 4-72 for a description of this task.
 - Split an existing end-to-end wire into two end-to-end wires

See [Splitting Layer 2 Service End to End Wires](#), page 4-73 for a description of this task.

- Join existing end-to-end wires into a single end-to-end wire
See [Joining Layer 2 Service End to End Wires](#), page 4-74 for a description of this task.
- Delete an existing end-to-end wire.
See [Deleting Discovered Layer 2 Services Grouped by VPN](#), page 4-70 for instructions on this task.

Step 2 To view detailed information about a Layer 2 service, check the check box next to a VPN that has details you want to view, and then click the **Details** button.

The Link Details window appears, as shown in [Figure 4-49](#).

Figure 4-49 Link Details Window

The screenshot shows a window titled "Link Detail" with a "Close" button at the bottom right. The window is divided into two sections: "General" and "Link Properties".

General	
VPN Name:	DiscoveredVPLSVPN_vpls_mpls_ers-1003
Customer Name:	Default_Customer
Policy Name:	DiscoveredVPLSPolicy_VPLS_ERMS_NO_CE
Link Properties	
N-PE:	mlpe8
NPE Interface:	GigabitEthernet7/2
U-PE:	mlsw1
UNI:	GigabitEthernet0/9
VLAN:	753
CE:	
CE Interface:	

149091

Step 3 When you are finished viewing the link details, click the **Close** button.

Step 4 If you want to view the details of the interfaces in the end-to-end wire, click the interface name in either the AC1 UNI or AC2 UNI field.

If you click on an interface name, the Interface Detail window appears, as shown in [Figure 4-50](#).

Figure 4-50 Interface Detail Window

Interface Detail

General

VPN Name:

DiscoveredVPWSVPN_1005

Provider Name:

Customer Name:

Device Information

Device Host Name:

mlpe5

Device Domain Name:

cisco.com

Interface Detail

Interface Name:

FastEthernet8/2

Interface Description:

Is Subinterface ?:

false

Maximum Allowed MAC Address:

Encapsulation:

DOT1Q

Interface Type:

FastEthernet

Switch Mode:

TRUNK

MAC Access Group:

Speed:

UNKNOWN

Duplex:

UNKNOWN

Close

149086

The Interface Detail window shows details about the selected interface, such as the hostname of the host where the interface is located, the type of encapsulation used on the interface, and the switch mode used on the interface.

Step 5 When you are finished viewing the interface details, click the **Close** button.

Editing the VPN Associated with an End to End Wire

From the Metro Ethernet End to End Wires window, you can also edit the VPN that is associated with the end-to-end wire.

Follow these steps to edit the VPN associated with an end-to-end wire:

Step 1 In the Metro Ethernet End to End Wires window, click a VPN name shown in the VPN name field. The Edit VPN window appears, as shown in [Figure 4-51](#).

Figure 4-51 *Edit VPN Window for L2VPN VPNs*

Step 2 To edit the VPN name, enter a new VPN name in the VPN Name field.

Step 3 To edit the Customer Name, follow these steps:

- a. Click the **Select** button next to the Customer Name.
A list of customers appears.
- b. Click the radio button next to the new Customer Name that you want to configure.
- c. Click the **Save** button.

The new VPN name and/or Customer Name appears in the Metro Ethernet End to End Wires window.

Splitting Layer 2 Service End to End Wires

You can split off an existing end-to-end wire from the VPN that it is associated with and associate it with a new VPN.

Follow these steps to split an end-to-end wire from an existing VPN:

Step 1 In the Metro Ethernet End to End Wires window, check the check box next to an end-to-end wire entry that you want to split from a VPN.



Note If there is only one ID for the VPN associated with the end-to-end wire, then you cannot perform a split action on the wire.

Step 2 Click the **Split** button.

A message appears asking if you want to proceed.

Step 3 If you want to continue with the process, click **OK**.

The end-to-end wires are split and are associated with two new VPNs. These names of the VPNs are created by the system by adding a new number to the end of the existing VPN name.

Joining Layer 2 Service End to End Wires

You can join two existing end-to-end wires to a single VPN.

Follow these steps to join two existing end-to-end wires:

-
- Step 1** In the Metro Ethernet End to End Wires window, check the check box next to several end-to-end wire entries that you want to join.
- A message appears asking if you want to proceed.
- Step 2** If you want to continue with the process, click **OK**.
- The selected end-to-end wires are joined to a new VPN. The name for this VPN is created by the system by adding a new number to the end of the existing highest numbered VPN name.
-

Deleting Layer 2 Service End to End Wires

Follow these steps to delete an existing end-to-end wire:

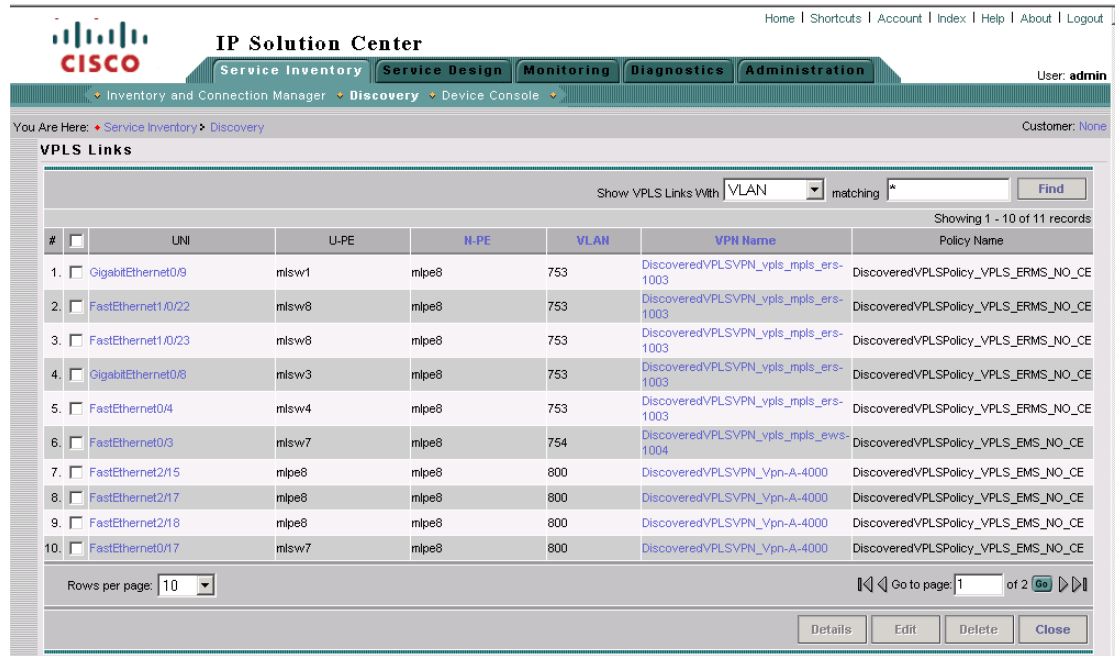
-
- Step 1** In the Metro Ethernet End to End Wires window, check the check box next to one or more end-to-end wires that you want to delete.
- A message appears asking if you want to proceed.
- Step 2** If you want to continue with the process, click **OK**.
- The selected end-to-end wire (or wires) is deleted. Any Attachment Circuit(s) associated with the wire(s) are also deleted.
- Step 3** Click **Close** to close the Metro Ethernet End to End Wires window.
-

Viewing Discovered Layer 2 VPLS Links

Follow these steps to view discovered Layer 2 VPLS links:

-
- Step 1** In the L2VPN Discovery (Ethernet Services) window, click the **VPLS Links** button.
- The VPLS Links window appears, as shown in [Figure 4-52](#).

Figure 4-52 VPLS Links Window



The VPLS Links window allows you to perform the following tasks:

- View detailed information about a VPLS link.
This task is explained in the following steps of this procedure.
- Display a window that allows you to edit the configuration information for an existing VPLS link.
See [Editing Discovered Layer 2 VPLS Links](#), page 4-76 for detailed instructions.
- Delete an existing Layer 2 VPN.
See [Deleting Discovered Layer 2 VPLS Links](#), page 4-77 for instructions on this task.

Step 2 To view detailed information about a VPLS link, check the check box next to a VPLS link that has details you want to view, and then click the **Details** button.

The Link Detail window appears, as shown in [Figure 4-53](#).

Figure 4-53 Link Detail Window

Link Detail

General

VPN Name:

DiscoveredVPLSVPN_vpls_mpls_ers-1003

Customer Name:

Default_Customer

Policy Name:

DiscoveredVPLSPolicy_VPLS_ERMS_NO_CE

Link Properties

N-PE:

mlpe8

NPE Interface:

GigabitEthernet7/2

U-PE:

mlsw1

UNI:

GigabitEthernet0/9

VLAN:

753

CE:

CE Interface:

Close

149091

The Link Detail window shows the details about the discovered VPN, such as the User-Network Interface (UNI), in a table format.

Step 3 When you are finished viewing the link details, click the **Close** button.

Editing Discovered Layer 2 VPLS Links

You can edit a discovered Layer 2 VPLS link to change the policy that is applied to the service. Follow these steps to edit a Layer 2 VPLS link:

Step 1 In the VPLS Links window, check the check box next to a VPLS link that you want to edit and then click the **Edit** button.

The Edit Link Policy window appears, as shown in [Figure 4-54](#).

Figure 4-54 Edit Link Policy Window

IP Solution Center

Service Inventory | Service Design | Monitoring | Diagnostics | Administration

Inventory and Connection Manager | **Discovery** | Device Console

You Are Here: Service Inventory > Discovery

Edit Link Policy

Policy Name:

Selected Links:

#	UNI	U-PE	N-PE	Policy Name
1.	GigabitEthernet0/9	mls-w1	m1pe8	DiscoveredVPLSPolicy_VPLS_ERMS_NO_CE

Showing 1 - 1 of 1 record

Rows per page: 10

Note: * - Required Field

Step 2 To change the link policy for the link, follow these steps:

- a. Click the **Policy** button next to the Policy Name field.

A list of policies appears.

You can change the list of policies by choosing a filter from the pull-down list in the **Show VPN policies with** field and/or entering a search mask in the **Matching** field.

You can filter the policy list by Policy Name, Customer Name, Provider Name, or Global policy name. And you can limit the lists of policies displayed in the selected category by entering a value in the Matching field.

Step 3 Click the radio button next to a policy that you want to apply to the service, and then click **Select**.

Step 4 Do one of the following:

- Click **Save** to save your changes.
- Click **Cancel** to cancel the changes.

Deleting Discovered Layer 2 VPLS Links

Follow these steps to delete a VPLS link:

Step 1 In the VPLS Links window, check the check box next to a VPLS link that you want to delete and then click the **Delete** button.

The following message appears:

The selected link(s) will be deleted. Do you really want to Delete?

Step 2 If you are sure that you want to delete the VPLS, click **OK**; otherwise, click **Cancel**.

If you click **OK**, the VPLS link(s) are deleted.

Step 3 Click **Close** to close the VPLS links window.

Saving the L2VPN Metro Ethernet Policy and Initiating Service Creation

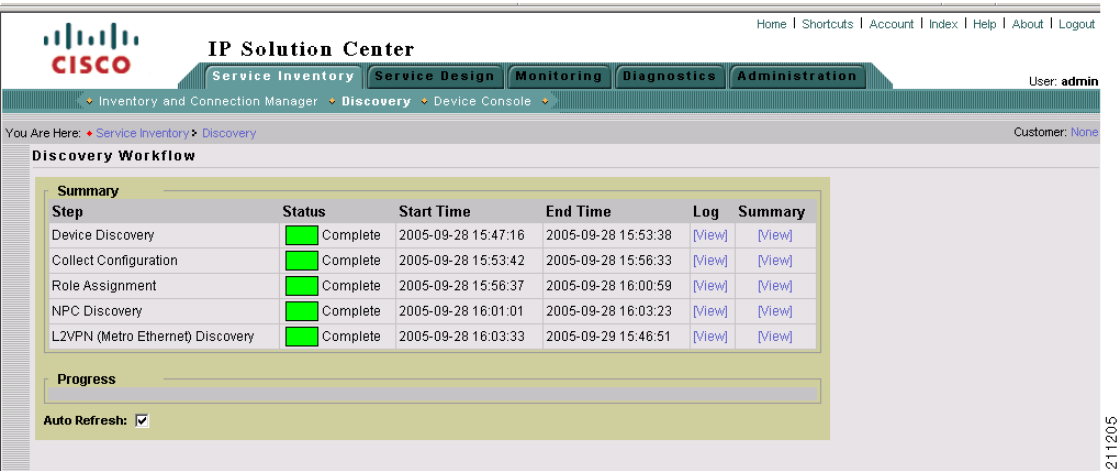
After you are finished viewing or editing the discovered L2VPN Metro Ethernet topology, click the **Close** button to return to the L2VPN Discovery (Ethernet Services) window.

Click the **Continue** button to initiate the L2VPN Service Discovery process.

The Discovery Workflow window appears and indicates that the **L2VPN Service Discovery process is In Progress**. The status indicator is yellow.

After the **L2VPN Service Discovery process is complete**, the status indicator changes to green, and the Discovery Workflow window indicates that the L2VPN Service Discovery process is **Complete**, as shown in [Figure 4-55](#).

Figure 4-55 Discovery Workflow Window with L2VPN Service Discovery Completed



Step 8: Commit Discovered Devices and Services to ISC Repository

Click the **Continue** button to commit the discovered devices and services to the ISC repository. Prior to this step, discovery workflow stores the discovered devices and services in a temporary repository, which gets committed to ISC only at the last step of discovery workflow.

Step 9: Create and Run a Collect Config Task for the Discovered Devices

Before you view and edit services, follow these steps to run a Create Config task for the devices:

**Note**

For additional information on the Create Config task, see the [“Create” section on page 7-3](#) for [Tasks](#).

-
- Step 1** On the ISC Start page, select **Monitoring**.
The Monitoring window appears.
- Step 2** Select **Task Manager**.
The Tasks window appears.
- Step 3** Click the **Create** button and choose **Collect Config** from the pull-down list.
The Create Task window appears.
- Step 4** Click the **Next** button.
The Collect Config Task window appears.
- Step 5** On the Collect Config task window, follow these steps to create and run a Collect Config task:
- Click the **Select/Deselect** button.
A dialog window appears, listing the devices that were discovered by the Discovery process.
 - Select all of the devices shown on the list.
 - Click the **Select** button.
The Collect Config Task window appears again.
 - Specify the additional settings for the Collect Config task as required.
 - Click the **Submit** button.

You are now ready to view and edit services as described in the following section, [Step 10: View and Edit Services](#), page 4-79

Step 10: View and Edit Services

After you have successfully completed the MPLS VPN and/or L2VPN Metro Ethernet service creation process, you can view the services that were created and modify them using the service requests editors. Follow these steps to view the L2VPN services:

-
- Step 1** If the Service Inventory window is not currently active, click the **Service Inventory** tab.
The Service Inventory window is now active.
- Step 2** In the Service Inventory window, click **Service Inventory**.
The Inventory and Connection Manager window appears, as shown in [Figure 4-56](#).

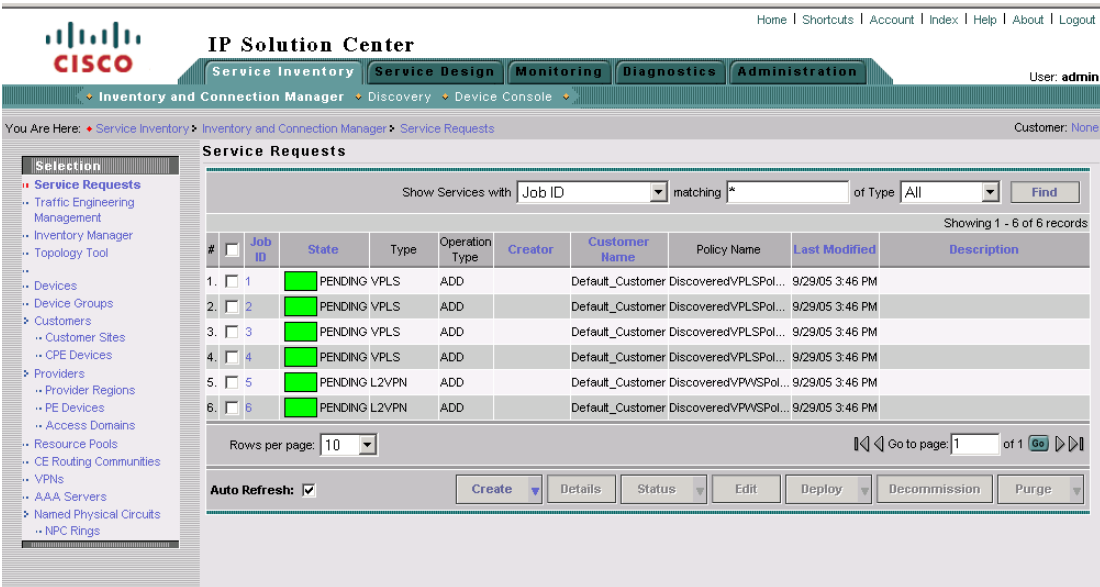
Figure 4-56 Inventory and Connection Manager Window



Step 3 Click **Service Requests**.

The Service Requests window appears, as shown in Figure 4-57.

Figure 4-57 Service Requests Window



You can modify the service requests shown in the Service Requests window as required.



Note

If you need to edit MPLS VPNs as part of this process, see the [Splitting a VPN](#), page 4-59, [Creating a VPN](#), page 4-62, [Viewing VPN Link Details](#), page 4-64, and [Saving the MPLS VPNs and Initiating MPLS VPN Service Creation](#), page 4-65.

Step 4 For detailed information on modifying Service Requests for L2VPN Metro Ethernet networks, see the [Cisco IP Solution Center Metro Ethernet and L2VPN User Guide, 5.0](#).

- Step 5** For general information on the release, see the [Release Notes for Cisco IP Solution Center, 5.0.1](#), provided with the release.
-



CHAPTER 5

Service Inventory—Device Console

From the Home window of Cisco IP Solution Center (ISC), which 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](#), “[Example of 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**, follow these steps:

- Step 1** Choose **Service Inventory > Device Console** and you receive a window as shown in the example in [Figure 5-2](#), “[Example of Device Console Selections](#).”



Note

The radio button last selected will be the one shown in [Figure 5-2](#).

Figure 5-2 Example of 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 apply only to Live mode, *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 section.
- [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 5-13](#) Remotely reloads devices.

Download Commands

To download commands, follow these steps:

- Step 1** Choose **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, check the check box for each device you want. Uncheck 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, check the check box for each group you want. Uncheck 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 unchecked, you do *not* upload the configuration file after the download.
- Step 8** If you leave the **Retrieve device attributes** check box unchecked, you do not retrieve any device attributes. If you check the **Retrieve device attributes** check box, after the template is downloaded, SNMP is used to retrieve interface information and issue additional **show** commands, such as **show version**.
- Step 9** 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 10** When you click **Download**, you return to [Step 6](#) to download additional commands on the selected devices.
- Step 11** When you click **Done**, you return to [Figure 5-2](#).

Download Template



Note

Multiple datafiles belonging to different templates cannot be downloaded through the device console.

To download a template, follow these steps:

- Step 1** Choose **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 8 to delete devices; or click **Next** to proceed to Step 10 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**,” check the check box(es) for each device you want to select. Then click **Select**.

Figure 5-5 Device Selection

Showing 1 - 8 of 8 records

#	☐	Device Name	Management IP Address	Type	Parent Device Name
1.	☐	pe1		Cisco IOS Device	
2.	☐	pe3		Cisco IOS Device	
3.	☐	sw2		Cisco IOS Device	
4.	☐	sw8		Cisco IOS Device	
5.	☐	sw4		Cisco IOS Device	
6.	☐	ce3		Cisco IOS Device	
7.	☐	ce8		Cisco IOS Device	
8.	☐	ce13		Cisco IOS Device	

Rows per page: 10 Go to page: 1 of 1 Go

Select Cancel

- Step 5** You return to [Figure 5-4](#) with the added devices.
- Step 6** 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 7** You can repeat [Step 3](#) to [Step 6](#) to **add** more devices, you can delete devices, as explained in [Step 8](#), or you can proceed by going to [Step 9](#).
- Step 8** To delete devices, check the check box(es) for the devices you want to delete and then click **Delete**. Select carefully, because there is no chance to confirm this deletion.
- Step 9** When you have all the devices you want, click **Next**. You proceed to **3. Select Device Groups**, starting in [Step 10](#).
- Step 10** 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. Enter Download Commands**.
- Step 11** Click **Add**, as shown in [Figure 5-6](#), to **3. Select Device Groups**. Adding Device Groups is optional.

Figure 5-6 Device Group Selection

Showing 0 of 0 records

#	☐	Device Group Name	Description

Rows per page: 10 Go to page: 1 of 1 Go

Add Delete

- Step 12** From the resulting window, as shown in [Figure 5-7](#), “Group Association,” check the check box(es) for each device group you want to select. Then click **Select**.

Figure 5-7 Group Association

#	Device Group Name	Description
1.	☐ Device-Group-1	
2.	☐ Device-Group-2	

Rows per page: 10 Go to page: 1 of 1 Go

Select Cancel

- Step 13** You return to [Figure 5-6](#) with the added device groups. You can repeat [Step 11](#) 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 15](#).
- Step 14** To delete device groups, check the check box(es) for the devices you want to delete 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. Select Download Template**, starting in [Step 16](#).
- Step 16** For **4. Select Download Template**, the resulting window is shown in [Figure 5-8](#), “Select Download Template.”

Figure 5-8 Select Download Template

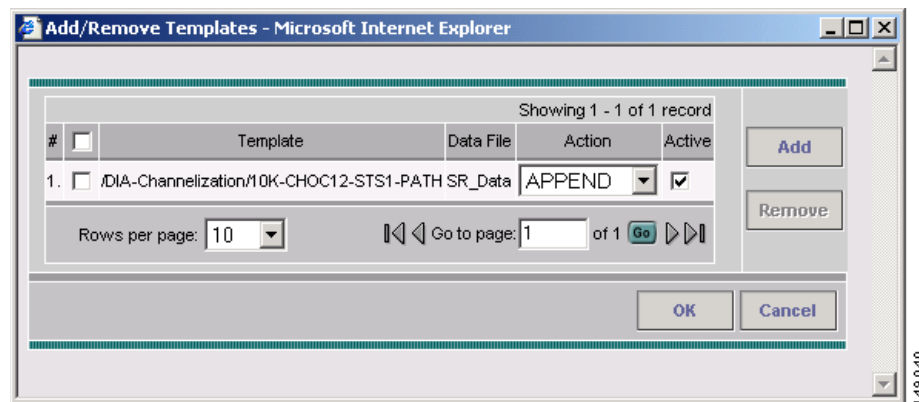
#	Template	Data File	Action

Rows per page: 10 Go to page: 1 of 1 Go

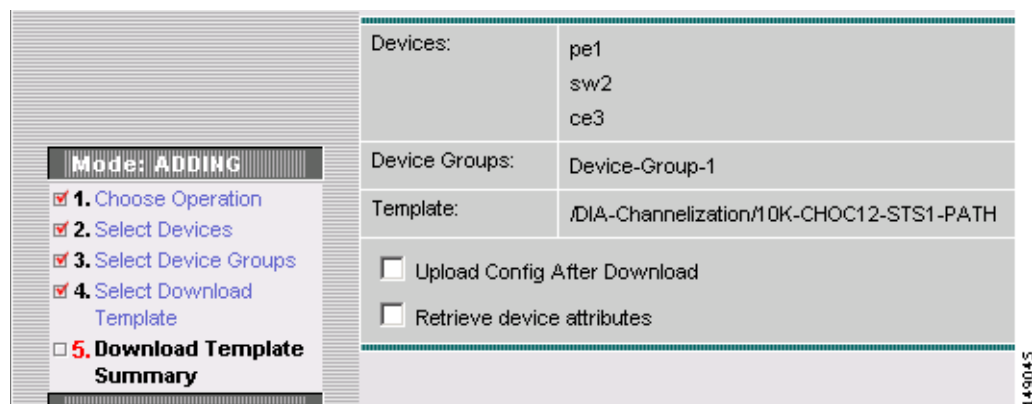
Select

- Step 17** In [Figure 5-8](#), you can click the **Select** button.
- Step 18** 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 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](#), check the check box(es) for the template(s) you want. In each template row, click the **Action** drop-down list and choose **APPEND** or **PREPEND** to add information after or before, respectively; check or uncheck the **Active** check box; and then click **OK**.

Figure 5-9 Add/Remove Templates

- Step 19** You return to [Figure 5-8](#) with the updated information.
- Step 20** Click **Next** and you proceed to **5. Download Template Summary**, as explained in [Step 21](#).
- Step 21** For **5. Download Commands Summary**, a window as shown in [Figure 5-10](#), “**Download Template Summary**,” appears.

Figure 5-10 Download Template Summary

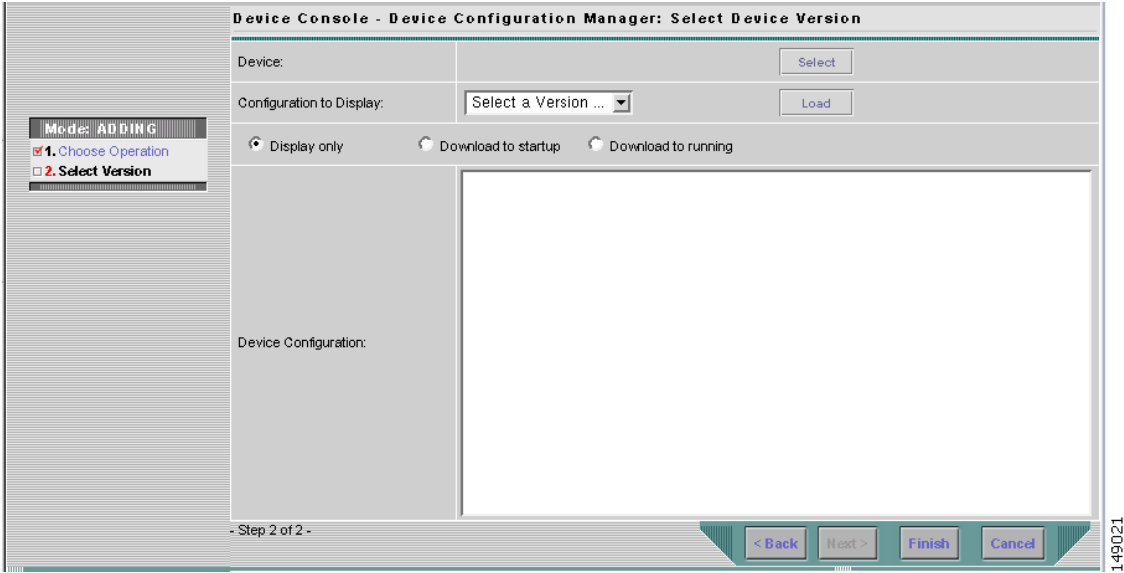
- Step 22** In [Figure 5-10](#), if you leave the **Upload Config After Download** check box unchecked, you do *not* upload the configuration file after the download. If you check the **Upload Config After Download** check box, you upload the new configuration file after you download the templates in [Step 18](#). If you leave the **Retrieve device attributes** check box unchecked, you do not retrieve any device attributes. If you check the **Retrieve device attributes** check box, after the template is downloaded, SNMP is used to retrieve interface information and issue additional **show** commands, such as **show version**.
- Step 23** 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 mark for **Succeeded**.
- Step 24** 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, follow these steps:

- Step 1** Choose **Service Inventory > Device Console > Device Configuration Manager** and from [Figure 5-2](#) click **Next**. A window as shown in [Figure 5-11](#), “**Device Configuration Manager**,” appears.

Figure 5-11 *Device Configuration Manager*



- Step 2** In the **Device** row, click **Select** and a window as shown in [Figure 5-12](#), “**Device Selection**,” appears.

Figure 5-12 Device Selection

Showing 1 - 8 of 8 records

#		Device Name	Management IP Address	Type	Parent Device Name
1.	☐	pe1		Cisco IOS Device	
2.	☐	pe3		Cisco IOS Device	
3.	☐	sw2		Cisco IOS Device	
4.	☐	sw8		Cisco IOS Device	
5.	☐	sw4		Cisco IOS Device	
6.	☐	ce3		Cisco IOS Device	
7.	☐	ce8		Cisco IOS Device	
8.	☐	ce13		Cisco IOS Device	

Rows per page: 10 Go to page: 1 of 1

Select Cancel

- 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 5-11](#) 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 list. 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**. Dynamic Component Properties Library (DCPL) properties for DCS for both FTP and TFTP are specified in [Appendix C, “Property Settings”](#).

- **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**, follow these steps:

- Step 1** Choose **Service Inventory > Device Console > EXEC Commands** and in [Figure 5-2](#) click **Next**. A window as shown in [Figure 5-13](#), “**Device Console—EXEC Commands: Select Devices**,” appears.

Figure 5-13 *Device Console—EXEC Commands: Select Devices*

Device Console - EXEC Commands: Select Devices

Show Devices with Device Name matching * Find

Showing 0 of 0 records

#	Device Name	Management IP Address	Type
Showing 0 of 0 records			

Rows per page: 10 Go to page: 1 of 1

Add Delete

- Step 2 of 5 -

< Back Next > Finish Cancel

- Step 2** Continue with [Step 3](#) if you want to add devices; proceed to [Step 6](#) to delete devices; or click **Next** to proceed to [Step 8](#) for **3. Select Device Groups**.
- Step 3** Click **Add**, as shown in [Figure 5-13](#), to **2. Select Devices**.
- Step 4** From the resulting window, as shown in [Figure 5-14](#), “**Device Selection**,” check the check box(es) for each device you want to select. Then click **Select**.

Figure 5-14 Device Selection

#	☐	Device Name	Management IP Address	Type	Parent Device Name
1.	☐	pe1		Cisco IOS Device	
2.	☐	pe3		Cisco IOS Device	
3.	☐	sw2		Cisco IOS Device	
4.	☐	sw8		Cisco IOS Device	
5.	☐	sw4		Cisco IOS Device	
6.	☐	ce3		Cisco IOS Device	
7.	☐	ce8		Cisco IOS Device	
8.	☐	ce13		Cisco IOS Device	

Rows per page: 10 Go to page: 1 of 1 **Go**

Select **Cancel**

- Step 5** You return to [Figure 5-13](#) with the added devices. You can repeat [Step 3](#) to [Step 4](#) to **add** more devices, you can delete devices, as explained in [Step 6](#), or you can proceed by going to [Step 7](#).
- Step 6** To delete devices, check the check box(es) for the devices you want to delete and then click **Delete** in [Figure 5-13](#). Select carefully, because there is no chance to confirm this deletion.
- Step 7** When you have all the devices you want, click **Next**. You proceed to **3. Select Device Groups**, starting in [Step 8](#).
- Step 8** Continue with [Step 9](#) if you want to add device groups; proceed to [Step 12](#) to delete device groups; or click **Next** to proceed to [Step 14](#) for **4. Enter EXEC Commands**.
- Step 9** Click **Add**, as shown in [Figure 5-15](#), to **3. Select Device Groups**.

Figure 5-15 Device Group Selection

Device Console - EXEC Commands: Select Device Groups

Mode: **ADDING**

- ☒ 1. Choose Operation
- ☒ 2. Select Devices
- ☒ **3. Select Device Groups**
- ☐ 4. Enter EXEC Command
- ☐ 5. EXEC Commands
- Summary

ShowDevice 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 10** From the resulting window, as shown in [Figure 5-16](#), “Group Association,” check the check box(es) for each device group you want to select. Then click **Select**.

Figure 5-16 Group Association

#	Device Group Name	Description
1.	☐ Device-Group-1	
2.	☐ Device-Group-2	

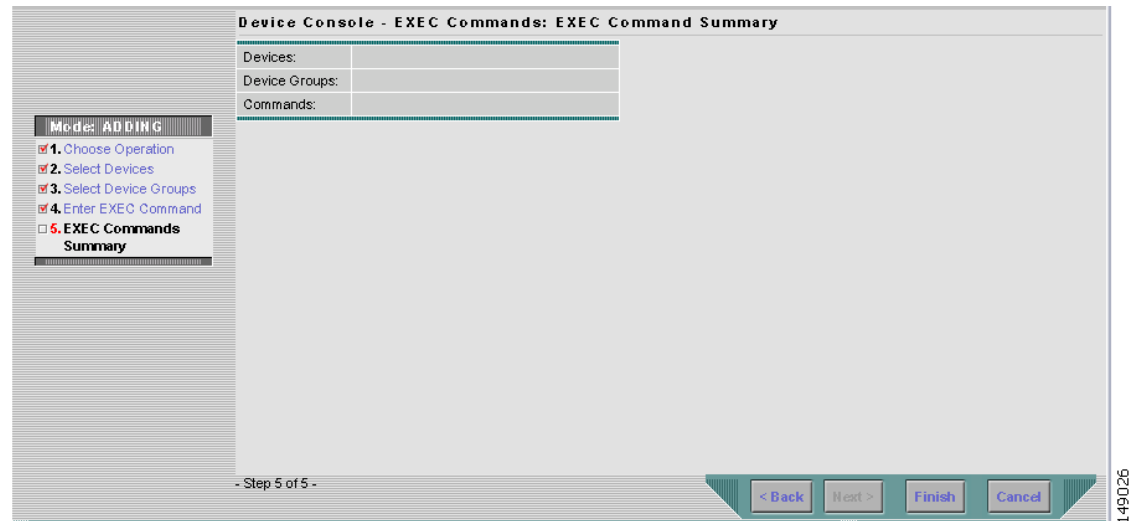
- Step 11** You return to [Figure 5-15](#) with the added device groups. You can repeat [Step 9](#) to [Step 10](#) to **add** more device groups, you can delete device groups, as explained in [Step 12](#), or you can proceed by going to [Step 13](#).
- Step 12** To delete device groups, check the check box(es) for the devices you want to delete and then click **Delete**. Select carefully, because there is no chance to confirm this deletion.
- Step 13** When you have all the device groups you want, click **Next**. You proceed to **4. Enter EXEC Commands**, starting in [Step 14](#).
- Step 14** For **4. Enter EXEC Commands**, the resulting window is shown in [Figure 5-17](#), “Operation Commands.”

Figure 5-17 Operation Commands

- Step 15** In [Figure 5-17](#), 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 16** Click **Next** and you proceed to **5. EXEC Commands Summary**, as explained in [Step 17](#).
- Step 17** For **5. EXEC Commands Summary**, a window as shown in [Figure 5-18](#), “EXEC Commands Summary,” appears.

Figure 5-18 EXEC Commands Summary



- Step 18** 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 mark for **Succeeded**. You can click **EXEC** or **Done**.
- Step 19** When you click **EXEC**, you return to [Step 14](#) to enter additional commands on the selected devices.
- Step 20** When you click **Done**, you return to [Figure 5-2 on page 5-2](#).

Reload

To reload (reboot) the router, follow these steps:

- Step 1** Choose **Service Inventory > Device Console > Reload** and from [Figure 5-2](#) click **Next**. A window as shown in [Figure 5-19](#), “Device Console—Reload: Select Devices,” appears.

Figure 5-19 Device Console—Reload: Select Devices

- Step 2** Continue with [Step 3](#) if you want to add devices; proceed to [Step 6](#) to delete devices; or click **Next** to proceed to [Step 8](#) for **3. Select Device Groups**.
- Step 3** Click **Add**, as shown in [Figure 5-19](#), to **2. Select Devices**.
- Step 4** From the resulting window, as shown in [Figure 5-20](#), “**Device Selection**,” check the check box(es) for each device you want to select. Then click **Select**.

Figure 5-20 Device Selection

#		Device Name	Management IP Address	Type	Parent Device Name
1.	☒	pe1		Cisco IOS Device	
2.	☒	pe3		Cisco IOS Device	
3.	☐	sw2		Cisco IOS Device	
4.	☐	sw3		Cisco IOS Device	
5.	☐	sw4		Cisco IOS Device	
6.	☐	ce3		Cisco IOS Device	
7.	☐	ce8		Cisco IOS Device	
8.	☐	ce13		Cisco IOS Device	

- Step 5** You return to [Figure 5-19](#) with the added devices. Repeat [Step 3](#) to [Step 4](#) to **add** more devices; delete devices, as explained in [Step 6](#); or proceed by going to [Step 7](#).
- Step 6** To delete devices, check the check box(es) for the devices you want to delete and then click **Delete**. Select carefully, because there is no chance to confirm this deletion.

- Step 7** When you have all the devices you want, click **Next**. You proceed to **3. Select Device Groups**, starting in [Step 8](#).
- Step 8** Continue with [Step 9](#) if you want to add device groups; proceed to [Step 12](#) to delete device groups; or click **Next** to proceed to [Step 14](#) for **4. Reload Devices Summary**.
- Step 9** Click **Add**, as shown in [Figure 5-21](#), to **3. Select Device Groups**.

Figure 5-21 Device Group Selection

- Step 10** From the resulting window, as shown in [Figure 5-22](#), “**Group Association**,” check the check box(es) for each device group you want to select. Then click **Select**.

Figure 5-22 Group Association

- Step 11** You return to [Figure 5-21](#) with the added device groups. Repeat [Step 9](#) to [Step 10](#) to **add** more device groups; delete device groups, as explained in [Step 12](#); or proceed by going to [Step 14](#).
- Step 12** To delete device groups, check the check box(es) for the devices you want to delete in [Figure 5-21](#) and then click **Delete**. Select carefully, because there is no chance to confirm this deletion.
- Step 13** When you have all the device groups you want, click **Next**. You proceed to **4. Reload Devices Summary**, starting in [Step 14](#).

Step 14 For **4. Reload Devices Summary**, a window as shown in [Figure 5-23](#), “Reload Summary,” appears.

Figure 5-23 *Reload Summary*

Device Console - Reload: Reload Devices Summary

Devices:	
Device Groups:	

Mode: ADDING

- ☒ 1. Choose Operation
- ☒ 2. Select Devices
- ☒ 3. Select Device Groups
- ☐ 4. Reload Devices Summary

- Step 4 of 4 -

< Back Next > Finish Cancel

149029

Step 15 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 mark for **Succeeded**.

Step 16 Click **Finish** and you return to [Figure 5-2 on page 5-2](#).



CHAPTER 6

Service Design

From the Home window of Cisco IP Solution Center (ISC), which 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 choose the following selections:

- [Policies, page 6-1](#) Create and manage Policies for licensed services.
- [Templates, page 6-2](#) Create and manage Templates and associated data.

Policies

Policies is explained in each of the *User Guides* for each of the applicable licensed services.

Templates

Templates supports the browsing, creation, and deletion of Template Folders, Templates, and Data Files and it supports 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. Another method is to use the Device Console feature to download templates independent of Service Requests, as explained in the [“Download Template” section on page 5-3](#).

ISC provides a way to integrate a template with ISC configlets.

For a given customer edge router and/or provider 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).

Template commands are treated independently from those associated with a service creation (Multi Protocol Label Switching (MPLS), Layer 2 Virtual Private Network (L2VPN), Virtual Private LAN Service (VPLS), Traffic Engineering (TE), and so on). Consequently, template commands must be removed separately from the device(s) during a service decommission. To remove prior template commands, a separate template is needed during a decommission process. Decommissioning a service request does not automatically remove the original template commands. A separate negate template needs to be added to the decommission process and the original templates must be removed. The negate template must contain the necessary NO commands to successfully remove any unwanted IOS commands added by the original template.



Note

For additional information about template usage, see the [Appendix D, “Template Usage”](#).

To use Templates, follow these steps:

-
- Step 1** Choose **Service Design > Templates** and you receive a window as shown in [Figure 6-2, “Templates.”](#)

Figure 6-2 **Templates**

The screenshot shows a web interface for managing templates. At the top, there is a 'Folder:' label. Below it is a search bar with the text 'Show Templates' followed by a dropdown menu set to 'Name', the word 'matching', and an empty text input field. A 'Show' button is to the right. Below the search bar, it says 'Showing 0-0 of 0 records'. There is a table with two columns: 'Template Name' and 'Description'. The table is currently empty, with the text 'No records.' below it. At the bottom, there are pagination controls: 'Rows per page: 10' with a dropdown, 'Go to page: 1 of 1 Pages' with a 'Go' button, and navigation arrows. At the very bottom, there are four buttons: 'Create Template', 'Create Data File', 'Edit', and 'Delete'.

Template examples are shown in the left column. A complete list of template examples is specified in the [Template Examples, page 6-22](#). A complete list of Repository variables is shown in the “[Summary of Repository Variables](#)” section on [page 6-23](#). An explanation of a tool for importing and exporting templates into and from an ISC database is given in the “[Importing and Exporting Templates](#)” section on [page 6-36](#).

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 6-13](#)
- [Edit, page 6-18](#)
- [Delete, page 6-20](#)

View Templates Tree and Data Pane

When you choose **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 check 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 Templates matching** or **Show Data Files matching** filter in the upper right-hand corner of the data pane can be very useful. For example, you can click the drop-down list for **Show Templates** or **Show Data Files** and choose to match (matches are case-sensitive) the **Name** or **Description** and then in the **matching** box you can choose to work with templates or data files, respectively, that start with **abc**. In this case, enter **abc*** in the field and then click the **Show** button. Only the templates or data files, respectively, that start with **abc** appear. For more information about filters, see [Filters, page 1-7](#).

**Note**

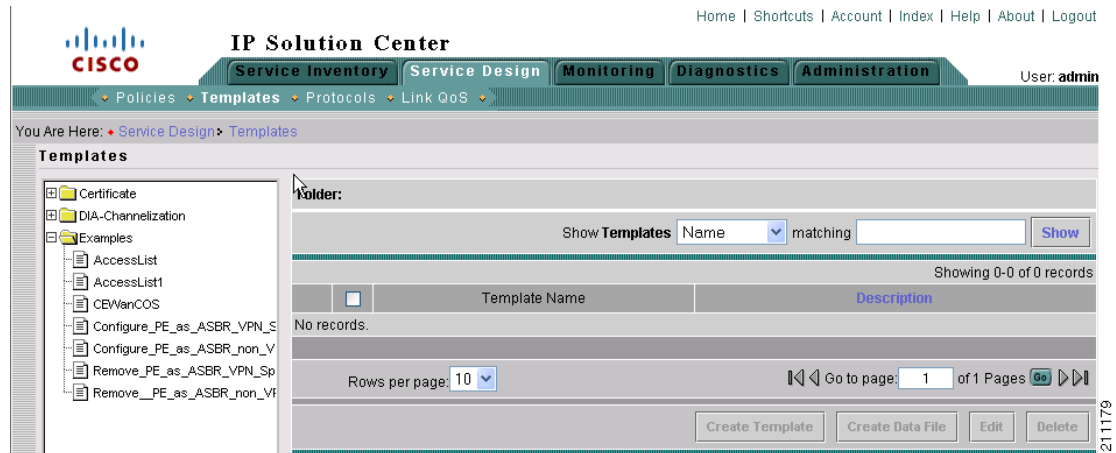
The template search facility applies to the folder currently selected and not across all folders.

**Note**

The data file search applies to the template currently selected and not across all folders and templates.

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, follow these steps:

- Step 1** Choose **Service Design > Templates**.
- Step 2** In the **Templates** tree, right-click in the white area and choose **New > Folder** to create a new folder or right-click on an existing folder or subfolder and choose **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.

Copying Folders or Subfolders

To copy a folder or subfolder and paste it into another folder or subfolder, follow these steps:

- Step 1** Select a folder or subfolder and then right-click and you receive the opportunity to copy. Click **Copy**.
- Step 2** Right-click on the folder or subfolder into which you want to paste the copied folder or subfolder and all its content and click **Paste**.

- Step 3** You will see the new folder or subfolder and all its content in the selected location. You can edit 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, follow these steps:

- Step 1** Choose **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 6-4, “Folder with Existing Templates.”](#)

Figure 6-4 Folder with Existing Templates

Folder: Examples

Show Templates Name matching Show

Showing 1-7 of 7 records

	☐	Template Name	Description
1.	☐	AccessList	adescription
2.	☐	AccessList1	cdescription
3.	☐	CEWanCOS	bdescription
4.	☐	Configure_PE_as_ASBR_VPN_Specific_Template_TMPL_	
5.	☐	Configure_PE_as_ASBR_non_VPN_Specific_Template_TMPL_	
6.	☐	Remove_PE_as_ASBR_VPN_Specific_Template_TMPL_	
7.	☐	Remove__PE_as_ASBR_non_VPN_Specific_Template_TMPL_	

Rows per page: 10 Go to page: 1 of 1 Pages Go

Create Template Create Data File Edit Delete

- Step 4** You can use the **Show Templates** drop-down list to choose whether to view the templates alphabetically by **Name** or by **Description**. Then click the **Show** button to activate how you view the templates. If you enter characters in the **matching** field before you click the **Show** button, you minimize the list of templates that appear either by **Name** or by **Description**. For more details, see [View Templates Tree and Data Pane, page 6-3](#).
- Step 5** Click the **Create Template** button and you receive a window as shown in [Figure 6-5, “Template Editor.”](#)

Figure 6-5 *Template Editor*

Template Editor

Template Editor

Template Name : *

Description:

Body : *

* Required Fields ☐ Has User Section

Select & Click Go Go Save Close

129057

Step 6 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 (VTL) directives, and variables that you want included.

**Note**

The VTL is explained at <http://velocity.apache.org>. For more specific information, you might like to navigate to <http://velocity.apache.org/engine/devel/user-guide.html> or <http://velocity.apache.org/engine/devel/vtl-reference-guide.html>.

**Note**

For additional information about template usage, see the [Appendix D, “Template Usage”](#).

An example template is shown in [Figure 6-6, “Example Template.”](#)

Figure 6-6 Example Template

Template Editor

Template Name: /Examples/CEWanCOS

Description:

Body:

```
## This template demonstrate if-else statements, repeat statements,
## mathematic
## 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")
```

* Required Fields ☐ Has User Section

Select & Click Go Go Save Close

Step 7 Click the **Select & Click Go** drop-down list. If you want to validate the information you entered in [Step 6](#), 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 6-7, Template Variables](#)”.

Figure 6-7 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.	CESubInterface	String	

Rows per page: 10 Go to page: 1 of 4 Pages Edit OK

Step 8 Click the radio button for the Variable you want to edit and click **Edit**. You receive a window as shown in [Figure 6-8, “Variable Definition—Type String.”](#)

Figure 6-8 Variable Definition—Type String

The screenshot shows a 'Variable Definition' dialog box for a variable named 'bestEffort-pct'. The 'Type' is set to 'String'. The 'Required' checkbox is checked. The 'Dimension' is set to '0'. There are input fields for 'Description', 'Pattern', 'Minimum Length', 'Maximum Length', and 'Default Value'. The 'Available Values (comma separated)' radio button is selected. At the bottom right are 'OK' and 'Cancel' buttons. A status bar at the bottom left says 'Required Fields'.

Step 9 In [Figure 6-8](#), click the drop-down list for **Type** to receive the following choices:

- **String** Proceed to [Step 10](#).
- **Integer** Proceed to [Step 11](#).
- **Float** Proceed to [Step 12](#).
- **IPv4 Address** Proceed to [Step 13](#).
- **Sub-Template** Proceed to [Step 14](#).

Step 10 The default Type to appear is **String**, a combination of ASCII characters considered as a group. The resulting Variable window is shown in [Figure 6-8](#) and its attributes are as follows:

- **Description** (optional) You can enter any descriptive statement about this variable here.
- **Required** Leave the default of the checked check box if this variable is required. Otherwise, uncheck 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.
- **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.
- **Radio Button: Default** (optional) If there is a default value for the specified variable, specify it here.
- **Radio Button: 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 6-7](#), 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 6-5](#). Create a Data File is shown in the “[Create Data File](#)” section on page 6-13, **Edit** is shown in the “[Edit](#)” section on page 6-18, and **Delete** is shown in the “[Delete](#)” section on page 6-20.

Step 11 When you choose the Type **Integer**, a whole number, 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 checked check box if this variable is required. Otherwise, uncheck 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.
- **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.
- **Radio Button: Default** (optional) If there is a default value for the specified variable, specify it here.
- **Radio Button: 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 6-7](#), 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 6-5](#). Create a Data File is shown in the “[Create Data File](#)” section on page 6-13, **Edit** is shown in the “[Edit](#)” section on page 6-18, and **Delete** is shown in the “[Delete](#)” section on page 6-20.

Figure 6-9 Variable Definition — Type Integer

The screenshot shows a dialog box titled "Variable bestEffort-pct". It contains the following fields and controls:

- Type:** A dropdown menu set to "Integer".
- Description:** An empty text box.
- Required:** A checked checkbox.
- Dimension:** A dropdown menu set to "0".
- Minimum Value:** An empty text box.
- Maximum Value:** An empty text box.
- Default Value:** A radio button that is selected.
- Available Values (comma separated):** A radio button that is unselected.
- Buttons:** "OK" and "Cancel" buttons at the bottom right.
- Footer:** A note that says "* Required Fields".

Step 12 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 6-10](#) and its attributes are as follows:

- **Description** (optional) You can enter any descriptive statement about this variable here.
- **Required** Leave the default of the checked check box if this variable is required. Otherwise, uncheck 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.
- **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.
- **Radio Button: Default** (optional) If there is a default value for the specified variable, specify it here.
- **Radio Button: 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 6-7](#), 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 6-5](#). Create a Data File is shown in the “[Create Data File](#)” section on page 6-13, **Edit** is shown in the “[Edit](#)” section on page 6-18, and **Delete** is shown in the “[Delete](#)” section on page 6-20.

Figure 6-10 Variable Definition—Type Float

The screenshot shows a window titled "Variable bestEffort-pct". It contains the following fields and controls:

- Type:** A dropdown menu set to "Float".
- Description:** An empty text box.
- Required:** A checked checkbox.
- Dimension:** A dropdown menu set to "0".
- Minimum Value:** An empty text box.
- Maximum Value:** An empty text box.
- Default Value:** A radio button that is selected.
- Available Values (comma separated):** An empty text box.
- Buttons:** "OK" and "Cancel" buttons at the bottom right.
- Footer:** A note that says "* Required Fields".

On the right side of the window, there is a vertical label "129060".

Step 13 When you choose the Type **IPv4 Address**, 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 checked check box if this variable is required. Otherwise, uncheck 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.
- **Subnet Mask** (optional) Enter a valid subnet mask.
- **Class** (optional) Enter the class of the IP address. The options are: **Undefined**, **A**, **B**, or **C**.
- **Radio Button: Default** (optional) If there is a default value for the specified variable, specify it here.
- **Radio Button: 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 6-7](#), 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 6-5](#). Create a Data File is shown in the “[Create Data File](#)” section on page 6-13, **Edit** is shown in the “[Edit](#)” section on page 6-18, and **Delete** is shown in the “[Delete](#)” section on page 6-20.

Figure 6-11 Variable Definition — Type IPv4

The screenshot shows a 'Variable Definition' dialog box for a variable named 'bestEffort-pct'. The 'Type' is set to 'IPv4 Address'. The 'Required' checkbox is checked. The 'Dimension' is set to '0'. The 'Class' is set to 'Undefined'. There are 'OK' and 'Cancel' buttons at the bottom right. A status bar at the bottom left indicates 'Required Fields'.

Step 14 When you choose the Type **Sub-Template**, you instantiate one subtemplate into the Main template. 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 checked check box if this variable is required. Otherwise, uncheck 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 6-7](#), 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 6-5](#). Create a Data File is shown in the “[Create Data File](#)” section on page 6-13, **Edit** is shown in the “[Edit](#)” section on page 6-18, and **Delete** is shown in the “[Delete](#)” section on page 6-20.

Figure 6-12 Variable Definition—Type Sub-Template

Copying Templates

To copy a template and paste it into another folder, follow these steps:

-
- Step 1** Select a template and then right-click and you receive the opportunity to copy. Click **Copy**.
 - Step 2** Right-click on the folder into which you want to paste the copied template and all its data files and click **Paste**.
 - Step 3** You will see the new template and all its data files in the selected location. You can edit 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, follow these steps:

-
- Step 1** Choose **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
 2. 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 6-13](#), [“Choose Existing Template > Create Data File.”](#)

Figure 6-13 Choose Existing Template > Create Data File

Folder: Examples

Show Templates Name matching

Showing 1-7 of 7 records

	☐	Template Name	Description
1.	☐	AccessList	adescription
2.	☐	AccessList1	cdescription
3.	☐	CEWanCOS	bdescription
4.	☐	Configure_PE_as_ASBR_VPN_Specific_Template_TMPL_	
5.	☐	Configure_PE_as_ASBR_non_VPN_Specific_Template_TMPL_	
6.	☐	Remove_PE_as_ASBR_VPN_Specific_Template_TMPL_	
7.	☐	Remove__PE_as_ASBR_non_VPN_Specific_Template_TMPL_	

Rows per page: 10

Check 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 6-14](#), “Choose Existing Template > Create Data File.”

Figure 6-14 Choose Existing Template > Create Data File

Template: AccessList1

Show Data Files Name matching

Showing 1-3 of 3 records

	☐	Data File Name	Configlet	Description	In Use
1.	☐	Protocol-IP	View	IP configuration	Yes
2.	☐	Protocol-TCP	View	TCP configuration	Yes
3.	☐	TCP-IP	View	Combines TCP and IP configuration	No

Rows per page: 10

Click **Create Data File** and proceed to [Step 5](#).

- Step 5** An example of a window that appears is shown in [Figure 6-15](#), “Template Data File Editor.”

Figure 6-15 **Template Data File Editor**

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.

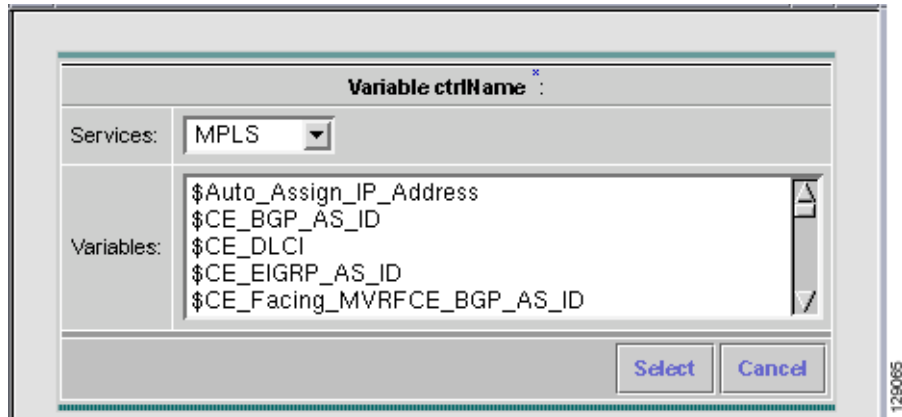
Step 7 In the example in [Figure 6-15](#), in the **Variables** area, **ctrlName** is a string variable (**Dimension** defined when the template was created was **0**); you can also create a one-dimensional array (**Dimension** defined when the template was created was **1**); and **t1-list** is a two-dimensional array (**Dimension** defined when the template was created was **2**).

If **t1-list** is a Dynamic Java Class variable, you *must* enter the entire Java Class package name. For example: com.cisco.isc.class_name.

**Note**

ctrlName can *only* be a string variable.

Step 8 If you click **Vars** as shown in [Figure 6-15](#), you receive a window as shown in [Figure 6-16](#), “[Template Data File Editor](#).”

Figure 6-16 Template Data File Editor

Click the **Services** drop-down list to have access to variables for:

- **MPLS**
- **L2VPN**
- **VPLS**

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 6-15](#), the resulting window depends on whether you are editing a **1** or **2** dimensional array.

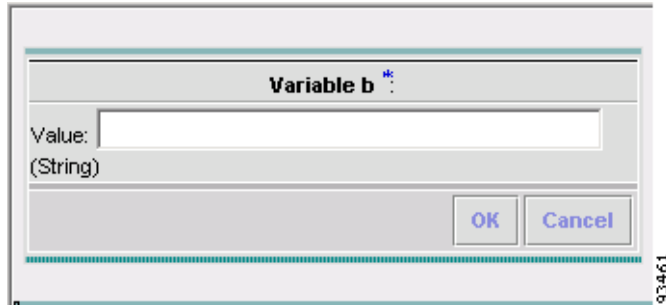
Proceed to [Step 10](#) for information about a **1** dimensional array.

Proceed to [Step 13](#) for information about a **2** dimensional array.

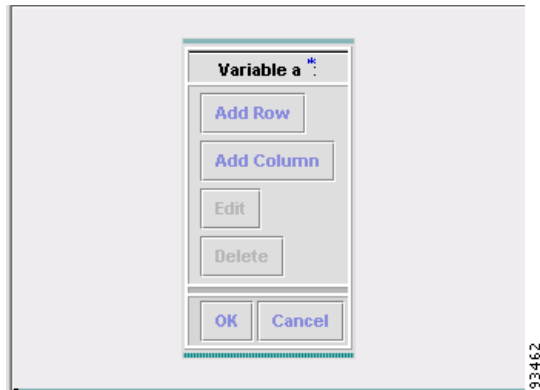
Step 10 For a one-dimensional array (set as **Dimension 1** when creating the template), when you click **Edit**, you receive a window as shown in [Figure 6-17](#), “Editing a One-Dimensional Array.”

Figure 6-17 Editing a One-Dimensional Array

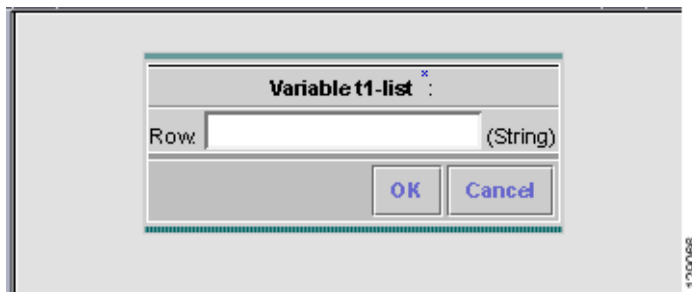
Step 11 To add a variable, click **Add** and a window, as shown in [Figure 6-18](#), “Adding a Variable,” appears in which you can add the variable. Then click **OK**.

Figure 6-18 Adding a Variable

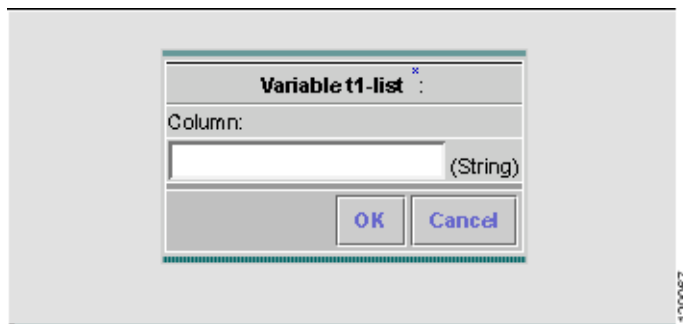
- Step 12** To edit or delete a variable, highlight the variable in [Figure 6-17](#) and click **Edit** or **Delete**. For **Edit** you receive a window as shown in [Figure 6-18](#). Then click **OK**. For **Delete**, *be sure* you want to delete. After you click **Delete**, it automatically occurs and 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 6-19](#), “[Editing a Two-Dimensional Array](#)”.

Figure 6-19 Editing a Two-Dimensional Array

- Step 14** Click **Add Row** in [Figure 6-19](#) and a window, as shown in [Figure 6-20](#), “[Enter Row Information](#),” appears. Enter a value and click **OK**.

Figure 6-20 Enter Row Information

- Step 15** Click **Add Column** in [Figure 6-19](#) and a window as shown in [Figure 6-21](#), “[Enter Column Information](#),” appears. Enter a value and click **OK**.

Figure 6-21 Enter Column Information

Step 16 A resulting window, as shown in [Figure 6-22](#), “Two-Dimensional Array Results,” appears.

Figure 6-22 Two-Dimensional Array Results

- Step 17** You can check 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 6-22](#).
- Step 19** A window as shown in [Figure 6-15](#) 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, follow these steps:

- Step 1** Choose **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 6-23, “Choose Existing Template > Edit.” To edit a data file, a window appears as shown in Figure 6-24, “Choose Existing Data File > Edit.”

Figure 6-23 Choose Existing Template > Edit

Folder: Examples

Show Templates Name matching Show

Showing 1-7 of 7 records

	☐	Template Name	Description
1.	☐	AccessList	adescription
2.	☐	AccessList1	cdescription
3.	☐	CEWanCOS	bdescription
4.	☐	Configure_PE_as_ASBR_VPN_Specific_Template_TMPL_	
5.	☐	Configure_PE_as_ASBR_non_VPN_Specific_Template_TMPL_	
6.	☐	Remove_PE_as_ASBR_VPN_Specific_Template_TMPL_	
7.	☐	Remove__PE_as_ASBR_non_VPN_Specific_Template_TMPL_	

Rows per page: 10 Go to page: 1 of 1 Pages Go

Create Template Create Data File Edit Delete

Figure 6-24 Choose Existing Data File > Edit

Template: AccessList1

Show Data Files Name matching Show

Showing 1-3 of 3 records

	☐	Data File Name	Configlet	Description	In Use
1.	☐	Protocol-IP	View	IP configuration	Yes
2.	☐	Protocol-TCP	View	TCP configuration	Yes
3.	☐	TCP-IP	View	Combines TCP and IP configuration	No

Rows per page: 10 Go to page: 1 of 1 Pages Go

List All SRs Create Template Create Data File Edit Delete

- Step 4** You can use the **Show Templates** or **Show Data Files** drop-down list to choose whether to view the templates or data files alphabetically by **Name** or by **Description**. Then click the **Show** button to activate how you view the templates or data files. If you enter characters in the **matching** field before you click the **Show** button, you minimize the list of templates or data files that appear either by **Name** or by **Description**. For more details, see the **Show Templates matching** or **Show Data Files matching** filter in the upper right-hand corner of the data pane can be very useful. For example, you can click the drop-down list for **Show Templates** or **Show Data Files** and choose to match (matches are case-sensitive) the **Name** or **Description** and then in the **matching** box you can choose to work with

templates or data files, respectively, that start with **abc**. In this case, enter **abc*** in the field and then click the **Show** button. Only the templates or data files, respectively, that start with **abc** appear. For more information about filters, see [View Templates Tree and Data Pane, page 6-3](#).

Step 5 Check 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 6 Click **Edit**.

Step 7 When editing a template, you receive a window as shown in [Figure 6-5, “Template Editor.”](#) Then proceed as in [Step 6](#) in the [Create Template](#) section. When editing a data file, you receive a window as shown in [Figure 6-14, “Choose Existing Template > Create Data File.”](#) Then proceed as in [Step 5](#) in the [Create Data File](#) section.

Delete

To delete a Template or Data File, follow these steps:

Step 1 Choose **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 6-25, “Choose Existing Template > Delete.”](#) To delete a data file, a window appears as shown in [Figure 6-26, “Choose Existing Data File > Delete.”](#)

Figure 6-25 Choose Existing Template > Delete

Folder: Examples

Show Templates matching

Showing 1-7 of 7 records

	☐	Template Name	Description
1.	☐	AccessList	adescription
2.	☐	AccessList1	cdescription
3.	☐	CEWanCOS	bdescription
4.	☐	Configure_PE_as_ASBR_VPN_Specific_Template_TMPL_	
5.	☐	Configure_PE_as_ASBR_non_VPN_Specific_Template_TMPL_	
6.	☐	Remove_PE_as_ASBR_VPN_Specific_Template_TMPL_	
7.	☐	Remove__PE_as_ASBR_non_VPN_Specific_Template_TMPL_	

Rows per page:

211180

Figure 6-26 Choose Existing Data File > Delete

	☐	Data File Name	Configlet	Description	In Use
1.	☐	Protocol-IP	View	IP configuration	Yes
2.	☐	Protocol-TCP	View	TCP configuration	Yes
3.	☐	TCP-IP	View	Combines TCP and IP configuration	No

Step 4 You can use the **Show Templates** or **Show Data Files** drop-down list to choose whether to view the templates or data files alphabetically by **Name** or by **Description**. Then click the **Show** button to activate how you view the templates or data files. If you enter characters in the **matching** field before you click the **Show** button, you minimize the list of templates or data files that appear either by **Name** or by **Description**. For more details, see the **Show Templates matching** or **Show Data Files matching** filter in the upper right-hand corner of the data pane can be very useful. For example, you can click the drop-down list for **Show Templates** or **Show Data Files** and choose to match (matches are case-sensitive) the **Name** or **Description** and then in the **matching** box you can choose to work with templates or data files, respectively, that start with **abc**. In this case, enter **abc*** in the field and then click the **Show** button. Only the templates or data files, respectively, that start with **abc** appear. For more information about filters, see [View Templates Tree and Data Pane, page 6-3](#).

Step 5 Check 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 6 Click the **Delete** button. A confirmation window appears prompting you to confirm the deletion. Before deleting a datafile, make sure it is not associated with a service request, by checking that the **In Use** column is set to **No**. When deleting a folder or a template, make sure that none of the datafiles they contain are associated with a service request. By clicking **OK**, you continue the deletion, and by clicking **Cancel**, you cancel the deletion.

Step 7 You receive an updated window as shown in [Figure 6-25, “Choose Existing Template > Delete”](#) or [Figure 6-26, “Choose Existing Data File > Delete”](#) with the deleted template or data file no longer available.

List All SRs

The **In Use** column, as shown in [Figure 6-26](#), **Yes** indicates that the data file is in use and **No** indicates that the data file is not in use. If **Yes** appears, you can click on it and you receive a list of all the associated service requests. If **Yes** appears, a **List All SRs** button is enabled in the bottom row. If you click the **List All SRs** button, all the service requests associated with the selected data file(s) appears, as shown in [Figure 6-27](#). If **No** appears in the **In Use** column, the **List All SRs** button is disabled.

From [Figure 6-27](#), if you click the **Close** button, the previous screen appears.

Figure 6-27 List All SRs

Service Requests										
Showing 1 - 4 of 4 records										
#	Data File Name	Job ID	State	Type	Operation Type	Creator	Customer Name	Policy Name	Last Modified	Description
1.	Protocol-IP,Protocol-TCP	1	☐	REQUESTED VRF	MODIFY	admin	PerfCustomer	None	1/15/08 4:08 PM	
2.	Protocol-IP,Protocol-TCP	4	☐	REQUESTED VPLS	MODIFY	admin	Customer1	vppls-policy	1/15/08 4:07 PM	
3.	Protocol-IP,Protocol-TCP	8	☐	REQUESTED MPLS	ADD	admin	Customer1	mpls-policy	1/15/08 4:38 PM	
4.	Protocol-IP,Protocol-TCP	11	☐	REQUESTED L2VPN	ADD	admin	Customer1	l2vpn	1/15/08 4:55 PM	
Rows per page: 10 v Go to page: 1 of 1 Go v										
Auto Refresh: ☒										Close

211162

**Note**

The only data files listed in the **Data File Name** column are those selected previously by the user to get to this window. The service request might be associated with other data files that are not displayed.

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
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.
	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.

Table 6-1 *Template Examples and Their Descriptions (continued)*

Folder	Template	Description
	AccessList1	Demonstrates the simplest template variable substitution.
	CEWanCOS	Demonstrates if-else statements, repeat statements, mathematical expressions, and one-dimensional variables.
QoS/L2/ATM	CLP_Egress	Sample template to demonstrate the setting of qos_group and ATM Cell Loss Priority at the output of an interface.
	CLP_Ingress	Sample template sets MPLS experimental bit of the ATM Cell marked with Cell Loss Priority, at the input of an interface.
QoS/L2/Ethernet	3400_Egress	
QoS/L2/FrameRelay	classification	Sample template to demonstrate the bandwidth reservation based on FrameRelay DLCI value.

Summary of Repository Variables

This section contains the following tables:

- [Table 6-2 on page 6-23, “L2VPN Repository Variables”](#)
- [Table 6-3 on page 6-26, “MPLS Repository Variables”](#)
- [Table 6-4 on page 6-34, “VPLS Repository Variables”](#)

[Table 6-2](#) provides a summary of the L2VPN Repository variables available from ISC Templates.

Table 6-2 *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

Table 6-2 L2VPN Repository Variables (continued)

Repository Variable	Dimension	Description
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)
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)

Table 6-2 L2VPN Repository Variables (continued)

Repository Variable	Dimension	Description
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
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

Table 6-2 L2VPN Repository Variables (continued)

Repository Variable	Dimension	Description
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 6-3 provides a summary of the MPLS Repository variables available from ISC Templates.

Table 6-3 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

Table 6-3 MPLS Repository Variables (continued)

Repository Variable	Dimension	Description
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
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 MVRFCE

Table 6-3 MPLS Repository Variables (continued)

Repository Variable	Dimension	Description
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
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

Table 6-3 MPLS Repository Variables (continued)

Repository Variable	Dimension	Description
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
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

Table 6-3 MPLS Repository Variables (continued)

Repository Variable	Dimension	Description
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 MVRFCE 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
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

Table 6-3 MPLS Repository Variables (continued)

Repository Variable	Dimension	Description
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
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 MVRFCE 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

Table 6-3 MPLS Repository Variables (continued)

Repository Variable	Dimension	Description
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
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

Table 6-3 MPLS Repository Variables (continued)

Repository Variable	Dimension	Description
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 MVRCE 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 MVRCE 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
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 6-4 provides a summary of the VPLS Repository variables available from ISC Templates.

Table 6-4 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
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

Table 6-4 VPLS Repository Variables (continued)

Repository Variables	Dimension	Description
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
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

Table 6-4 VPLS Repository Variables (continued)

Repository Variables	Dimension	Description
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

Importing and Exporting Templates

The **importExportTemplateDB** tool is available to import and export templates into and from an ISC database. You can import or export the complete or partial template database by specifying appropriate arguments. You can find this tool at: `$ISC_HOME/bin/importExportTemplateDB.sh`.

Enter the following:

```
importExportTemplateDB.sh <admin_user_id> <password> [<other_arguments>]
```

where:

<admin_user_id> is user identifier for someone with the **admin** role.

<password> is the password for the one with the **admin** role.

<other_arguments> is any combination of the following arguments separated by a space:

-nooverwrite

If you choose to use this **nooverwrite** argument, to prevent the overwriting of existing templates in the database, it must precede all other arguments and must be in the third position after <admin_user_id> and <password>.



Note The default (when **nooverwrite** is not specified) is to overwrite the templates.

-exp_db <dest-dir>

Use this argument to export all templates and datafiles in the database, where <dest-dir> is the destination directory to which you want to export.

-imp_db <src-dir>

Use this argument to import all the files in <src-dir> into the database, where <src-dir> is the source directory from which you want to import. The files in <src-dir> are created by the **exp_db** process.

-exp_template_folder <src-folder-path> <dest-dir>

Use this argument to export a database template folder and its subfolders, where <src-folder-path> is the full path of the template folder to export and <dest-dir> is the directory where to place the exported files.

-imp_template_folder <src-dir> <dest-folder>

Use this argument to import all files in <src-dir> into the database, where <src-dir> is the source directory to import, and <dest-folder> is the destination import template folder.

-imp_template <srcfile> <dest-folder> <template-name>

Use this argument to import a template into the database, where <srcfile> is the full path of the template to import, <dest-folder> is the full path of the parent folder, and <template-name> is the template name in the database.

-imp_datafile *<srcfile> <dest-template> <datafile-name>*

Use this argument to import a template datafile into the database, where *<srcfile>* is the full path of the datafile to import, *<dest-template>* is the full path of the parent template, and *<datafile-name>* is the datafile name in the database.

-exp_template *<template-pathname> <output-file>*

Use this argument to export the database template to a file, where *<template-pathname>* is the full path of the template to export, and *<output-file>* is the output filename.

-exp_datafile *<datafile-pathname> <output-file>*

Use this argument to export a template datafile to a file, where *<datafile-pathname>* is the full path of the template datafile to export, and *<output-file>* is the output filename.



CHAPTER 7

Monitoring

From the Home window of Cisco IP Solution Center (ISC), which 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 choose 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 7-11](#) Manage probes and view reports.
- [TE Performance Report, page 7-41](#) TE performance report.
- [Reports, page 7-41](#) Create and schedule reports.

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 7-7](#)

Tasks

This section contains the following topics:

- [Starting Task Manager, page 7-2](#)
- [Create, page 7-3](#)
- [Audit, page 7-5](#)
- [Details, page 7-6](#)
- [Schedules, page 7-6](#)
- [Logs, page 7-7](#)
- [Delete, page 7-7](#)

Starting Task Manager

To start Task Manager, follow this step:

- Step 1** Click the **Task Manager** icon. The Tasks list page appears, as shown in [Figure 7-2](#), “Tasks.”

Figure 7-2 Tasks

#	Task Name	Type	Targets	Schedule	User Name	Created on
1.	SLA enable_traps 2005-11-22 21:11:00.0	SLA Traps Enable		Single run at 2005-11-22 21:11:00.0	admin	2005-11-22 21:11:32.237
2.	SLA enable_probes 2005-11-22 21:11:00.0	SLA Enable		Single run at 2005-11-22 21:11:00.0	admin	2005-11-22 21:11:18.524
3.	SLA Creation 2005-11-22 18:53:00.0	SLA Creation		Single run at 2005-11-22 18:53:00.0	admin	2005-11-22 18:50:47.189

The Tasks window displays information about each task by **Task Name**, **Type**, **Targets**, **Schedules** date and time, the **User Name** who created those tasks, and the date **Created on**. To view, schedule, or delete the listed tasks, check the corresponding check box.

New Tasks can also be created or audited using this window.

Create

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 and interface bandwidth utilization using SNMP.

Figure 7-3 Create Tasks

Create Task	
Name :	Service Deployment 2005-12-06 18:14:24.448
Type:	Service Deployment
Description:	Created on 2005-12-06 18:14:24.448
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)**. If you choose **Simplified**, you can make many selections in one window. If you choose **Advanced (via wizard)**, you navigate through many windows to make your selections.

- 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](#), “Service Deployment Task,” respectively, with variations.

Figure 7-4 Task Devices

Devices:	Select/Deselect
Groups:	Select/Deselect
Options:	☒ Retrieve device attributes ☒ Retrieve Interfaces
Schedule:	☒ Now ☐ Later ☐ None
Task Owner:	☐ Customer ☐ Provider ☒ None
Submit Cancel	

Note: * - Required Field

149190

Figure 7-5 Service Deployment Task

Service Deployment Task	
Deployment Task: Service Deployment 2005-12-06 18:14:24.448	
Service Requests *	Select/Deselect
Options:	☐ Force Deployment ☒ Provision and Audit ☐ Regenerate IPsec Pre-shared Keys
Schedule:	☒ Now ☐ Later ☐ None
Task Owner:	☐ Customer ☐ Provider ☒ None
Submit Cancel	

Note: * - Required Field

149192

- 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](#), “Service Deployment Task,” 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 does not appear or after you complete this device group selection, proceed to [Step 10](#).

- Step 10** Choose the **Options**. If the **Retrieve Interfaces** checkbox is checked, ISC uses Simple Network Management Protocol (SNMP) to retrieve device interface information, such as ifIndex, and so on. If the **Retrieve Interfaces** check box is unchecked, configuration collection information is still retrieved, but SNMP is not used. All scenarios other than doing IP Service Level Agreement (SLA) probes do not require SNMP or this option.
- 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

- 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,”:
- **Config Audit** - compares ISC generated configlet against the one in the device.
 - **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.

Details

To get details about a particular task, follow these steps:

-
- Step 1** From the **Tasks** page, as shown in [Figure 7-2](#), “**Tasks**,” check a check box for one task for which you want to see a detailed list of information.
 - Step 2** Click **Details**.
 - Step 3** Click **OK** to return to [Figure 7-2](#), “**Tasks**.”
-

Schedules

To change the scheduling of an existing task, follow these steps:

-
- Step 1** From the **Tasks** page, as shown in [Figure 7-2](#), “**Tasks**,” check a check box for the one task for which you want to reset the scheduling directions.
 - Step 2** Click **Schedules**.
 - Step 3** If you want to delete this task, proceed to [Step 4](#). If you want to reset the scheduling directions, proceed to [Step 5](#).
 - Step 4** In the new window, check the check box for the task you want to delete and click the **Delete** button. Then proceed to [Step 7](#).
 - Step 5** In the new window, click **Create**, and you receive a window as shown in [Figure 7-7](#), “**Task Scheduling**.”

Figure 7-7 Task Scheduling

-
- Step 6** Make the new scheduling selections you want and click **Save** to reset the scheduling directions.
 - Step 7** Uncheck any check boxes and click **OK** to return to [Figure 7-2](#), “**Tasks**.”
-

Logs

This selection from the **Tasks** page, as shown in [Figure 7-2](#), “**Tasks**,” is another way of doing what is explained in the “**Task Logs**” section on page 7-7.

Delete

To delete one or more tasks, follow these steps:

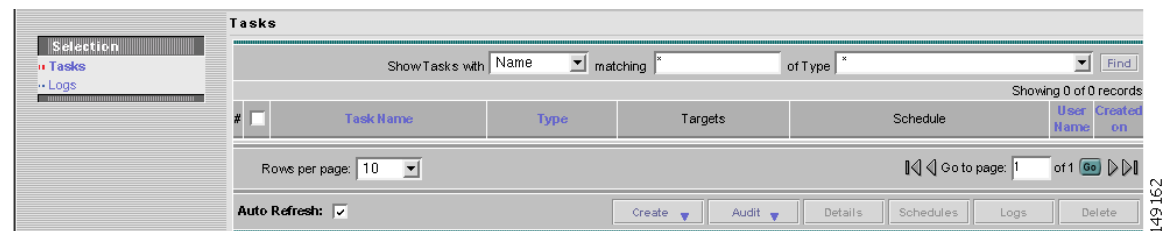
-
- Step 1** From the **Tasks** page, as shown in [Figure 7-2](#), “**Tasks**,” check one or more check boxes for the task(s) you want to delete.
- Step 2** You receive a confirmation window. If you want to delete, click **OK**. If not, click **Cancel**.
- Step 3** You return to an updated **Tasks** page, as shown in [Figure 7-2](#), “**Tasks**.”
-

Task Logs

Task Logs can be used to understand the status of a task, whether 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:

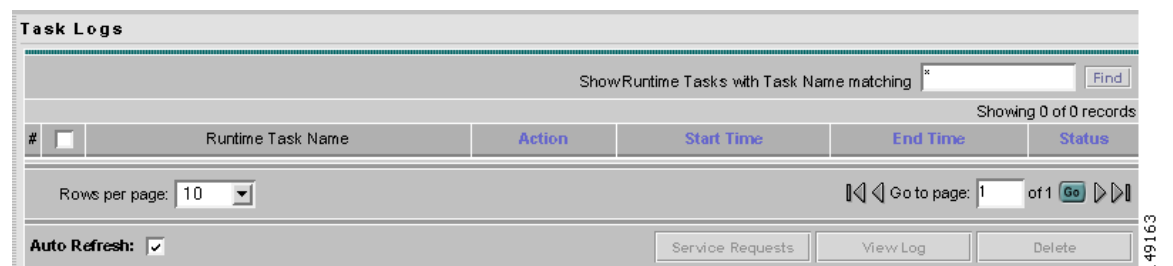
-
- Step 1** Click **Task Manager**. The Tasks page appears, as shown in [Figure 7-8](#), “**Tasks**.”

Figure 7-8 **Tasks**



- Step 2** Click **Logs** under the TOC heading located on the left-hand side. The Task Logs page appears, as shown in the [Figure 7-9](#), “**Task Logs**.”

Figure 7-9 **Task Logs**



This window displays the task by **Runtime Task Name**, and the **Action**, **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, check the check box for the row that represents the task and click the **View Log** button.
- Step 4** 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: **Config** 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/misc/tmp/firewall/1048888547147
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](#)

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 5** Click **Return to Logs** to specify another log to view.

Ping

Ping is the way ISC monitors the VPN connectivity, that is, verifies the connectivity among various edge devices comprising the VPN.



Note

Ping features are not supported on devices running IOS XR.

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 service deployment.

However, Ping does not do the following:

- Ping does not work in environments where ICMP traffic is blocked, for example, in a Cisco IOS router with an access-list denying all ICMP traffic.

- 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.

**Note**

ISC has a component Cisco MPLS Diagnostics Expert that might help you. See the [Cisco MPLS Diagnostics Expert 2.1 Failure Scenarios Guide on ISC 5.0](#).

After you choose **Monitoring > Ping**, you receive a window as shown in [Figure 7-11](#), “Services.”

Figure 7-11 Services

Services

Show Services with Job ID matching * of Type MPLS VPN Find

Showing 1 - 2 of 2 records

#	Job ID	State	Type	Operation Type	Creator	Customer Name	Policy Name	Last Modified	Description
1.	1	REQUESTED	MPLS	ADD	admin	Customer1	MPLSPolicy_PCE	10/27/05 5:25 PM	
2.	2	REQUESTED	MPLS	ADD	admin	Customer1	MPLSPolicyNO_CE	10/27/05 5:25 PM	

Rows per page: 10 Go to page: 1 of 1 Go

Auto Refresh: ☒ Configure Ping Parameters

The **Type** field indicates **MPLS**. Follow these steps:

- Step 1** Check the check box next to each row for which you want to configure ping parameters.
- 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

Datagram Size: 100

Start Ping

Fill in the following and then click **Start Ping**:

- Ping Type—Do PE to CE Ping** 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 endpoint 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 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 endpoint in the service request. When this selection is chosen, then after you click **Start Ping**, you go 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 checked, then a ping from device2 to device1 also occurs.
- Packet Repeat Count** (default: 5) This value indicates how many ICMP packets to use for a ping.
- Datagram size** (default: 100) This value is the packet size of ICMP used for ping.

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		Site-ence61 Incomplete
Rows per page: 10								
Start MPLS CE Ping								

Step 4 Check the check box next to each row for which you want to select a CE.

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

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.
- **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.

**Note**

SLA features are not supported on devices running IOS XR.

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)
- 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 choose **Monitoring > SLA**, implement the setup procedures in the “[Setup Prior to Using SLA](#)” section on page 7-12.”

Then choose **Monitoring > SLA and** you can select one of the following:

- [Probes, page 7-12](#) is the default selection.
- [Reports, page 7-36](#)

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** or **From MPLS PE or MVRP-CE**, the service requests associated with the devices *must* be in the Deployed state.

Probes

When you choose **Monitoring > SLA > Probes**, you receive a window as shown in [Figure 7-15](#), “[SLA Probes](#).”

Figure 7-15 SLA Probes

The default button that is enabled is **Create** and from the **Create** drop-down list, you can choose to create SLA probes **From Any SA Agent Device(s)**; **From MPLS CPE**; or **From MPLS PE or MVRP-CE**. However, if you select one or more existing probes by clicking the row(s) of existing probe(s), then you have access to the other buttons, **Details**, **Delete**, **Enable**, and **Disable**. For **Enable** and **Disable**, the drop-down list contains options to enable or disable SLA **Probes** and SLA **Traps**.

The explanations of the buttons and subsequent drop-down lists is given as follows:

- [Create Common Parameters, page 7-13](#) This section explains the SLA common parameters for all of the probe creation types: **From Any SA Agent Device(s)**; **From MPLS CPE**; or **From MPLS PE or MVRP-CE**.
- [Create From Any SA Agent Device\(s\), page 7-16](#) This section explains how to create probes from any SA Agent device(s) and begins after creating common parameters.
- [Create from MPLS CPE, page 7-18](#) This section explains how to create probes from an MPLS CPE and begins after creating common parameters.
- [Create From MPLS PE or MVRP-CE, page 7-22](#) This section explains how to create probes from an MPLS PE or MVRP-CE and begins after creating common parameters.
- [Protocols, page 7-24](#) This section is common Probes information for each of the **Create** paths.
- [Details, page 7-30](#) This section gives details about a specified probe.
- [Delete, page 7-31](#) This section explains how to delete a probe.
- [Enable Probes, page 7-32](#) This section explains how to enable the Probe and change its status from Created to Active state.
- [Enable Traps, page 7-33](#) This section explains how to enable traps.
- [Disable Probes, page 7-34](#) This section explains how to disable the Probe and change its status from Active to Disabled.
- [Disable Traps, page 7-35](#) This sections explains how to disable traps.

Create Common Parameters

When you choose **Monitoring > SLA > Probes**, the default is the **Probes** page with only the **Create** button enabled, as shown in [Figure 7-15](#). From the **Create** drop-down list, you can choose **From Any SA Agent Device(s)**, **From MPLS CPE**, or **From MPLS PE or MVRP-CE**. The first window to appear in all ways of creation is specified here. Then you proceed to the specific creation type you have chosen.

Follow these steps:

-
- Step 1** The window to appear is as shown in [Figure 7-16](#), “[SLA Common Parameters](#).”

Figure 7-16 SLA Common Parameters

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

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 choose the **Precedence** radio button for **TOS Category**, you have one set of type of service (TOS) values. If you choose 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 choose a ToS value of 5, then choose 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: unchecked)** If you check 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 an unchecked 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 checked. 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: unchecked, which means No) If you check 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 unchecked, 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 checked**. 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 Next you proceed to [Create From Any SA Agent Device\(s\)](#), page 7-16, [Create from MPLS CPE](#), page 7-18, or [Create From MPLS PE or MVRP-CE](#), page 7-22.

Create From Any SA Agent Device(s)

After you have completed the steps in [Create Common Parameters, page 7-13](#), follow these steps:


Note

IP connectivity must be available between the SA Agent devices.

Step 1 The next window to appear is as shown in [Figure 7-17, “SLA Source Devices.”](#)

Figure 7-17 SLA Source Devices

SLA Source Devices

Showing 1 - 3 of 3 records

#	☐	Device Name	Interface	Type
1.	☐	pe1	172.29.146.21 Select	CISCO_ROUTER
2.	☐	sw2	172.29.146.38 Select	CISCO_ROUTER
3.	☐	ce3	172.29.146.26 Select	CISCO_ROUTER

Rows per page: 10

Go to page:

1

of 1

Go

Add

Delete

49036

149 036

Step 2 Click the **Add** button and a window appears as shown in [Figure 7-18, “SLA Devices > Add,”](#) which lists all the devices in the database that have a minimum of one interface. Check the check box next to each row for the device you want to select, then click **Select**.

Figure 7-18 SLA Devices > Add

Show Devices with Device Name matching * Find					
Showing 1 - 8 of 8 records					
#	☐	Device Name	Management IP Address	Type	Parent Device Name
1.	☐	pe1		Cisco IOS Device	
2.	☐	pe3		Cisco IOS Device	
3.	☐	sw2		Cisco IOS Device	
4.	☐	sw3		Cisco IOS Device	
5.	☐	sw4		Cisco IOS Device	
6.	☐	ce3		Cisco IOS Device	
7.	☐	ce8		Cisco IOS Device	
8.	☐	ce13		Cisco IOS Device	
Rows per page: 10					
Go to page: 1 of 1 Go					
Select Cancel					

149 017

- Step 3** You return to [Figure 7-17](#) 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. Select one radio button for an interface and click **Select** and the IP address changes in [Figure 7-17](#).
 - **Type** Gives you the type of the source device.
- Step 4** You can repeat [Step 2](#) to [Step 3](#) to add more devices, or you can delete any of the currently selected source devices. To delete, check the check box next to each row for the device you want to delete and then click **Delete**.

**Note**

There is no second chance for deleting source devices. There is no confirm window.

- Step 5** Click **Next**. The next window to appear is as shown in [Figure 7-19](#), “SLA Destination Devices.”

Figure 7-19 SLA Destination Devices

#	Device Name	Interface	Type
1. ☐	pe3	172.29.146.23 Select	CISCO_ROUTER
2. ☐	sw3	172.29.146.39 Select	CISCO_ROUTER
3. ☐	ce8	172.29.146.31 Select	CISCO_ROUTER

Showing 1 - 3 of 3 records

Rows per page: 10 Go to page: 1 of 1 [Go](#)

[Add](#) [Delete](#)

- Step 6** Click the **Add** button and a window appears as shown in [Figure 7-18](#), “SLA Devices > Add.” Check the check box next to each row for the device you want to select. Then click **Select**.
- Step 7** You return to [Figure 7-19](#) 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. Select one radio button for an interface and click **Select** and the IP address changes in [Figure 7-19](#).
 - **Type** Gives you the type of the source device.
- Step 8** You can repeat [Step 6](#) to [Step 7](#) to add more devices, or you can delete any of the currently selected destination devices. To delete, check the check box next to each row for the device you want to delete and then click **Delete**.

**Note**

There is no second chance for deleting destination devices. There is no confirm window.

- Step 9** Click **Next**. Proceed to the “[Protocols](#)” section on page 7-24.”

Create from MPLS CPE

After you have completed the steps in [Create Common Parameters](#), page 7-13, follow these steps:

- Step 1** The next window to appear is as shown in [Figure 7-20](#), “SLA CPE Parameters.”

Figure 7-20 SLA CPE Parameters

- Step 2** Click the **Select** button for **VPN** and a window appears as shown in [Figure 7-21](#), “Select VPN,” which lists all the VPNs in the database.

Figure 7-21 Select VPN

#	VPN Name	Customer Name
1.	Mpls-VPN-1	Customer1
2.	Mpls-VPN-2	Customer1
3.	Vpn1	Customer1
4.	Vpn2	Customer1
5.	Vpn3	Customer2
6.	Vpn4	Customer2

Click the radio button for the VPN you want to select. Then click **Select**.

- Step 3** You return to [Figure 7-20](#) and the newly added VPN and Customer information appear and a **Select** button appears for **CPE**. You can change the VPN by repeating [Step 2](#).
- Step 4** Click the **Select** button for **CPE** and a window appears as shown in [Figure 7-22](#), “Select CPE,” which lists the CPEs associated with the selected VPN. Click the radio button for the CPE you want to select. Then click **Select**.

Figure 7-22 **Select CPE**

#	Select	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

- Step 5** You return to [Figure 7-20](#) and the newly added **CPE** and its first interface appear and a **Select** button appears for **CPE Interface**. You can change the CPE by repeating [Step 4](#).
- Step 6** If you want to change the default **CPE Interface** information that appears, click **Select** and you receive a window as shown in [Figure 7-23](#), “**Interfaces**.”

Figure 7-23 **Interfaces**

#	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	

Interfaces for device **ence51**

ShowDevice Interfaces with Interface Name matching * Find

Showing 1-6 of 6 records

Rows per page: 10

Select Cancel

Click the radio button next to the row for the interface you want to select. Then click **Select**.

- Step 7** You return to [Figure 7-20](#) and the newly added **CPE Interface** appears. You can change the CPE Interface by repeating [Step 6](#).
- Step 8** 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 9](#). If you click the **CPEs** radio button, proceed to [Step 12](#).
- Step 9** Click **Select** for **Connected PE Interface** and a window appears as shown in [Figure 7-24](#), “**Connected PE Interface**.”

Figure 7-24 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:

Click the radio button next to the row for the interface you want to select. Then click **Select**.

- Step 10** You return to [Figure 7-20](#) and the newly added **Connected PE Interface** appears. You can change the Connected PE Interface by repeating [Step 9](#).
- Step 11** Click **Next** and proceed to the [“Protocols” section on page 7-24](#).
- Step 12** When you click **CPEs**, the window is as shown in [Figure 7-25](#), “CPEs.”

Figure 7-25 CPEs

You Are Here: [Monitoring](#) > [SLA](#) > [Probes](#)

Mode: ADDING

- ☒ 1. Common Parameters
- ☐ 2. SLA Devices
- ☐ 3. Protocols
- ☐ 4. Summary

SLA Source and Destination Devices

VPN Information

VPN *: Mpls-VPN-1 [Select](#)

Customer: Customer1

Source Device

CPE *: ce3 [Select](#)

CPE Interface *: 172.29.146.26 [Select](#)

Destination Device(s)

Type: ☐ Connected PE ☒ CPEs

CPEs: Showing 0 of 0 records

#	Device Name	Interface	Select	Remove
Rows per page: 10 Go to page: 1 of 1 Go				

- Step 2 of 4 -

[< Back](#) [Next >](#) [Finish](#) [Cancel](#)

- Step 13** Click the **Select** button for CPEs and a window appears as shown in [Figure 7-26](#), “**Select CPE Associated with the Specified VPN**,” which lists all the CPEs associated with the specified VPN in the database.

Figure 7-26 Select CPE Associated with the Specified VPN

CPEs associated with **Customer1_VPN**

Showing 1-2 of 2 records

#	☐	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](#)

Check the check box next to the row(s) for the CPE(s) you want to select. Then click **Select**.

**Note**

Do *not* add a device chosen as a **Source Device** to **Destination Device(s)**.

- Step 14** You return to [Figure 7-25](#) and the newly added **Device Name** appears.
- Step 15** Click **Select** in the **Interface** column and a window appears as in [Figure 7-23](#). Click the radio button next to the row for the CPE you want to select. Then click **Select**.

- Step 16** You return to [Figure 7-25](#) and the newly added **CPE Interface** appears. You can change the CPE Interface by repeating [Step 15](#).
- Step 17** Check the check box next to each row for the Devices you want to remove. Then click the **Remove** button and a window as shown in [Figure 7-25](#) appears without the removed Device(s).
- Step 18** When [Figure 7-25](#) reflects what you want, click **Next** and proceed to the “[Protocols](#)” section on [page 7-24](#).

Create From MPLS PE or MVRF-CE

After you have completed the steps in [Create Common Parameters, page 7-13](#), follow these steps:

- Step 1** The next window to appear is as shown in [Figure 7-27](#), “[SLA Source and Destination Devices](#).”

Figure 7-27 *SLA Source and Destination Devices*

VPN Information

VPN :

Customer:

Source Device

PE/MVRF-CE :

VRF :

Destination Device(s)

PEs and CPEs: ☐ Showing 0 of 0 records

#	Device Name	Interface
Rows per page: 10 Go to page: 1 of 1 Go		

- Step 2** Click the **Select** button for **VPN** and a window appears as shown in [Figure 7-28](#), “[Select VPN](#),” which lists all the VPNs in the database. Click the radio button next to the row for the VPN you want to select. Then click **Select**.

Figure 7-28 *Select VPN*

Show VPNs with VPN Name matching

Showing 1 - 6 of 6 records

#	VPN Name	Customer Name
1.	Mpls-VPN-1	Customer1
2.	Mpls-VPN-2	Customer1
3.	Vpn1	Customer1
4.	Vpn2	Customer1
5.	Vpn3	Customer2
6.	Vpn4	Customer2

Rows per page: 10 | Go to page: 1 of 1 |

- Step 3** You return to [Figure 7-27](#) and the newly added VPN and Customer information appears. You can change the VPN and Customer by repeating [Step 2](#).
- Step 4** Click the new **Select** button for **PE/MVRF-CE** and you receive a drop-down list from which you can choose **PE** or **MVRF-CE**. If you choose **PE**, a window appears as shown in [Figure 7-29](#), “**Select PE**,” which lists all the PEs associated with the selected VPN. If you choose MVRF-CE, a window appears as shown in [Figure 7-30](#), “**Select CPE**,” which lists all the MVRF-CEs associated with the selected VPN. Click the radio button next to the row for the PE or MVRF-CE you want to select. Then click **Select** or **OK**.

Figure 7-29 **Select PE**

#	Provider Name	PE Region Name	Device Name	Role Type
1.	Provider1	region_1	pe1	N-PE

Rows per page: 10 Go to page: 1 of 1 **Go**

Select **Cancel**

Figure 7-30 **Select CPE**

#	Customer Name	Site Name	Device Name	Management Type

Rows per page: 10 Go to page: 1 of 1 **Go**

OK **Cancel**

- Step 5** You return to [Figure 7-27](#) and the newly added PE or MVRF-CE information appears. You can change this selection by repeating [Step 4](#).
- Step 6** If in [Step 4](#) you chose MVRF-CE information, you can click the **VRF** drop-down list.
- Step 7** Click the new **Select** button for **Destination Device(s)**—**PEs and CPEs** and from a drop-down list, choose **PEs** or **CPEs**. If you choose **PEs**, a window appears as shown in [Figure 7-31](#), “**Select PEs**,” which lists all the PE Interfaces in the database. If you choose **CPEs**, a window appears as shown in [Figure 7-32](#), “**Select CPEs**,” which lists all the CPE Interfaces in the database. Click the radio button next to the row for the Device Interface you want to select. Then click **Select**.



Note

Do *not* add a device chosen as a **Source Device** to **Destination Device(s)**.

Figure 7-31 **Select PEs**

#	Provider Name	PE Region Name	Device Name	Role Type
1.	Provider1	region_1	pe1	N-PE

Rows per page: 10 Go to page: 1 of 1 Go

Select Cancel

Figure 7-32 **Select CPEs**

#	Customer Name	Site Name	Device Name	Management Type
1.	Customer1	east	ce3	MANAGED

Rows per page: 10 Go to page: 1 of 1 Go

Select Cancel

- Step 8** You return to [Figure 7-27](#) and you receive interface information. Click **Select** and you get a window from which you can click a radio button next to a different interface. Click **Select** and the new interface replaces the old interface. You can change the Interface by repeating this step.
- Step 9** Click **Next** and proceed to the “[Protocols](#)” section on [page 7-24](#).

Protocols

You choose this location after you have completed all the steps in one of the **Create** functions: [Create Common Parameters, page 7-13](#); [Create from MPLS CPE, page 7-18](#); or [Create From MPLS PE or MVRP-CE, page 7-22](#). Follow these steps:

- Step 1** The next window to appear is as shown in [Figure 7-33](#), “[Protocols](#).”

Figure 7-33 Protocols

Step 2 Click the **Add** drop-down list and select:

- **ICMP Echo** (only available if destination devices are available) Proceed to [Step 3](#).
- **TCP Connect** (not available for Create From MPLS PE or MVRF-CE; 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 or MVRF-CE) Proceed to [Step 7](#).
- **DNS** (not available for Create from MPLS PE or MVRF-CE) Proceed to [Step 8](#).
- **HTTP** (not available for Create from MPLS PE or MVRF-CE) Proceed to [Step 9](#).
- **DHCP** (not available for Create from MPLS PE or MVRF-CE) Proceed to [Step 10](#).

Step 3 From [Step 2](#), if you chose **ICMP Echo**, you receive a window as shown in [Figure 7-34](#), “Protocol ICMP Echo.”

Figure 7-34 Protocol ICMP Echo

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 7-35](#), “Protocol TCP Connect.”

Figure 7-35 Protocol TCP Connect

SLA Protocol	
Protocol:	TCP Connect
Destination Port *:	23 (1 - 65535)
Request Size:	1 (1 - 16384 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 7-36](#), “Protocol UDP Echo.”

Figure 7-36 Protocol UDP Echo

SLA Protocol	
Protocol:	UDP Echo
Destination Port *:	7 (1 - 65535)
Request Size:	16 (4 - 8192 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 7-37](#), “Protocol Jitter.”

Figure 7-37 Protocol Jitter

SLA Protocol	
Protocol:	Jitter
Destination Port*:	8000 (1 - 65535)
Request Size:	32 (16 - 1500 bytes)
Number of Packets:	10 (1 - 1000)
Interval:	20 (1 - 1000 msec)
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 7-38](#), “Protocol FTP.”

Figure 7-38 Protocol FTP

SLA Protocol	
Protocol:	FTP
User Name:	
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 7-39](#), “Protocol DNS.”

Figure 7-39 Protocol DNS

Protocol:	DNS	
Name Server *:		
Name to be Resolved *:		
Request Size *:	1	(0 - 16384 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 7-40](#), “Protocol HTTP.”

Figure 7-40 Protocol HTTP

SLA Protocol	
Protocol:	HTTP
Version:	1.0
URL *:	
Cache:	☒
Proxy Server:	
Name Server:	
Operation:	HTTPGet ▼
Raw Request *:	
Request Size *:	1 (1 - 16384 bytes)
OK Cancel	
Note: * - Required Field	

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 an unchecked check box, the HTTP request should not download cached pages. For a checked 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 list 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 receive a window as shown in [Figure 7-41](#), “Protocol DHCP.”

Figure 7-41 Protocol DHCP

Enter the required information as follows, click **OK**, and then proceed to [Step 11](#).

- **Destination IP Address** (required)

Step 11 You return to [Figure 7-33](#) 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.

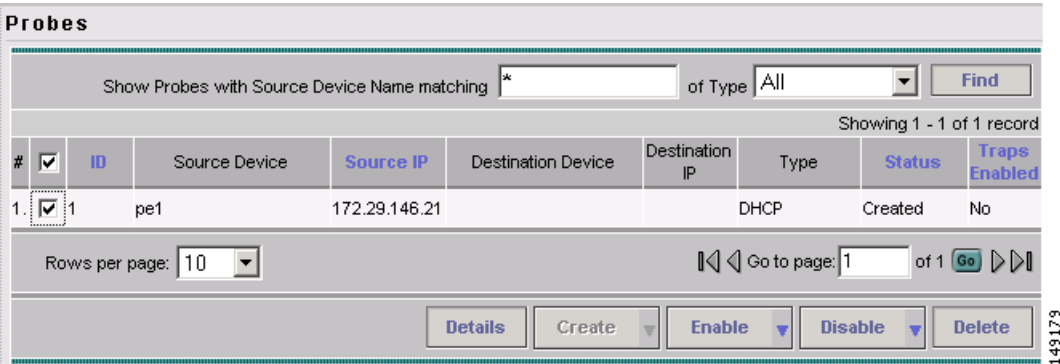
Step 12 The next window to appear is a Probe Creation Task Summary window that shows the **Description** (date and time created), **Common Parameters**, **Source Devices**, **Destination Devices**, and **Protocols** that you have defined. If all exists the way you want it, click **Finish**. Otherwise, click **Back** and make corrections.

Details

When you choose **Monitoring > SLA > Probes**, you can get details by following these steps:

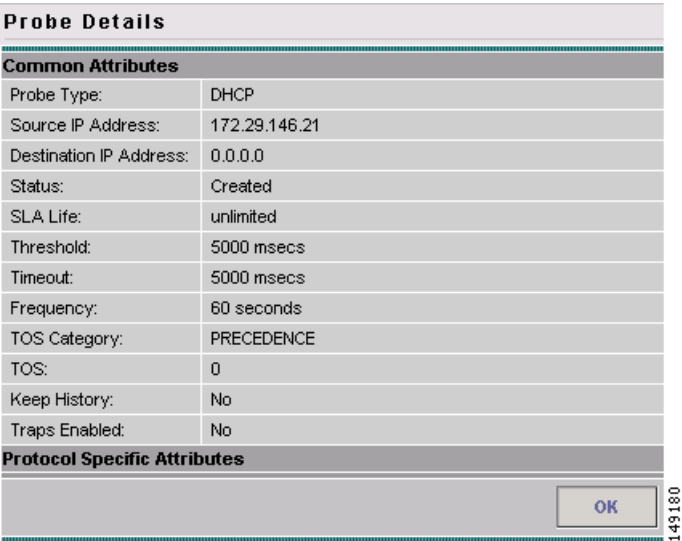
- Step 1
- Select an existing probe by checking the corresponding check box for which you want details. Then you have access to the **Details** button, as shown in [Figure 7-42](#), “SLA Probes > Details.”

Figure 7-42 SLA Probes > Details



- Step 2
- After you click the **Details** button, you receive a window as shown in [Figure 7-43](#), “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 7-43 SLA Probes Details



- Step 3
- Click **OK** to return to a window as shown in [Figure 7-42](#). You can continue to select more **Details** or complete another function.

Delete

When you choose **Monitoring > SLA > Probes**, you can delete probes from the list by following these steps:

- Step 1** Select one or more existing probes by checking the check box(es) for the row(s) of existing probe(s). Then you have access to the **Delete** button, as shown in [Figure 7-44](#), “**SLA Probes > Delete**.”

Figure 7-44 *SLA Probes > Delete*

Probes

Show Probes with Source Device Name matching of Type

Showing 1 - 1 of 1 record

#	☒	ID	Source Device	Source IP	Destination Device	Destination IP	Type	Status	Traps Enabled
1	☒	1	pe1	172.29.146.21			DHCP	Created	No

Rows per page: Go to page: of 1

- Step 2** After you click the **Delete** button, a window as shown in [Figure 7-45](#), “**Confirm Delete Probes**,” appears.

Figure 7-45 *Confirm Delete Probes*

Selected Probes

Confirm Delete Probes

Showing 1 - 1 of 1 record

#	ID	Source Device	Source IP	Destination Device	Destination IP	Type	Status	Traps Enabled
1.1	pe1	172.29.146.21				DHCP	Created	No

Rows per page: Go to page: of 1

- Step 3** Click **OK** if [Figure 7-45](#) 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.

- Step 4** You return to [Figure 7-44](#) with updated information.

Enable Probes

When you choose **Monitoring > SLA > Probes**, you can enable probes by following these steps:

- Step 1** Select one or more existing probes by checking the check box(es) for the row(s) of existing probe(s). Then you have access to the **Enable** button. From the **Enable** drop-down list, you have access to **Probes**, as shown in [Figure 7-46](#), “SLA Probes > Enable > Probes.”

Figure 7-46 SLA Probes > Enable > Probes

The screenshot shows the 'Probes' management page. At the top, there is a search bar with the text 'Show Probes with Source Device Name matching *' and a 'Find' button. Below this, a table lists the probes. The table has columns: #, ID, Source Device, Source IP, Destination Device, Destination IP, Type, Status, and Traps Enabled. There is one row with ID 1, Source Device pe1, Source IP 172.29.146.21, Type DHCP, Status Created, and Traps Enabled No. Below the table, there are buttons for 'Details', 'Create', 'Enable', 'Disable', and 'Delete'. The 'Enable' button is highlighted, and a dropdown menu is open showing 'Probes' and 'Traps' options. The page number 149182 is visible on the right side.

- Step 2** After you choose **Enable > Probes**, a window as shown in [Figure 7-47](#), “Confirm Enable Probes,” appears.

Figure 7-47 Confirm Enable Probes

The screenshot shows the 'Confirm Enable Probes' dialog box. It has a title bar 'Confirm Enable Probes' and a table with the same columns as Figure 7-46. There is one row with ID 1, Source Device pe1, Source IP 172.29.146.21, Type DHCP, Status Created, and Traps Enabled No. Below the table, there are buttons for 'OK' and 'Cancel'. The page number 149183 is visible on the right side.

- Step 3** Click **OK** if [Figure 7-47](#) reflects the probes you want to enable or click **Cancel** if it does not. In both cases, you return to [Figure 7-46](#).
- 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 choose **Monitoring > SLA > Probes**, you can enable traps by following these steps:

- Step 1** Select one or more existing probes by checking the check box(es) for the row(s) of existing probe(s). Then you have access to the **Enable** button. From the **Enable** drop-down list, you have access to **Traps**, as shown in [Figure 7-48](#), “**SLA Probes > Enable > Traps**.”

Figure 7-48 *SLA Probes > Enable > Traps*

The screenshot shows the 'Probes' configuration page. At the top, there is a search bar with the text 'Show Probes with Source Device Name matching' and a dropdown menu set to 'All'. Below this is a table with the following columns: #, ID, Source Device, Source IP, Destination Device, Destination IP, Type, Status, and Traps Enabled. The table contains one row with the following data: 1, 1, pe1, 172.29.146.21, , DHCP, Created, No. Below the table, there is a 'Rows per page' dropdown set to 10 and a 'Go to page' dropdown set to 1 of 1. At the bottom, there are buttons for 'Details', 'Create', 'Enable', 'Disable', and 'Delete'. The 'Enable' button is highlighted, and a dropdown menu is open, showing 'Probes' and 'Traps' options.

- Step 2** After you choose **Enable > Traps**, a window as shown in [Figure 7-49](#), “**Confirm Enable Traps**,” appears. All the traps have 3000 ms as the falling threshold set automatically

Figure 7-49 *Confirm Enable Traps*

The screenshot shows the 'Confirm Enable Traps' dialog box. It has a title bar 'Selected Probes' and a subtitle 'Confirm Enable Traps'. Below the subtitle is a table with the following columns: #, ID, Source Device, Source IP, Destination Device, Destination IP, Type, Status, and Traps Enabled. The table contains one row with the following data: 1, 1, pe1, 172.29.146.21, , DHCP, Created, No. Below the table, there is a 'Rows per page' dropdown set to 10 and a 'Go to page' dropdown set to 1 of 1. At the bottom, there are buttons for 'OK' and 'Cancel'.

- Step 3** Click **OK** if [Figure 7-49](#) reflects the traps you want to enable or click **Cancel** if it does not. In both cases you return to [Figure 7-48](#).
- 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 choose **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 checking the check box(es) for the row(s) of existing probe(s). Then you have access to the **Disable** button. From the **Disable** drop-down list, you have access to **Probes**, as shown in [Figure 7-50](#), “**SLA Probes > Disable > Probes**.”

Figure 7-50 *SLA Probes > Disable > Probes*

Probes

Show Probes with Source Device Name matching of Type

Showing 1 - 1 of 1 record

#	☒	ID	Source Device	Source IP	Destination Device	Destination IP	Type	Status	Traps Enabled
1.	☒	1	pe1	172.29.146.21			DHCP	Created	No

Rows per page: Go to page: of 1

Probes
Traps

- Step 2** After you choose **Disable > Probes**, a window as shown in [Figure 7-51](#), “**Confirm Disable Probes**,” appears.

Figure 7-51 *Confirm Disable Probes*

Selected Probes

Confirm Disable Probes

Showing 1 - 1 of 1 record

#	ID	Source Device	Source IP	Destination Device	Destination IP	Type	Status	Traps Enabled
1.	1	pe1	172.29.146.21			DHCP	Created	No

Rows per page: Go to page: of 1

- Step 3** Click **OK** if [Figure 7-51](#) reflects the probes you want to disable or click **Cancel** if it does not. In both cases you return to [Figure 7-50](#).
- 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 choose **Monitoring > SLA > Probes**, you can disable traps by following these steps:

- Step 1** Select one or more existing probes by checking the check box(es) for the row(s) of existing probe(s). Then you have access to the **Disable** button. From the **Disable** drop-down list, you have access to **Traps**, as shown in [Figure 7-52](#), “**SLA Probes > Disable > Traps**.”

Figure 7-52 *SLA Probes > Disable > Traps*

The screenshot shows the 'Probes' management interface. At the top, there is a search bar: 'Show Probes with Source Device Name matching' followed by a text input field containing an asterisk (*), 'of Type' followed by a dropdown menu set to 'All', and a 'Find' button. Below this, it says 'Showing 1 - 1 of 1 record'. A table lists the probes with columns: #, ID, Source Device, Source IP, Destination Device, Destination IP, Type, Status, and Traps Enabled. The first row is: 1, 1, pe1, 172.29.146.21, , DHCP, Created, No. Below the table, there is a 'Rows per page' dropdown set to 10, and pagination controls: 'Go to page: 1 of 1' with 'Go' and navigation arrows. At the bottom, there are buttons: 'Details', 'Create', 'Enable', 'Disable' (with a dropdown arrow), and 'Delete'. The 'Disable' dropdown menu is open, showing 'Probes' and 'Traps' options.

- Step 2** After you choose **Disable > Traps**, a window as shown in [Figure 7-53](#), “**Confirm Disable Traps**,” appears.

Figure 7-53 *Confirm Disable Traps*

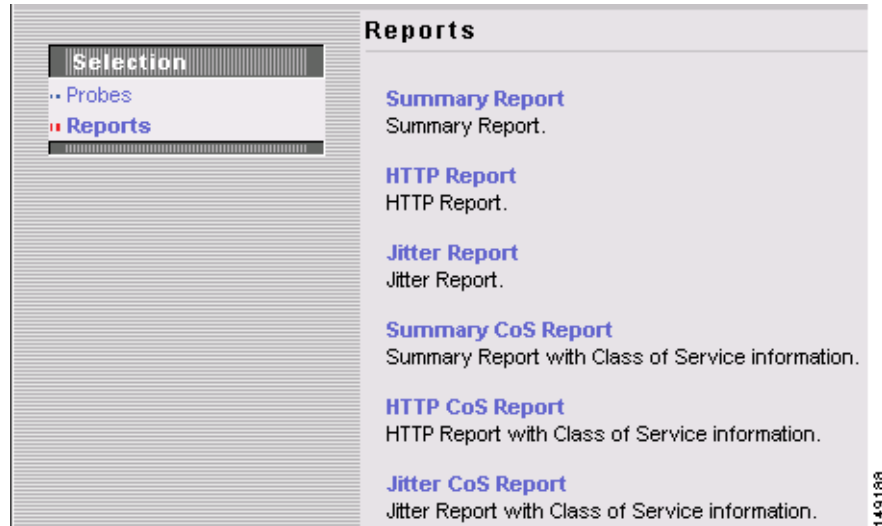
The screenshot shows the 'Confirm Disable Traps' dialog box. It has a title bar 'Selected Probes' and a main title 'Confirm Disable Traps'. Below the title, it says 'Showing 1 - 1 of 1 record'. A table lists the selected probes with columns: #, ID, Source Device, Source IP, Destination Device, Destination IP, Type, Status, and Traps Enabled. The first row is: 1, 1, pe1, 172.29.146.21, , DHCP, Created, No. Below the table, there is a 'Rows per page' dropdown set to 10, and pagination controls: 'Go to page: 1 of 1' with 'Go' and navigation arrows. At the bottom, there are 'OK' and 'Cancel' buttons.

- Step 3** Click **OK** if [Figure 7-53](#) reflects the traps you want to disable or click **Cancel** if it does not. In both cases you return to [Figure 7-52](#).
- 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 choose **Monitoring > SLA > Reports**, you receive a window as shown in [Figure 7-54](#), “SLA Reports.”

Figure 7-54 SLA Reports



You can then click on any of the following choices and receive that report

- [Summary Report, page 7-36](#) 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 7-39](#) This is a summary report for HTTP information.
- [Jitter Report, page 7-39](#) This is a summary report for Jitter information.
- [Summary CoS Report, page 7-40](#) 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 7-41](#) This report is for HTTP CoS information.
- [Jitter CoS Report, page 7-41](#) This report is for Jitter CoS information.

Summary Report

From [Figure 7-54](#), choose **Summary Report** and follow these steps:

-
- Step 1** The resulting window is shown in [Figure 7-55](#), “Parameters of Summary Report.”

Figure 7-55 Parameters of Summary Report

Parameters of Summary Report

Layout

Value Displayed :

Aggregate By : ☒ All ☐ Customer ☐ Provider ☐ VPN ☐ Source Router ☐ Probe

Timeline : ☐ All ☐ Yearly ☐ Monthly ☒ Weekly ☐ Daily ☐ Hourly

Filtering

Customer:

Provider:

VPN:

Source Routers:

Destination Routers:

Probes:

Precedence:

DSCP:

Probe Type:

Note: * - Required Field

Step 2 For [Figure 7-55](#), fill in the **Layout** fields, as follows:

- **Value Displayed** (required) (default: **All**) Click the drop-down list and choose 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 lists for the year, month, day of the month, and time of day for which to start the report.

Step 3 For [Figure 7-55](#), 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 7-55](#) 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 7-55](#) 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 7-55](#) 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, check the check box(es) for device(s). Then click **Select**. The result is that you return to [Figure 7-55](#) 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, check the check box(es) for device(s). Then click **Select**. The result is that you return to [Figure 7-55](#) 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, check the check box(es) for source probe(s). Then click **Select**. The result is that you return to [Figure 7-55](#) 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 list 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 choose a ToS value of 5, then choose 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 list 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.

- **Probe Type** (default: **All**) Click the drop-down list 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 7-24.

Step 4 Click **OK** in [Figure 7-55](#) 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 7-55](#) in which you can modify your selections as explained in the previous steps.

HTTP Report

From [Figure 7-54](#), choose **HTTP Report** and proceed similarly to the “[Summary Report](#)” section on page 7-36, with the following exceptions:

- **Value Displayed** has different drop-down choices.
- There is no **Destination Routers** selection
- There is no **Probe Type** drop-down list in the equivalent of [Figure 7-55](#), because the probe type is automatically **HTTP**. The result is an HTTP Report.

Jitter Report

From [Figure 7-54](#), choose **Jitter Report** and proceed similarly to the “[Summary Report](#)” section on page 7-36, with the following exceptions:

- **Value Displayed** has different drop-down choices.
- There is no **Destination Routers** selection
- There is no **Probe Type** drop-down list in the equivalent of [Figure 7-55](#), because the probe type is automatically **Jitter**. The result is a Jitter Report.

Summary CoS Report

From [Figure 7-54](#), choose **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 follow these steps:

- Step 1** The resulting window is shown in [Figure 7-56](#), “Parameters of CoS Summary Report.”

Figure 7-56 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 7-56](#), fill in the **Layout** fields, as shown in [Step 2](#) of the “Summary Report” section on [page 7-36](#), 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 7-36](#).
- Step 3** For [Figure 7-56](#), fill in the **Filtering** fields, as shown in [Step 3](#) of the “Summary Report” section on [page 7-36](#), with the exception that there are no **Precedence** or **DSCP** drop-down lists. They are now in the **Layout** fields, as explained in [Step 2](#) in this section.
- Step 4** Click **OK** in [Figure 7-56](#) 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 7-56](#) in which you can modify your selections as explained in the previous steps.

HTTP CoS Report

From [Figure 7-54](#), choose **HTTP Report** and proceed exactly as in the “[Summary CoS Report](#)” section on [page 7-40](#), with the following exceptions:

- **Value Displayed** has the same drop-down choices as **HTTP Report**.
- There is no **Destination Routers** selection
- There is no **Probe Type** drop-down list in the equivalent of [Figure 7-56](#), because the probe type is automatically **HTTP CoS**. The result is a CoS HTTP Report. This CoS HTTP report is based on the TOS values of the SLA probes.

Jitter CoS Report

From [Figure 7-54](#), choose **Jitter Report** and proceed exactly as in the “[Summary CoS Report](#)” section on [page 7-40](#), with the following exceptions:

- **Value Displayed** has the same drop-down choices as **Jitter Report**.
- There is no **Destination Routers** selection
- There is no **Probe Type** drop-down list in the equivalent of [Figure 7-56](#), because the probe type is automatically **Jitter CoS**. The result is a CoS Jitter Report. This CoS Jitter report is based on the TOS values of the SLA probes.

TE Performance Report

TE Performance Report for Traffic Engineering Management is explained in detail in the [Cisco IP Solution Center Traffic Engineering Management User Guide, 5.0](#).

Reports

When you choose **Monitoring > Reports**, a tree of reports appears in the data pane. Click on the + sign for each folder in the data pane and you receive a listing of all the provided reports. The non-SAMPLE reports in the L2VPN folder are explained in the [Cisco MPLS Diagnostics Expert 2.1 Failure Scenarios Guide on ISC 5.0](#) and the non-SAMPLE reports in the MPLS folder are explained in the [Cisco IP Solution Center MPLS VPN User Guide, 5.0.1](#).

Click on any of the specific reports and you can define how to set up the report. [Figure 7-57](#), “[Inventory > SAMPLE - Template Report - Report Window](#),” shows the sample file under the folder **Inventory**.

Figure 7-57 *Inventory > SAMPLE - Template Report - Report Window*

Reports

Layout

Title: SAMPLE - Template Report

Chart Type: Tabular

Filters (All field values are required, * or a valid value.)

Template Path: *

Template Definition Name: *

Template Name: *

Sorting

Field: Template Path Ascending

Output Fields

Template Path
Template Definition Name
Template Name

View

This section explains the Reports feature and how to use it in the following areas:

- [Introducing Reports, page 7-42](#)
- [Accessing Reports, page 7-43](#)
- [Using Reports GUI, page 7-43](#)
- [Running Reports, page 7-44](#)
- [Using the Output from Reports, page 7-45](#)
- [Creating Custom Reports, page 7-47](#)

Introducing Reports

Network operators often want to have detailed reports on the services provisioned. For example, for a given customer, you might want to see a list of the PE-CE connections and their detailed PE-CE configuration parameters or you might want to see specific Layer2 or Layer3 service requests on a PE. These reports help network operators by providing a centralized location for finding Service Requests (SRs) and VPN information.

When you choose **Monitoring > Reports**, reports are grouped by type to allow for easy navigation. ISC displays only predefined (canned) reports for which the user has RBAC permission.

You can select the filtering criteria and the outputs to be displayed in the report. You can save reports to a variety of formats.

In addition to the predefined reports that are documented in the *Cisco IP Solution Center Metro Ethernet and L2VPN User Guide, 5.0* and the *Cisco IP Solution Center MPLS VPN User Guide, 5.0.1*, ISC provides additional sample reports. Sample reports are provided for informational purposes only and are untested and unsupported.

The data structures that ISC uses to provide reports in the GUI are defined in an XML format.

Accessing Reports

To access the reports, follow these steps:

-
- Step 1** To access the reports framework in the ISC GUI, choose **Monitoring > Reports**.
- Step 2** Click on the folders to display the available reports.
- The Reports window appears, as shown in [Figure 7-57](#).
- Step 3** From the reports listed under one of the folders in the left navigation tree, click on the desired report to bring up the window associated with that report.
-

**Note**

Several sample reports are provided in each of the reports folders. These reports begin with the title **SAMPLE-**. These reports are provided for informational purposes only. They are untested and unsupported. You might want to use them, along with the supported reports, as a basis for creating your own custom reports. See the [“Creating Custom Reports” section on page 7-47](#) for information about custom reports.

Using Reports GUI

This section provides some general comments on using the reports GUI. This information applies to all reports. When you invoke a report, you see a window like the one shown in [Figure 7-57](#).

The window is divided into several areas:

- [Layout, page 7-43](#)
- [Filters, page 7-43](#)
- [Output Fields, page 7-44](#)
- [Sorting, page 7-44](#)

Layout

This area displays the title of the report and allows you to select the chart type. You can enter your own report title by overwriting the Title field.

**Note**

Only tabular output is supported.

Filters

In this pane you can define inputs or search criteria for the reports. Values entered here are compared against corresponding values associated with data objects in the ISC repository. Values must be entered for all fields. An asterisk (*) can be used as a wild-card character for an entire string.

For each filterable field, the GUI displays a label and a text input field. For certain fields, the GUI also displays a Select button that allows you to choose an existing object (for example, customer, Service Type, SR State, and so on). All available output fields are displayed in the window, allowing you to select the fields to include in the report. All output fields are selected by default.

**Note**

Filter values must be in the same format as the values represented within ISC. For example, a Service Request (SR) ID must be a number.

Output Fields

In this pane you can choose output fields to be displayed in the report. You can choose any or all of the output fields by selecting them with the mouse. Use the Shift key to select a continuous range of output values. Or, use the Control key to select random output values.

Sorting

This pane allows you to select how you want to sort the report output. For Field:, use the first drop-down list to select each filter field and then the second drop-down list to choose whether to display the report fields in ascending or descending order. The sort order can also be changed after you have the report output displayed (see [Figure 7-58](#)).

Running Reports

To run the report, click **View** in the lower right corner of the report window. This generates the report output. An example of a report output is shown in [Figure 7-58](#).

Figure 7-58 Report Output

The screenshot shows the IP Solution Center interface with a 'SAMPLE - Template Report' window. The window displays a table with 14 records. The table has three columns: Template Path, Template Definition Name, and Template Name. The records are numbered 1 through 14. The table is paginated, showing 1-14 of 14 records. The 'Rows per page' is set to 20. The 'Go to page' is set to 1 of 1 pages. The 'Go' button is highlighted. The '211207' timestamp is visible in the bottom right corner.

	Template Path	Template Definition Name	Template Name
1.	ATM	CLP_Egress	Data0
2.	ATM	CLP_Ingress	Data0
3.	DIA-Channelization	10K-CHOC12-ST51-PATH	SR_Data
4.	DIA-Channelization	10K-CT3-CHANNELIZED	SR_Data
5.	DIA-Channelization	10K-CT3-UNCHANNELIZED	SR_Data
6.	DIA-Channelization	PA-MC-E3-CHANNELIZED	SR_Data
7.	DIA-Channelization	PA-MC-STM1-AU3-CHANNELIZED	SR_Data
8.	DIA-Channelization	PA-MC-STM1-AU4-CHANNELIZED	SR_Data
9.	DIA-Channelization	PA-MC-T3-CHANNELIZED	SR_Data
10.	Examples	AccessList	Act2000
11.	Examples	AccessList1	Protocol-IP
12.	Examples	AccessList1	Protocol-TCP
13.	Examples	CEWanCOS	CEWanCOS
14.	FrameRelay	classification	Data0

The reports GUI supports output in tabular format. The output is listed in columns, which are derived from the outputs you selected in the reports window.

Each row (or record) represents one match of the search criteria you set using the filter fields in the reports window.

In some cases, the value returned in a field can be displayed as one of the following:

- **-1** means no information updated for this field
- **F** means false
- **T** means true

The column heading with a triangle icon is the output by which the records are sorted. By clicking on any column heading, you can toggle between ascending and descending sort order. To sort on another output value, click on the heading for that value.

For information on working with report output, see the [“Using the Output from Reports” section on page 7-45](#).

Using the Output from Reports

The icons at the upper right of the report output window (see [Figure 7-59](#)) provide the following functions, respectively, moving from left to right:

- Export explained in the [“Exporting Reports” section on page 7-46](#)
- Print explained in the [“Printing Reports” section on page 7-46](#)
- E-mail explained in the [“E-mailing Reports” section on page 7-46](#)
- Link to web-based product documentation explained in the [“Invoking Help” section on page 7-47](#)

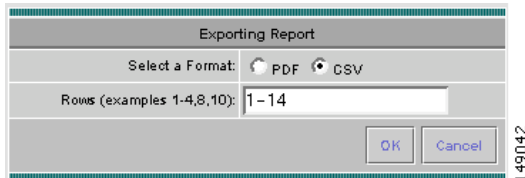
Figure 7-59 **Report Output Icons**



Exporting Reports

Click on the **Export** icon in [Figure 7-59](#), “[Report Output Icons](#),” to bring up a window like the one shown in [Figure 7-60](#) and then follow these steps.

Figure 7-60 *Exporting Report Window*



-
- Step 1** Select the appropriate radio button for the format you want:
- PDF file – Adobe’s portable document format.
 - CSV file – Comma Separated Values format that allows for the data to be easily exported into a variety of applications.
- Step 2** Select the rows you would like to save, then click **OK**.
ISC generates the report in the format you selected.
-



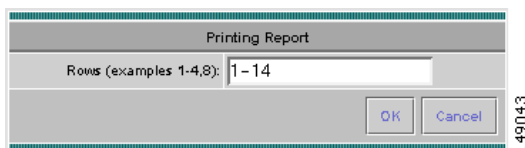
Note

You must have the appropriate application on your system (for example, Acrobat Reader or Excel) to view and save the output.

Printing Reports

Click on the **Print** icon in [Figure 7-59](#), “[Report Output Icons](#),” to bring up a window like the one shown in [Figure 7-61](#).

Figure 7-61 *Print Report*



This window allows you to display the report in a form more appropriate for printing. Select the desired rows, then click **OK**. The results are displayed in your web browser, from which you can print the report.

E-mailing Reports

Click on the **E-mail** icon in [Figure 7-59](#), “[Report Output Icons](#),” to bring up a window like the one shown in [Figure 7-62](#) and then follow these steps.

Figure 7-62 E-mail Report

-
- Step 1** In the To: field (required), specify one or more e-mail addresses to which the report should be sent.
- Step 2** In the From: field (optional), enter an e-mail address you want to appear in the message header. This allows a reply message to be sent to a valid e-mail address.
- Step 3** In the CC: field (optional), enter e-mail addresses for recipients you want to receive copies of this report.
- Step 4** The subject field shows the title of the report being sent. You can overwrite this field to rename the report. This is what appears in the Subject field of the e-mail message.
- Step 5** Select the radio button for the output format (PDF or CSV) in which you want the report sent.
- Step 6** Select the number of rows you want sent.
- Step 7** If applicable, in the Message field, write a message to announce the report, then click **Send**.
-

Invoking Help

Click on the **Help** (?) icon in Figure 7-59, “Report Output Icons,” to link to the ISC documentation set on the Cisco Systems web site:

http://www.cisco.com/en/US/products/sw/netmgts/ps4748/tsd_products_support_series_home.html

From that location, you can choose the type of ISC document you want to see.

Creating Custom Reports

The reports listed in the ISC GUI in the each folder are derived from an underlying configuration file. The file is in XML format. You can access the file in the following location:

\$ISC_HOME/resources/nbi/reports/ISC/<folder_name>_report.xml

where <folder_name> is **Inventory**, **L2**, or **MPLS**.

Each of the available reports (including sample reports) is defined by XML content contained within an `<objectDef name>` start and end tag under **packageDef name = “`<folder_name>`”**. The intervening XML content specifies the title of the report, all allowable filter parameters, outputs, and the default sorting behavior. You can modify existing reports or copy them to use as templates for new reports.

To do this, follow these steps:

-
- Step 1** Stop the ISC server using the **stopall** command. See [Chapter 2, “WatchDog Commands”](#) for information on starting and stopping ISC.
- Step 2** Open the **\$ISC_HOME/resources/nbi/reports/ISC/`<folder_name>`_report.xml** (where: `<folder_name>` is **Inventory, L2, or MPLS**) configuration file using an editing tool of your choice.
- 
-
- Note** You should backup the file before making any changes to it.
-
- Step 3** Depending on your needs, either modify an existing report or copy one and use it as the basis for a new one.
- Step 4** Save the modified **\$ISC_HOME/resources/nbi/reports/ISC/`<folder_name>`_report.xml** file.
- Step 5** Restart the ISC server using the **startwd** command. See [Chapter 2, “WatchDog Commands”](#) for information on starting and stopping ISC.
-

After restarting ISC, the modifications take effect, based on changes you made to the **\$ISC_HOME/resources/nbi/reports/ISC/`<folder_name>`_report.xml** file.



CHAPTER 8

Diagnostics

From the Home window of Cisco IP Solution Center (ISC), which you receive upon logging in, click the **Diagnostics** tab and you receive a window as shown in [Figure 8-1](#), “[Diagnostics Selection](#).”

Figure 8-1 **Diagnostics Selection**



The Cisco MPLS Diagnostics Expert (MDE) application is an automated, workflow-based network management application that troubleshoots and diagnoses problems in Multiprotocol Label Switching (MPLS) VPNs. MDE offers users the capability to reduce the amount of time required to diagnose MPLS-related network outages—in many cases from hours to minutes. It performs diagnostics based on analysis of network failure scenarios, across MPLS access, edge, and core networks. It is equally applicable to both service provider and enterprise “self-deployed” MPLS VPN networks. Network operations center (NOC) support technicians as well as second-line and third-line support can benefit from this product. MDE optionally integrates with the provisioning features of the ISC MPLS VPN component. To diagnose MPLS VPN core problems, Cisco IOS or IOS XR software releases supporting MPLS operations and maintenance (OAM) features including label-switched path (LSP) ping and LSP traceroute are required.

This application is explained in detail in the [Cisco MPLS Diagnostics Expert 2.1 User Guide on ISC 5.0](#).

The [Cisco MPLS Diagnostics Expert 2.1 Failure Scenarios Guide on ISC 5.0](#) provides details of all feature scenarios and observations reported by the MDE application for ISC. It also lists all IOS and IOS XR commands executed by the troubleshooting workflows.

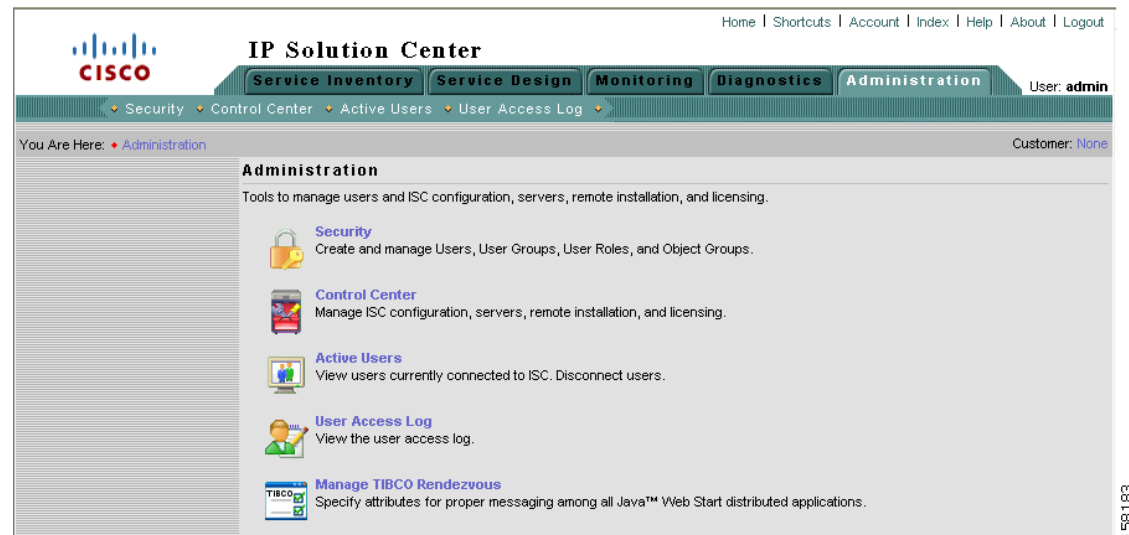


CHAPTER 9

Administration

From the Home window of Cisco IP Solution Center (ISC), which you receive upon logging in, click the **Administration** tab and you receive a window as shown in [Figure 9-1](#), “Administration Selections.”

Figure 9-1 Administration Selections



Then you can choose the following selections:

- [Security, page 9-1](#) Create and manage Users, User Groups, User Roles, and Object Groups
- [Control Center, page 9-21](#) Manage ISC configuration, servers, and licensing
- [Active Users, page 9-30](#) View users currently connected to ISC. Disconnect users.
- [User Access Log, page 9-31](#) View the user access log.
- [Manage TIBCO Rendezvous, page 9-33](#) Specify attributes for proper messaging among all Java™ Web Start distributed applications.

Security

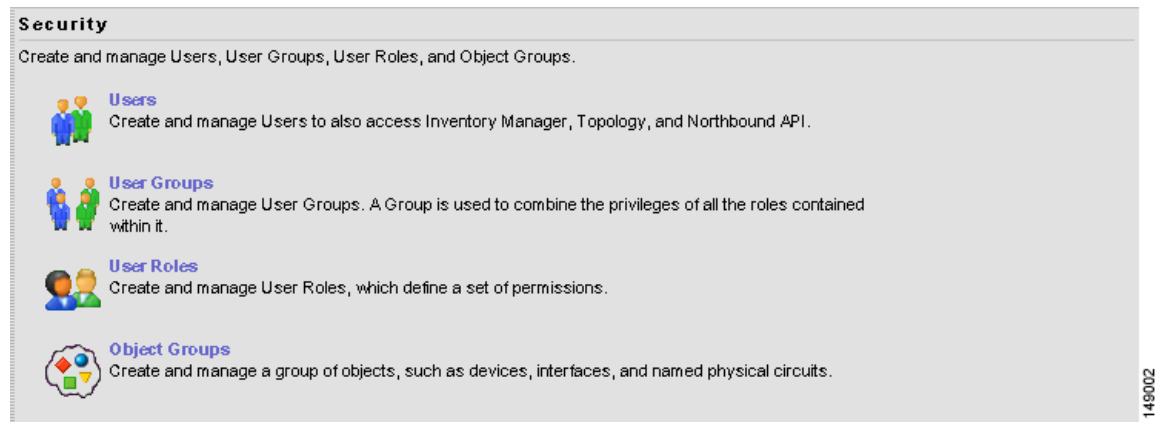
This section describes how system administrators create, edit, and delete users, user groups, user roles, and object groups and how privileges are assigned to these entities.

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**.

Choose **Administration > Security** to access the user management tools. The window shown in [Figure 9-2](#), “**Security Window**,” appears.

Figure 9-2 Security Window



From the Security window, choose the following:

- [Users](#), [page 9-2](#) to manage users
- [User Groups](#), [page 9-7](#) to manage user groups
- [User Roles](#), [page 9-9](#) to manage user roles
- [Object Groups](#), [page 9-15](#) 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 9-18](#).

Users

Choose **Administration > Security > Users** and follow these steps:

-
- Step 1** The window in [Figure 9-3](#), “**Users Window**,” appears.

Figure 9-3 Users Window

Users

Show users with matching

Showing 1 - 1 of 1 record

#	User ID	First Name	Last Name	Work Phone	Mobile Phone
1. ☐	admin	System	Administrator		

Rows per page:

Go to page: of 1

Step 2 The explanations of the buttons are given as follows:

- [Details, page 9-3](#) View a User Detail Report
- [Create, page 9-3](#) Create a new user
- [Copy, page 9-6](#) Make a copy of an existing user and make changes to create a new user
- [Edit, page 9-6](#) Edit selected user
- [Delete, page 9-6](#) Delete selected user(s).

Details

When you click the **Details** button, located at the bottom of [Figure 9-3](#), you receive 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.

Create

When you click the **Create** button, located at the bottom of [Figure 9-3](#), a user with the required privileges can create a new user. Follow these steps:

- Step 1** Choose **Administration > Security > Users**.
- Step 2** Click the **Create** button and the window shown in [Figure 9-4](#), "Create/Copy/Edit Users Window," appears.

Figure 9-4 Create/Copy/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 v
Rows per page:	10 v
Logging Level:	Warning v
Initial Screen:	Home v
Save Cancel	

116080

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:
 - ISC requires a non-blank password.
 - ISC passwords must be a minimum of five characters and no practical maximum length.
 - ISC does not employ any password restrictions or complexity rules; use good judgment in determining passwords.
 - ISC passwords are encrypted when stored in the repository.
 - ISC passwords do not expire.
 - ISC monitors inactivity and auto-logout per the settings defined in the Dynamic Component Properties Library (DCPL) properties for **repository/rbac**, see [Appendix C, “Property Settings.”](#)
- **Verify Password** (required) Confirm by re-entering the selected password.

- **Permission for Others** Check 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 is 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, check the check box next to each group to which you want to add this user. 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 9-8).
- **Assigned Roles** Click **Edit** and you receive a list of the roles. You can filter this list. From the selected roles, check the check box next to each role to which you want to assign this 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 list 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.
- **Email** (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 list 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, 100, 500, 1000, and 2500.
- **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**, and **Diagnostics**. This is a way to specify the first window you will see after logging in.

Step 6 Click **Save**. [Figure 9-3](#) reappears with the new user listed.

Copy

The **Copy** button, located at the bottom of [Figure 9-3](#), 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** Choose **Administration > Security > Users**.
 - Step 2** Check 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 9-4](#), “[Create/Copy/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 9-3](#).
 - Step 6** Click **Save** and you will return to [Figure 9-3](#). 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 9-3](#), allows a user with the required privileges to edit user-specific information. Follow these steps:

-
- Step 1** Choose **Administration > Security > Users**.
 - Step 2** Check 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 9-4](#), “[Create/Copy/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 the “[Create](#)” section on [page 9-3](#).
 - Step 5** Click **Save**. [Figure 9-3](#) reappears with the edited user listed.
-

Delete

The **Delete** button, located at the bottom of [Figure 9-3](#), allows a user with the required privileges to delete user-specific information. Follow these steps:

-
- Step 1** Choose **Administration > Security > Users**.
 - Step 2** Check the check box(es) for the row(s) of the user(s) you want to delete.
 - Step 3** Click the **Delete** button and a window as shown in [Figure 9-5](#), “[Users Confirm Delete](#)” appears.

Figure 9-5 Users Confirm Delete

Confirm Delete		
Showing 1 - 1 of 1 record		
#	User ID	Full Name
1.	new1	Jane Doe

Rows per page: 10 Go to page: 1 of 1 Go

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 9-3](#), “[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, choose **Administration > Security > User Groups** and follow these steps:

- Step 1** The window in [Figure 9-6](#), “[User Groups Window](#)” appears.

Figure 9-6 User Groups Window

User Groups

Show groups with Name matching * Find

Showing 0 of 0 records

#	Name	Description

Rows per page: 10 Go to page: 1 of 1 Go

Create Edit Delete

- Step 2** The explanations of the remainder of the buttons is given as follows:
- [Create, page 9-8](#) Create a new user group
 - [Edit, page 9-8](#) Edit selected user group
 - [Delete, page 9-9](#) Delete selected user group(s)

Create

The **Create** button, located at the bottom of [Figure 9-6](#), allows a user with the required privileges to create a user group. Follow these steps:

-
- Step 1** Choose **Administration > Security > User Groups**.
- Step 2** Click the **Create** button and the window shown in [Figure 9-7](#), “Create/Edit User Groups Window,” appears.

Figure 9-7 Create/Edit User Groups Window

The screenshot shows a window titled "Create/Edit User Groups Window". It contains the following fields and controls:

- Name :** A text input field with a small "x" icon in the top right corner.
- Description:** A larger text area for a description.
- Roles:** A list box with an **Edit** button to its right.
- Users:** A list box with an **Edit** button to its right.
- At the bottom right, there are **Save** and **Cancel** buttons.

937 47

- 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, check the check box next to each role you want to attach 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, check the check box next to each user you want to attach to this user group. Then click **OK**. You can repeat this procedure if you want to change your selection.
- Step 4** Click **Save**. [Figure 9-6](#) reappears with the new user group listed.
-

Edit

The **Edit** button, located at the bottom of [Figure 9-6](#), allows a user with the required privileges to edit user group-specific information. Follow these steps:

-
- Step 1** Choose **Administration > Security > User Groups**.
- Step 2** Check 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 9-7](#), “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 9-8](#).
- Step 5** Click **Save**. [Figure 9-6](#) reappears with the edited user group list.

Delete

The **Delete** button, located at the bottom of [Figure 9-6](#), allows a user with the required privileges to delete user group-specific information. Follow these steps:

- Step 1** Choose **Administration > Security > User Groups**.
- Step 2** Check the check box(es) for the row(s) of the user group(s) you want to delete.
- Step 3** Click the **Delete** button and a window as shown in [Figure 9-8](#), “User Groups Confirm Delete,” appears.

Figure 9-8 User Groups Confirm Delete

#	Name	Description
1.	newgroup1	

Showing 1 - 1 of 1 record

Rows per page: 10 Go to page: 1 of 1 Go

Delete Cancel

- Step 4** Click **Delete** to continue the process of deleting information for the specified user group(s). Otherwise click **Cancel**.
- Step 5** [Figure 9-6](#), “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 a 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, choose **Administration > Security > User Roles** and follow these steps:

Step 1 The window in [Figure 9-9](#), “User Roles Window,” appears.

Figure 9-9 User Roles Window

User Roles		
View roles with Name matching * Find		
Showing 1 - 25 of 25 records		
#	☐	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.	☐	DiscoveryRole ISC predefined role. It has the permission to manage Inventory and deploy Discovery Request.

The predefined roles 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 The explanations of the buttons is as follows:

- [Create, page 9-11](#) Create a new user role
- [Copy, page 9-13](#) Copy selected user role

- [Edit, page 9-14](#) Edit selected user role
- [Delete, page 9-14](#) Delete selected user role(s)

Create

The **Create** button, located at the bottom of [Figure 9-9](#), allows a user with the required privileges to create a new user role. Follow these steps:

- Step 1** Choose **Administration > Security > User Roles**.
- Step 2** Click the **Create** button and a window comprised of [Figure 9-10](#), “Create/Copy/Edit User Roles Window (Top),” and [Figure 9-11](#), “Create/Copy/Edit User Roles Window (Bottom),” appears.

Figure 9-10 *Create/Copy/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

116070

Figure 9-11 Create/Copy/Edit User Roles Window (Bottom)

Resource	All	Create	View	Modify	Delete
Persistent Task	☐	☐	☐	☐	☐
SAA Probe	☐	☐	☐	☐	☐
Workflow	☐	☐	☐	☐	☐
Device	☐	☐	☐	☐	☐
ISC Host	☐	☐	☐	☐	☐
Customer	☐	☐	☐	☐	☐
Provider	☐	☐	☐	☐	☐
PE	☐	☐	☐	☐	☐
CPE	☐	☐	☐	☐	☐
MPLS Policy	☐	☐	☐	☐	☐
MPLS Service Request	☐	☐	☐	☐	☐
L2VPN (P2P) Policy	☐	☐	☐	☐	☐
L2VPN Service Request	☐	☐	☐	☐	☐

211165

Step 3 Enter the following information in [Figure 9-10](#):

- **Name** (required) Enter the name of this new user role.
- **Enable Object Group Association** The default is that this check box is unchecked. In this case, **Parent Role**, **Customer**, and **Provider** are enabled and **Object Groups** is not enabled. A complete list of resources appears, as shown in the example in [Figure 9-9](#). If you check this check box, **Parent Role**, **Customer**, and **Provider** are not enabled and **Object Groups** is enabled. A window, as shown in [Figure 9-11](#), 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 9-9](#), 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, check the check box(es) for the object group(s) you want 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 is 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 9-9](#).

- **Users** (optional) Click **Edit** and a list of the existing users appears. You can filter this list. From the selected users, check the check box(es) for the user(s) you want assigned 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, check the check box(es) for the user group(s) you want assigned to this role. Then click **OK**. You can repeat this procedure if you want to change your selection.

Step 4

In [Figure 9-11](#), 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.

**Note**

Template controls the template manager functions and **Associate Template** controls the ability to associate templates with service requests. If you choose **Create** permission in **Template**, you also automatically receive **Modify** permission. If you choose any or all permissions in **Associate Template**, you automatically turn on the **View** permission in **Template**.

Step 5

Click **Save**. [Figure 9-9](#) reappears with the new user role listed.

Copy

The **Copy** button, located at the bottom of [Figure 9-9](#), 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

Choose **Administration > Security > User Roles**.

Step 2

Check 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 9-10](#), “**Create/Copy/Edit User Roles Window (Top)**,” and [Figure 9-11](#), “**Create/Copy/Edit User Roles Window (Bottom)**” appears.

- Step 4** The required entry is 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 9-11.
- Step 6** Click **Save** and you will return to [Figure 9-9](#). 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 9-9](#), allows a user with the required privileges to edit user role-specific information. Follow these steps:

- Step 1** Choose **Administration > Security > User Roles**.
- Step 2** Check 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 9-10](#) and [Figure 9-11](#) 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 9-11.
- Step 5** Click **Save**. [Figure 9-9](#) reappears with the edited user roles listed.

Delete

The **Delete** button, located at the bottom of [Figure 9-9](#), allows a user with the required privileges to delete user role-specific information. Follow these steps:

- Step 1** Choose **Administration > Security > User Roles**.
- Step 2** Check the check box(es) for the row(s) of the user role(s) you want to delete.
- Step 3** Click the **Delete** button and a window as shown in [Figure 9-12](#), “[User Roles Confirm Delete](#),” appears.

Figure 9-12 *User Roles Confirm Delete*

Confirm Delete		
#	Name	Description
1.	newrole1	Copy of ISC predefined role. It has the permission to manage Inventory and deploy L2VPN Service Request.

Showing 1 - 1 of 1 record

Rows per page: 20

Go to page: 1 of 1

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 9-9, “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 an Object Group or it can be associated with a grouping of Customer and Provider, but it cannot be associated with both of these. The association with a grouping of Customer and Provider is either with Customer(s), with Provider(s), or with Customer(s) and Provider(s). When a role is associated with Object Group(s), you can only define permissions for PE, CE, and NPC. Permissions on interfaces is implied 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 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 9-18.

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 Named Physical Circuits (NPCs), define a role to be associated with Object Group(s), Device, CE, PE, and NPC.

To access the Object Groups window, choose **Administration > Security > Object Groups** and follow these steps:

- Step 1** The window in Figure 9-13, “Object Groups Window,” appears.

Figure 9-13 Object Groups Window

- Step 2** The explanations of the buttons is as follows:
- [Create, page 9-11](#) Create a new object group
 - [Edit, page 9-14](#) Edit a selected object group
 - [Delete, page 9-14](#) Delete selected object group(s)

Create

The **Create** button, located at the bottom of [Figure 9-13](#), allows a user with the required privileges to create a new object group. Follow these steps:

- Step 1** Choose **Administration > Security > Object Groups**.
- Step 2** Click the **Create** button and the window [Figure 9-14](#), “**Create/Edit Object Group Window**,” appears.

Figure 9-14 Create/Edit Object Group Window

The screenshot shows a web-based form titled "Create/Edit Object Group Window". It contains the following elements:

- Name:** A text input field with a red asterisk indicating it is required.
- Description:** A large text area.
- PE Group Members:** A section containing a table with columns "#", "Name", and "Interface Members". Below the table are pagination controls: "Rows per page: 10" (dropdown), "Go to page: 1 of 1" (input), and "Go" (button).
- CE Group Members:** A section containing a table with columns "#", "Name", and "Interface Members". Below the table are pagination controls: "Rows per page: 10" (dropdown), "Go to page: 1 of 1" (input), and "Go" (button).
- NPC Group Members:** A section containing a table with columns "#", "Name", and "Interface Members". Below the table are pagination controls: "Rows per page: 10" (dropdown), "Go to page: 1 of 1" (input), and "Go" (button).
- Buttons:** "Save" and "Cancel" buttons at the bottom right.
- Note:** A note at the bottom left states: "Note: * - Required Field".

- Step 3** Enter the following information in [Figure 9-14](#):
- **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, check the check box(es) 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 9-14](#), “**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, check the check box(es) 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 is empty. All existing interfaces for each of the CE Groups in the **Name** column 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 9-14](#), “[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 NPCs appears. You can filter this list. From the selected NPCs, check the check box(es) 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 return to [Figure 9-14](#), “[Create/Edit Object Group Window](#),” and the **Name** for each NPC Group Member appears.

Step 4 Click **Save**. [Figure 9-14](#) reappears with the new object group listed.

Edit

The **Edit** button, located at the bottom of [Figure 9-14](#), allows a user with the required privileges to edit object group-specific information. Follow these steps:

-
- Step 1** Choose **Administration > Security > Object Groups**.
- Step 2** Check 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 9-13](#), 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 9-16](#).
- Step 5** Click **Save**. [Figure 9-13](#) reappears with the edited object groups listed.
-

Delete

The **Delete** button, located at the bottom of [Figure 9-13](#), allows a user with the required privileges to delete object group-specific information. Follow these steps:

-
- Step 1** Choose **Administration > Security > Object Groups**.
- Step 2** Check the check box(es) for the row(s) of the object group(s) you want to delete.
- Step 3** Click the **Delete** button and a window as shown in [Figure 9-15](#), “[Delete Object Groups Confirm Delete](#),” appears.

Figure 9-15 Delete Object Groups Confirm Delete

#	Name	Description
1.	objgp2	
2.	objgp3	

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

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 9-13, “Object 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 Design Example

This section gives an example situation, an illustration that shows this setup, and steps on how to setup this design:

- [Example, page 9-18](#)
- [Illustration of Setup, page 9-19](#)
- [Steps to Set Up Example, page 9-20](#)

Example

This section explains an example data center for which the following sections, [“Illustration of Setup” section on page 9-19](#) and [“Steps to Set Up Example” section on page 9-20](#) 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.

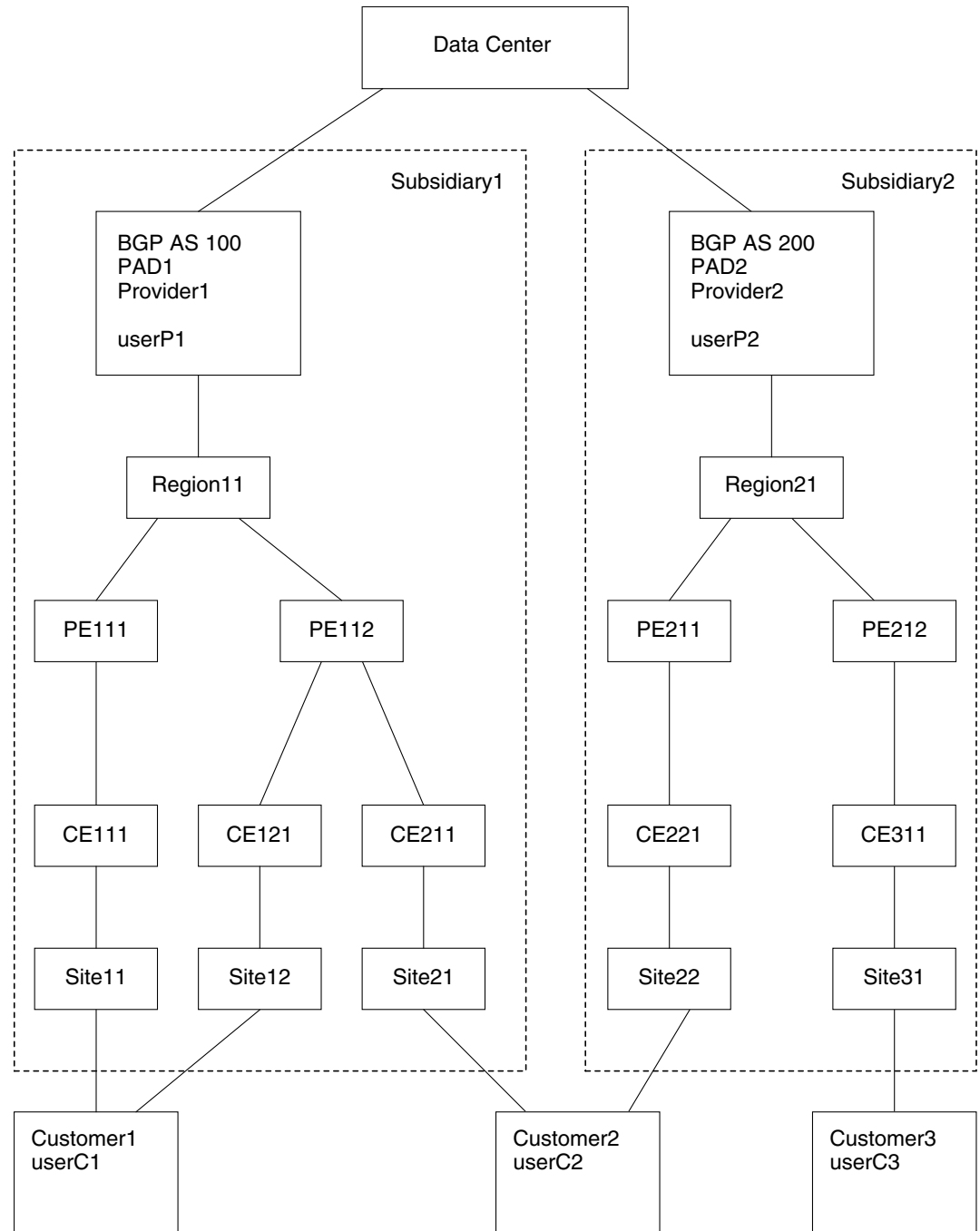
Inside a PAD, there are Customers with sites and VPNs with only local significance. Also, the IP addressing should be defined per PAD.

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 9-16, “Contents in Example,” shows the setup described in the “Example” section on page 9-18.

Figure 9-16 *Contents in Example*



111821

Steps to Set Up Example

This section explains the steps to create the example explained in the “[Example](#)” section on page 9-18 and shown in the “[Illustration of Setup](#)” section on page 9-19.

-
- Step 1** Create the following Object Groups (see the “[Create](#)” section on page 9-16, 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 9-11, 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 9-9.
- 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 9-2.
- 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 define collection zones; and how to install license keys.

Choose **Administration > Control Center** and you go to the default page of **Hosts** in the TOC, as shown in [Figure 9-17](#), “[Control Center > Hosts](#).”

Figure 9-17 *Control Center > Hosts*

#	Name	Server	Start Time	Stop Time	Running
1.	smiley-ultra.cisco.com	Master	Jul 18 11:50:57 AM PDT	UNKNOWN	Yes

From **Administration > Control Center**, you have the following three choices in the TOC:

- [Hosts, page 9-21](#) **Hosts** allows you to manage the various servers.
- [Collection Zones, page 9-26](#) **Collection Zones** are the means of associating the Master server with network devices.
- [Licensing, page 9-28](#) **Licensing** is where you install license keys, which is the only way to access services and APIs.

Hosts

Choose **Administration > Control Center > Hosts**.

A window as shown in [Figure 9-17](#) appears.



Note

Only the **Logs** buttons are enabled by default when there is no host selected. When the host is selected by checking the check box, the Logs buttons is disabled and the other buttons are enabled.

Click any of the buttons and proceed as follows:

- [Details, page 9-22](#) Available only when the host system is chosen.
- [Config, page 9-23](#) Available only when the host system is chosen.
- [Servers, page 9-24](#) Available only when the host system is chosen.

- [Watchdog, page 9-25](#) Available only when the host system is chosen.
- [Logs, page 9-26](#) Available only when no host system selection is made.

Details

For details about a chosen host, follow these steps:

- Step 1** Choose a host by checking the check box to the left of the hostname and then click the **Details** button.
- Step 2** You receive a window as shown in [Figure 9-18](#), “Host Details.” This shows the details about the chosen host.

Figure 9-18 Host Details

Host Details

Host: efgh-ultra10.cisco.com	
General	
Active:	Yes
Image:	isc3.0-20030406.00.Q
Registered Date:	May 21 03:29:10 PDT
UnRegistered Date:	
Install Location:	/disk2/opt/iscadm/isc3
Install Time:	2003-03-19 16:59:07.
Locations	
Server Logs:	/disk2/opt/iscadm/isc3
Task Logs:	/disk2/opt/iscadm/isc3
Temporary:	/disk2/opt/iscadm/isc3
Disk Stats	
Path:	/disk2/opt/iscadm/isc3
Total Disk Space:	19146 MB
Free Disk Space:	12810 MB; 66% Free
Path:	/disk2/opt/iscadm/isc3
Total Disk Space:	19146 MB
Free Disk Space:	12810 MB; 66% Free
Health Stats	
Last Heartbeat:	
Last Heartbeat Status:	
Last Heartbeat Duration:	
Collection Zones	
OK	

- Step 3** Click **OK** and you return to [Figure 9-17](#).

Config

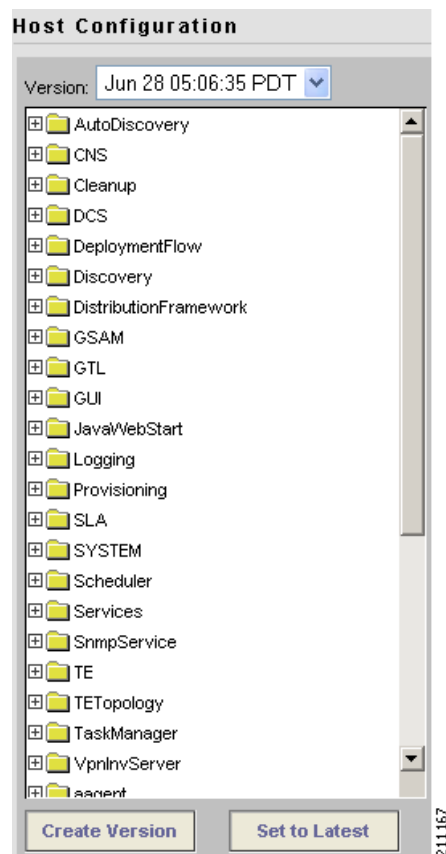
To view or change the Dynamic Component Properties Library (DCPL) properties, which replaces the csm.properties file for VPNSC, follow these steps:


Note

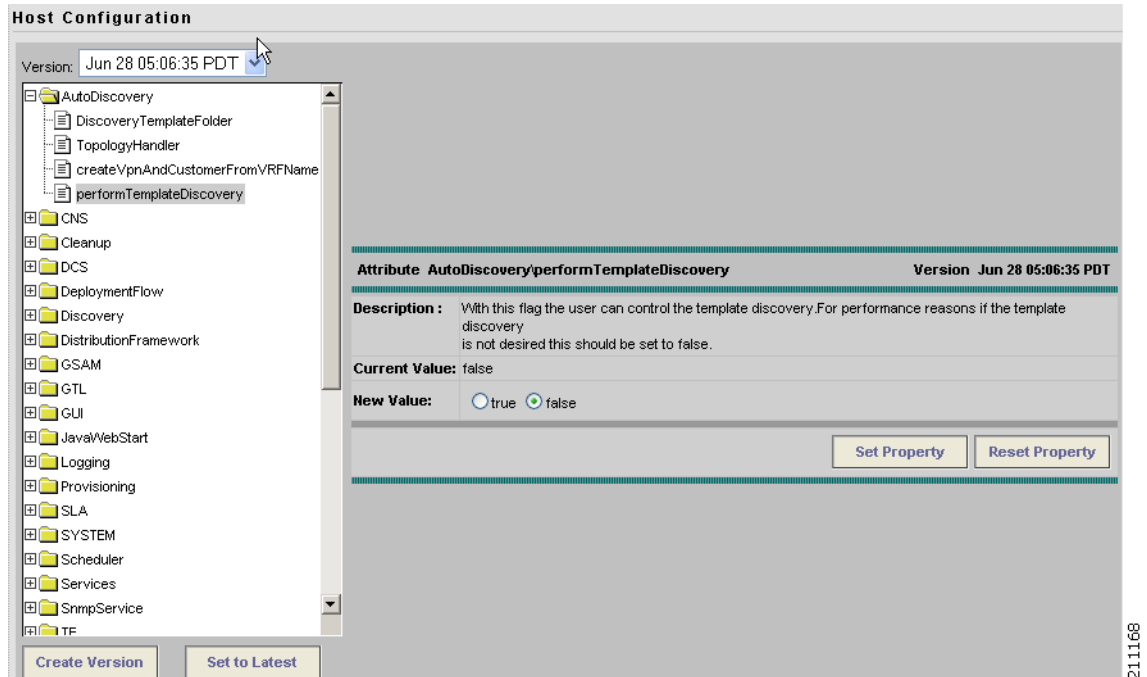
csm.properties in VPNSC cannot be migrated to DCPL settings in ISC.

- Step 1** From [Figure 9-17 on page 9-21](#), check a check box next to a hostname for which you want to know the existing properties and then click the **Config** button.
- Step 2** A window as shown in [Figure 9-19, “Properties,”](#) appears. It is a list of all the folders with all the properties. See [Appendix C, “Property Settings”](#) for a list of all the properties with explanations, defaults, and ranges/rules. If you do not know the property name, you can use a key word and do a Find on the pdf version of this appendix.

Figure 9-19 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 9-20, “Properties Detail Example.”](#)

Figure 9-20 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 list 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, follow these steps:

- Step 1** From [Figure 9-17 on page 9-21](#), check a check box next to a hostname for which you want to know the server statistics and then click the **Servers** button.
- Step 2** A window as shown in [Figure 9-21](#), “**Servers**,” appears.

Figure 9-21 Servers

Servers

[Refresh](#)

Showing 1 - 10 of 10 records

#	☐	Name	State	Generation	Start Time	PID	Successful Heartbeats	Missed Heartbeats
1.	☐	worker	started	1	Jul 18 11:51:07 AM PDT	16732	1460	0
2.	☐	dispatcher	started	1	Jul 18 11:51:07 AM PDT	16733	1470	0
3.	☐	discovery	started	1	Jul 18 11:51:07 AM PDT	16737	1464	0
4.	☐	lockmanager	started	1	Jul 18 11:51:07 AM PDT	16734	1457	0
5.	☐	nspoller	started	1	Jul 18 11:51:01 AM PDT	0	1462	0
6.	☐	scheduler	started	1	Jul 18 11:54:45 AM PDT	16750	1469	0
7.	☐	httpd	started	2	Jul 18 11:55:14 AM PDT	16751	1451	0
8.	☐	dbpoller	started	1	Jul 18 11:51:01 AM PDT	0	1472	0
9.	☐	rgserver	started	1	Jul 18 11:56:49 AM PDT	16762	1463	0
10.	☐	cnsserver	started	1	Jul 18 11:51:07 AM PDT	16731	1467	0

Rows per page: 10

- Step 3** Check 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 9-21](#).
- 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 9-21](#), you return to [Figure 9-17 on page 9-21](#).

Watchdog

To view the log information about WatchDog, follow these steps:

- Step 1** From [Figure 9-17 on page 9-21](#), check a check box next to a hostname for which you want to know the WatchDog logs and then click the **Watchdog** button.
- Step 2** A window as shown in [Figure 9-22](#), “**WatchDog Logs**,” appears.

Figure 9-22 WatchDog Logs

Name	Size	Last Modified
watchdog.0	300721	Thursday, October 27, 2005 4:26:26 PM PDT

- 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 9-22](#).
- Step 4** You can repeat the process in [Step 3](#) or click **OK** to return to [Figure 9-17 on page 9-21](#).

Logs

To view install and uninstall logs for the Master server, follow these steps:

- Step 1** From [Figure 9-17 on page 9-21](#), be sure that no check boxes are checked.
- Step 2** Click the **Logs** drop-down list 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 9-17 on page 9-21](#).

Collection Zones

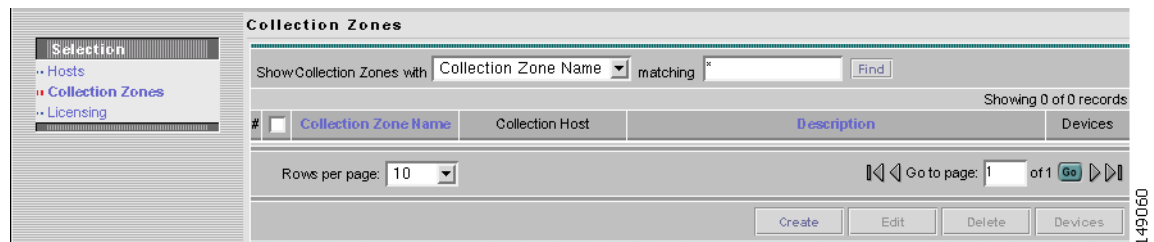
Choose **Administration > Control Center**.

A collection zone is a geographical grouping of devices. Each collection zone is associated with the Master server that collects data from its devices. However, a Master server can service multiple collection zones.

To define collection zones, follow these steps:

- Step 1** From the Control Center, choose **Collection Zones** from the TOC in the left column, and a window as shown in [Figure 9-23](#), “[Choose Control Center > Collection Zones](#)” appears.

Figure 9-23 Choose Control Center > Collection Zones



- Step 2** To **Create** a collection zone, proceed to [Step 3](#). To **Edit** a collection zone, proceed to [Step 6](#). To **Delete** a collection zone, proceed to [Step 8](#). To display the **Devices**, proceed to [Step 11](#).
- Step 3** From [Figure 9-23](#), without checking any check boxes, click the **Create** button.
- Step 4** A window as shown in [Figure 9-24](#), “[Create Collection Zone](#),” appears.

Figure 9-24 Create Collection Zone

Create Collection Zone

Name *

Description: Created on Sat Nov 19 00:11:15 PST 2005
By efgh-ultra.cisco.com

Collection Host: efgh-ultra.cisco.com

Save Cancel

Note: * - Required Field

149155

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 list if you want to select a different collection host.

- Step 5** Click **Save**. [Figure 9-23](#) reappears, the newly created collection zone is added, and a Status appears with a green check mark for **Succeeded**. You can repeat [Step 3](#) to [Step 5](#) to create another collection zone. For **Edit**, proceed to [Step 6](#). For **Delete**, proceed to [Step 8](#). To display the **Devices**, proceed to [Step 11](#).
- Step 6** To edit a collection zone, in [Figure 9-23](#), check the check box for the collection zone you want to edit and then click the **Edit** button.
- Step 7** A window as shown in [Figure 9-24](#) appears. Follow the instructions in [Step 4](#) and [Step 5](#).
- Step 8** To delete a collection zone, in [Figure 9-23](#), check one or more check boxes for the collection zone(s) you want to delete. Then click the **Delete** button.
- Step 9** A Confirm Delete window appears, to give you a chance to click **Cancel** and not delete, or to click **OK** and delete.
- Step 10** [Figure 9-23](#) reappears and the collection zone is removed. You can repeat [Step 8](#) and [Step 9](#) to delete more collection zones, you can proceed to [Step 3](#) to create a collection zone, you can proceed to [Step 6](#) to edit a collection zone, or you can proceed to [Step 11](#) to display and assign **devices**.
- Step 11** To display, add, or delete devices, in [Figure 9-23](#), check a check box for the desired collection zone. Then click the **Devices** button.
- Step 12** A window appears as shown in [Figure 9-25](#), “[Collection Zone Devices](#).” This window shows the current devices assigned to the selected collection zone.

Figure 9-25 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 13** 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 14** 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 15** [Figure 9-25](#) reappears with the updated device information for the selected collection zone.
- Step 16** When [Figure 9-25](#) has all the devices you want, click **OK** and [Figure 9-23](#) reappears with the updated information.

Licensing

Choose **Administration > Control Center**.

To install license keys, follow these steps:

- Step 1** From **Control Center**, choose **Licensing** from the TOC in the left column, as shown in [Figure 9-26](#), “Choose Control Center > Licensing.”

Figure 9-26 Choose Control Center > Licensing

Selection

- Hosts
- Collection Zones
- Licensing

Hosts

Refresh

Showing 1 - 1 of 1 record

#	Name	Role	Start Time	Stop Time	Running
1.	efgh-ultra.cisco.com	Master	Oct 27 04:19:56 PM PDT	UNKNOWN	Yes

Rows per page: 10

Go to page: 1 of 1 Go

Details Config Servers Watchdog Install Uninstall Logs

- Step 2** From the **Installed Licenses** table, click the **Install** button, as shown in [Figure 9-27](#), “**Installed Licenses**.” The Installed Licenses table explains the current statistics. The columns of information tell the **Type** of license keys you have installed (which can include ACTIVATION, API-L2VPN, API-L3MPLS, L2VPN, L3MPLS/VPN, MPLSDIAG, TE, TE/BRG, TE/RG, VPLS, VPN); the **Size**, which is valid for the **ACTIVATION** (licensed maximum global count of services), **TE** (number of TE-enabled nodes), 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. All of these licenses *must* be installed to have access to all the Cisco ISC TEM features, including Planning Tools for protection planning (backup tunnels). The **TE** license serves as an activation license for the maximum number of TE-enabled nodes to be managed by TEM (you purchase licenses and upgrade licenses based on a range of nodes); 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 9-27 *Installed Licenses*

Installed Licenses			
Type	Size	Usage	Date Updated
ACTIVATION	25		2005-11-18 23:42
API-L2VPN			2005-11-18 23:42
API-L3MPLS			2005-11-18 23:42
L2VPN			2005-11-18 23:42
L3MPLS/VPN			2005-11-18 23:42
MPLSDIAG			2005-11-18 23:42
QOS			2005-11-18 23:42
TE	25		2005-11-18 23:42
TE/BRG			2005-11-18 23:42
TE/RG			2005-11-18 23:42
VPLS			2005-11-18 23:42
VPN	50	6	2005-11-18 23:42
			Refresh Install

149156

- Step 3** In the resulting window, as shown in [Figure 9-28](#), “**Enter License Key**,” enter a **License Key** that you received on your *Right to Use* paperwork with your product.

Figure 9-28 Enter License Key

Install a License Key

License Key *

Save Cancel

Note: * - Required Field

- Step 4** Click **Save**. Your newly installed license appears in an updated version of the Installed License table, as shown in [Figure 9-27](#), “Installed Licenses.”
- 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.

Choose **Administration > Active Users** and follow these steps:

- Step 1** After you choose **Administration > Active Users**, a window that shows the currently logged users appears, as shown in [Figure 9-29](#), “Active Users.”

Figure 9-29 Active Users

Active Users

Show Active Users with User ID matching * Find

Showing 1 - 1 of 1 record

#	User ID	Device Host Name	Login Time	Last Access Time
1.	admin	efgh-ultra.cisco.com	8:41:53 PM PST 11/18/05	12:33:52 AM PST 11/19/05

Rows per page: 10 Go to page: 1 of 1 Go

Auto Refresh: ☒ Disconnect

- Step 2** In [Figure 9-29](#), if you have the privileges of **SysAdmin** or **UserAdmin**, you can disconnect one or more users. Check the check box next to each user you want to disconnect. 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.

Choose **Administration > User Access Log** and follow these steps:

- Step 1** After you choose **Administration > User Access Log**, a window appears as shown in [Figure 9-29](#), “[Active Users](#).”

Figure 9-30 User Access Log Viewer with Simple Filter

#	Date	Time	User Name	Origin Host	Action	Object	Severity	Activity	Message
1.	2005/11/18	23:34:49	backendadm		Logon	User	INFO	SecurityActivity	Login successfully.
2.	2005/11/18	23:30:56	backendadm		Logon	User	INFO	SecurityActivity	Login successfully.
3.	2005/11/18	22:53:43	admin	efgh-ultra.cisco.com	Delete	Role	INFO	SecurityActivity	Role newrole1 (id=265810285) is deleted.
4.	2005/11/18	22:49:15	admin	efgh-ultra.cisco.com	Create	Role	INFO	SecurityActivity	Role newrole1 (id=265810285) is created.
5.	2005/11/18	22:10:38	admin	efgh-ultra.cisco.com	Create	Group	INFO	SecurityActivity	Group newgroup1 (id=1203533294) is created.
6.	2005/11/18	21:46:26	admin	efgh-ultra.cisco.com	Modify	Role	INFO	SecurityActivity	Role SysAdminRole (id=-1234592039) is modified.
7.	2005/11/18	21:46:25	admin	efgh-ultra.cisco.com	Create	User	INFO	SecurityActivity	User new1 (id=1794273524) is created.
8.	2005/11/18	21:45:22	admin	efgh-ultra.cisco.com	Delete	User	INFO	SecurityActivity	User new1 (id=1794273524) is deleted.
9.	2005/11/18	21:44:59	admin	efgh-ultra.cisco.com	Modify	Role	INFO	SecurityActivity	Role SysAdminRole (id=-1234592039) is modified.
10.	2005/11/18	21:44:58	admin	efgh-ultra.cisco.com	Create	User	INFO	SecurityActivity	User new1 (id=1794273524) is created.

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 9-31](#), “**User Access Log Viewer with Advanced Filter**,” appears.

Figure 9-31 *User Access Log Viewer with Advanced Filter*

User Access Log Viewer

☐ Simple Filter ☒ Advanced Filter Find

Date: Action:

User Name: Severity:

Device Host Name: Activity:

Service Requests Select/Deselect

Showing 1 - 10 of 246 records

#	Date	Time	User Name	Origin Host	Action	Object	Severity	Activity	Message
1.	2005/11/18	23:34:49	back_endadm		Logon	User	INFO	SecurityActivity	Login successfully.
2.	2005/11/18	23:30:56	back_endadm		Logon	User	INFO	SecurityActivity	Login successfully.
3.	2005/11/18	22:53:43	admin	efgh-ultra.cisco.com	Delete	Role	INFO	SecurityActivity	Role newrole1 (id=265810285) is deleted.
4.	2005/11/18	22:49:15	admin	efgh-ultra.cisco.com	Create	Role	INFO	SecurityActivity	Role newrole1 (id=265810285) is created.
5.	2005/11/18	22:10:38	admin	efgh-ultra.cisco.com	Create	Group	INFO	SecurityActivity	Group newgroup1 (id=1203533294) is created.
6.	2005/11/18	21:46:26	admin	efgh-ultra.cisco.com	Modify	Role	INFO	SecurityActivity	Role SysAdminRole (id=-1234592039) is modified.
7.	2005/11/18	21:46:25	admin	efgh-ultra.cisco.com	Create	User	INFO	SecurityActivity	User new1 (id=1794273524) is created.
8.	2005/11/18	21:45:22	admin	efgh-ultra.cisco.com	Delete	User	INFO	SecurityActivity	User new1 (id=1794273524) is deleted.
9.	2005/11/18	21:44:59	admin	efgh-ultra.cisco.com	Modify	Role	INFO	SecurityActivity	Role SysAdminRole (id=-1234592039) is modified.
10.	2005/11/18	21:44:58	admin	efgh-ultra.cisco.com	Create	User	INFO	SecurityActivity	User new1 (id=1794273524) is created.

Rows per page: 10 Go to page: 1 of 25

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 *.

- **Device Host Name** Enter the beginning characters of the specific **Host Name** you want to view followed by a *.
 - **Action** Click the drop-down list 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 list and choose from: **UNKNOWN**; **INFO**; **WARNING**; **ERROR**. If you decide not to use this filter, just keep *.
 - **Activity** Click the drop-down list and choose from: **UNKNOWN**; **SecurityActivity**; or **UserActivity**. The result is that only the log information matching the entered filter appears.
- Step 7** **Service Requests** has a selection of **Select/Deselect**. Click this and you receive a list of Service Requests in the system from which you can check check box(es) for the User Access Log to handle. Then click the **Select** button. These Service Requests then appear on [Figure 9-31](#).
- Step 8** To exit this log report, choose another feature from the main product tabs.

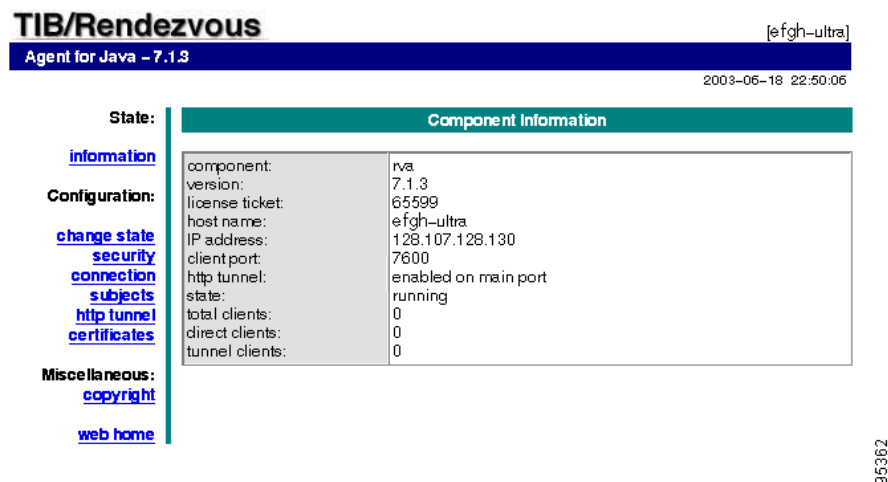
Manage TIBCO Rendezvous

The only reason you would ever use this functionality is if you change the TIBCO ports for TIBCO Rendezvous Agent (rva) or TIBCO Rendezvous Routing Daemon (rvrd) after installation. The changes being made here only affect the topology tool, a Java WebStart application.

Choose **Administration > Manage TIBCO Rendezvous** and follow these steps:

- Step 1** After you choose **Administration > Manage TIBCO Rendezvous**, a window appears as shown in [Figure 9-32](#), “**TIBCO Rendezvous**.”

Figure 9-32 *TIBCO Rendezvous*



- Step 2** From [Figure 9-32](#), 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 9-32](#).
- Step 3** In [Figure 9-32](#), when you click **connection**, a window such as [Figure 9-33](#), “**Connection Configuration**,” appears.

Figure 9-33 Connection Configuration

Connection Configuration	
Accept Client Connections on Listen Port:	7600
TIB/Rendezvous Daemon Connection:	
service:	7530
network:	
daemon:	
Submit	Reset

95391

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 **rverd** port number from the existing value, change the **service** field to your new rverd port number for ISC. Then click **Submit**. Then [Figure 9-33](#) 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 9-32](#), 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-5.0.1/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 the topology tool, these changes are in effect.



APPENDIX **A**

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 the [Cisco IP Solution Center Installation Guide, 5.0](#).

This appendix includes the following sections. Implement these sections in sequence:



Note

The “[Using Plug-and-Play](#)” section on [page A-7](#) 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-7](#)

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** Choose **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**

The screenshot shows the 'Devices' window with a search bar at the top. Below the search bar, it says 'Showing 1 - 8 of 8 records'. The table below lists 8 devices, all of type 'Cisco IOS Device'.

#	☐	Device Name	Management IP Address	Type	Parent Device Name
1.	☐	pe1		Cisco IOS Device	
2.	☐	pe3		Cisco IOS Device	
3.	☐	sw2		Cisco IOS Device	
4.	☐	sw3		Cisco IOS Device	
5.	☐	sw4		Cisco IOS Device	
6.	☐	ce3		Cisco IOS Device	
7.	☐	ce8		Cisco IOS Device	
8.	☐	ce13		Cisco IOS Device	

At the bottom, there is a 'Rows per page' dropdown set to 10, a 'Go to page' field set to 1 of 1, and buttons for 'Create', 'Edit', 'Delete', 'Config', 'E-mail', and 'Copy'.

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' with a 'General' tab. It contains four input fields: 'Device Host Name *', '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**. The **Description** field is optional. 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 Choose **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 Device**.

A window appears as shown in [Figure A-3, “Create Cisco Device Window.”](#)

Figure A-3 Create Cisco Device Window

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) ▾
OS:	IOS ▾
SNMP Version:	Default (SNMP v1/v2c) ▾
SNMP v1/v2c	
Community String RO:	
Community String RW:	
Additional Properties:	Show
Save Cancel	

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 choose **CNS** for the **Terminal Session Protocol**.

For the **Device and Configuration Access Information** section, the only valid **OS** selection is **IOS**. **IOS XR** is not supported for Cisco CNS IE2100 appliances with ISC.

- Step 6** Click the **Show** button for **Additional Properties** at the bottom of the window and this window expands to add the additional information that is shown in [Figure A-4](#), “Cisco Device Additional Properties,” appears.

Figure A-4 Cisco Device Additional Properties

Additional Properties:		Hide
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:	1.4 ▼	
CNS Device Transport:	HTTP ▼	
Device Platform Information		
Platform:		
Software Version:		
Image Name:		
Serial Number:		
Device Owner's Email Address:		
		Save Cancel

Note: * - Required Field

149196

Step 7 The following steps pertain to the **Terminal Server** and **CNS Options** section.

Step 8 Check 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 9-23. Choose **Administration > Control Center**. Choose a Host and then click **Config**. Then in the TOC in the left column, be sure to enter appropriate information in the following fields: **SYSTEM > email > from**; **SYSTEM > email > smtpHost**; **SYSTEM > fullyManaged > auditableCommandsFileLocation** (if information is not given here, all commands are audited); **SYSTEM > fullyManaged > enforcementAuditScript**; and **SYSTEM > fullyManaged > externalEventsEmailRecipients**.



Note

Verify that the **cns config notify** command is configured for the IOS device. This command ensures that configuration change events, which are the basis of the fully-managed feature, are sent out on the event bus. If this command is not configured on the device, the fully-managed feature will not work, because there will be no config-changed events reaching ISC.

Step 9 Specify the **Device State**, as follows:

- Choose **ACTIVE** (the default) if the router is physically present on the network.
- Choose **INACTIVE** if the router is not yet physically present on the network.

Step 10 Specify the **Device Event Identification**, as follows:

- Choose **HOST_NAME** if the **Device Host Name** as defined in [Step 5](#) is to be used as the **CNS Identification** for this device.
- Choose **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. If this command is not present on the device, the IE2100 will not send out any events on the bus using this CNS ID, and hence communication with the device will fail.

Step 11 Select the Cisco CNS **IE2100** appliance that serves this Cisco IOS device. Select one entry from the drop-down list of IE2100 devices already defined in the repository.

Step 12 Use the drop-down list 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, 1.4, 1.5, or 2.0).

Step 13 Use the drop-down list 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 **Save**. [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 3, “Service Inventory — Inventory and Connection 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.



APPENDIX **B**

ISC XML Reference

This appendix contains an alphabetical listing of the XML rules, tags, and attributes that are used in the XML files used for ISC Discovery.

For a detailed description of the XML files and XML examples, see [Chapter 4, “Service Inventory—Discovery.”](#)

Table B-1 *ISC XML Rules, Tags, and Attributes*

Tag	Description
<as-number>	Specifies the autonomous system (AS) number for the provider. The AS number can be an integer between 1 and 65535.
<CDP>	Starts a <CDP> tag. The <CDP> tag specifies an seed IP address and a hop count. The <CDP> tag must contain the following attributes: • ipaddress • hop
<connection>	Starts a <connection> tag. The <connection> tag must specify the following attributes: • discovery-protocol • fromDevice • FromIP • FromInterface • toDevice • toIP • toIF
<create-customer>	Starts a create-customer rule. The create-customer rule creates a region object. the create-customer rule must contain the following tags: • <customer-name> • <create-site>

Table B-1 ISC XML Rules, Tags, and Attributes (continued)

Tag	Description
<create-provider>	Starts a create-provider rule. The create-provider rule creates a service provider object. The create-provider rule must contain the following tags: • <provider-name> • <as-number> • <create-region>
<create-region>	Starts a create-region rule. The create-region rule creates a region object. The create-region rule must contain a region-name tag.
<create-site>	Starts a create-site rule. The create-site rule must contain a <site-name> tag.
<customer-name>	Specifies a customer name. Required within the create-customer rule.
<device>	Starts a <device> tag. The <device> tag must contain the following tags: • <device-name> • <ip-address> The following tags are optional within the <device> tag: • <system-object-id> • <snmp-info>
<device-name>	Specifies the name of the device. Required within the <device> tag.
<DISCOVERY_METHOD>	Starts a <DISCOVERY_METHOD> tag. The <DISCOVERY_METHOD> tag must contain a <CDP> tag.
discovery-protocol	Specifies the Discovery protocol used to discover the network topology. Normally, this is “CDP.”
fromDevice	Specifies the name of the device from which the Named Physical Circuit starts. Required attribute for the <connection> tag.
FromInterface	Specifies the name of the device interface from which the Named Physical Circuit starts. Required attribute for the <connection> tag.
FromIP	Specifies the management IP address of the device from which the Named Physical Circuit starts. Required attribute for the <connection> tag.

Table B-1 *ISC XML Rules, Tags, and Attributes (continued)*

Tag	Description
hop	Specifies the number of hops from the device identified by the ipaddress attribute to go in discovering devices. Required attribute for the <CDP> tag.
ipaddress	Specifies the IP address of a seed device. Required attribute for the <CDP> tag.
<ip-address>	Specifies the IP address of the device. Required within the <device> tag.
<provider-name>	Specifies the name of the provider.
<region-name>	Specifies the name of a region.
<ro-community>	Specifies the level of SNMP access for the device. Normally, this should be “public.” Required within the <snmp-info> tag.
<site-name>	Specifies a site name.
<snmp-info>	Specifies SNMP information for the device. The <snmp-info> tag must contain a <ro-community> tag. Optional within the <device> tag.
<system-object-id>	(optional) Can be included to specify the SNMP Object ID (OID) for the device. If this is provided, it is specified within the <device> tag.
toDevice	Specifies the name of the device to which the Named Physical Circuit connects. Required attribute for the <connection> tag.
toIF	Specifies the device interface on the device to which the Named Physical Circuit connects. Required attribute for the <connection> tag.
toIP	Specifies the management IP address of the device from which the Named Physical Circuit connects. Required attribute for the <connection> tag.



APPENDIX C

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.

None of these properties can be set on a per user basis, including logging.



Note

More details about this are explained in the [“Config” section on page 9-23](#).

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 C-1 **DCPL Properties**

Property	Default Value	Range/Rules	Explanation
AutoDiscovery Properties:			Controls the operation of Autodiscovery.
/DiscoveryTemplateFolder	/Discovery	string	Template folder under which the templates to be discovered for MPLS VPN Discovery will reside.
/TopologyHandler	Default	string	This property points to the topology handler for the discovery run.
/createVpnAndCustomerFromVRFName	true	The valid values are true and false .	This property controls whether the VPN and Customer objects can be created from the VRF names. This is valid only in certain scenarios when Service Providers have maintained such a mapping.
/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/TaskLogs/			This component cleans up old TaskLogs.

Table C-1 DCPL Properties (continued)

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/Tasks/			
maxAgeInHours	0	integer	Maximum age of the Tasks in hours. Tasks that have not been modified in over maxAge hours and that have no Active schedules 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 task cleanup service to wait between clean up cycles. Changing this value initiates an immediate cleanup cycle.
/Cleanup/TempFiles/			
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).
CNS Properties			
/CNS/defaultVersion	1.4	1.3, 1.3.1, 1.3.2, 1.4, 1.5, and 2.0	Default version of CNS to be selected while creating a device. The supported versions are: 1.3, 1.3.1, 1.3.2, 1.4, 1.5, and 2.0.

Table C-1 DCPL Properties (continued)

/CNS/deprecatedReboot	0	The valid values are 0 and 1 .	This is the flag to be used for reloading IOS 12.3 devices using cisco.mgmt.cns.config.reboot CNS event. Value 0 means IOS 12.3 devices may not be rebooted using cisco.mgmt.cns.config.reboot CNS event. So, IOS versions other than 12.3 can be rebooted. Value 1 means only IOS 12.3 devices are rebooted using cisco.mgmt.cns.config.reboot CNS event.
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/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.
ftpSubDirectory		string	FTP sub directory, used by DCS and GTL.
ftpUsername		string	Username for FTP server login, used by DCS and GTL.
/DCS/IOSUsePrimaryWarningExprOnly	false	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 C-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\$ % 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.*\$ 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 C-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\$ % VRF .* does not exist or does not have a RD\$.*warning.*
/DCS/IOSWarningExpressionsExitCfgMode		string	IOS warning expressions that can be safely ignored when exiting config term mode; regular expression must match whole warning message; for messages that wrap more than one line replace line terminations (CR and/or LF chars) with a single space character; replace each variable field with the meta-character sequence \\S+ that will match a single group of non-whitespace chars; literals are case insensitive; use \$ to separate entries.

Table C-1 DCPL Properties (continued)

/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.
/DCS/RCP/			RCP Settings.
rcpDirectory	/tmp	string	Directory to use for uploaded/downloaded config files.
/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/SSHv2/			SSHv2 Client Settings.
overWriteSSHv2Keys	true	The valid values are true and false .	Overwrite SSHv2 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.
/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 must be the same as that of the ISC server.
tftpSubDirectory		string	TFTP Sub Directory used by DCS and GTL.
/DCS/XR			IOS XR properties.

Table C-1 DCPL Properties (continued)

WarningExpressions	^.??.warning\$	string	IOS XR warning expressions that can be: safely ignored; case insensitive; . matches any character except newline, where: * means zero or more, + means one or more, ? means zero or one.
commitConfigTimeout	120	integer, 30-600	Maximum time in seconds to commit config target buffer to running config.
maxRetriesEnterCfgExcIMode	3	integer, 0-10	Maximum number of times to retry entering configure exclusive mode. 0 = no retries. Retry delay interval is fixed at 30 seconds.
/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/configUploadTimeout	300	integer, 60-900	Maximum time in seconds to wait for a device configuration to be uploaded.
/DCS/customPasswordPrompt	Password:		Device custom password prompt.
/DCS/customUsernamePrompt	Username:		Device custom username prompt.
/DCS/getCommitCLIConfigAfterDownload	true	The valid values are true and false .	Retrieve the committed CLI configuration after an XML configuration download. If the default of true is set, whenever a Service Request is deployed on an IOS XR device, a transaction is created. This transaction gets the configlet deployed in the CLI mode and stores it in the repository. This creation of a new transaction adds to the time of Service Request deployment. If this property is set to false , no transaction to retrieve the CLI configlet is created.
/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).
/DCS/maxDeviceConnectCompleteTime	60	integer, 15-600 seconds	Maximum time in seconds to wait for a terminal session connection to a device.

Table C-1 DCPL Properties (continued)

/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.
/DCS/misc			Miscellaneous settings.
ConfigForMergeXML		string, file name	Configuration file to be used for the merging of two XMLs.
allowPromptCharsInBanner	false	The valid values are true and false .	Controls if prompt characters, such as # and >, are allowed in banners. If true , a minimum of 2 seconds (default of loginSocketReadTimeout) is added to each login. Note that selecting this option requires “aaa authentication attempts login n” to be set to a minimum of 2.
loginSocketReadTimeout	2	integer, 1-45	Number of seconds to WAIT for a login authentication username or password prompt. Applicable if DCS\misc\allowPromptCharsInBanner is true . Increasing this value slows down device logins and counts against DCS\maxDeviceConnectCompleteTime who’s default is 60 seconds.
readBufferSize	32	integer, 4-96	Size in KBytes of the buffers used while reading device input streams with telnet and SSH. Increasing size might improve performance. Decrease size if there are memory issues.
DeploymentFlow Property:			Deployment flow Component: Used to create a flow of different types of steps such as mpls.
/DeploymentFlow/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).
Discovery Properties:			ISC auto discovery framework.

Table C-1 DCPL Properties (continued)

/Discovery/DeviceDiscovery			
continueOnError	false	The valid values are true and false .	A Boolean flag indicating whether device discovery should try to continue on an error. When the value is true , device discovery ignores the device and attempts to create other devices discovered. In this case, the device discovery is marked as SUCCESS, but indicates there were errors. The default behavior is device discovery is marked FAILED at the first error encountered. This property applies only to errors encountered during the device creation phase of device discovery like duplicate or missing hostnames in case of CDP and file based discovery options and invalid device configurations or insufficient read permissions for configurations files and so on, for the configuration file based discovery option. Any errors encountered during CDP discovery itself or while parsing XML files still result in the device discovery step being marked as FAILED. WARNING: If this property is set to true , discovery continues if there are any device creation errors, ignoring the device that caused the error, but only partial NPCs and services are discovered.
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 C-1 DCPL Properties (continued)

mgmtIpAddressLoopkupPattern		string	A comma separated list of interface name patterns to look for to determine the management IP address of the device discovered using the import configuration option. The configuration is parsed for the interface information, and the first available IP address of the interface from the given list is used as the management IP address of the device. For example, if the IP address of the loopback 0 interface should be used as the management IP address, the value of the property should be set to "loopback0". If the first available loopback should be used, set the value of the property to "loopback". A comma separated list can be specified as "Loopback0,Ethernet0". In this case, the first available IP address among the list of interfaces specified in that order is used as the management IP address.
/Discovery/DataCollection			
continueOnError	false	The valid values are true and false .	A Boolean flag indicating whether data collection should try to continue on an error. When the value is true , the data collection step does not collect discovery data for the failed device, but attempts to collect configuration for other devices discovered. In this case, the configuration collection step is marked as SUCCESS, but indicates there were errors. The default behavior is discovery data collection step is marked FAILED at the first error encountered. WARNING: If this property is set to true , discovery continues if there are any collection or parsing errors, ignoring the device that caused the error, but only partial NPCs and services are discovered.
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 C-1 DCPL Properties (continued)

reuseConfigsIfAvailable	false	The valid values are true and false .	If the Boolean flag is true , the discovery data collection step uses the config from the repository if available. If the configs are not in the repository, an attempt is made to contact the device to collect the current running configuration. The default behavior is discovery tries to collect the current running configs from the device.
/Discovery/MPLSService			MPLS services discovery.
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).
/Discovery/MetroEService			Metro Ethernet services discovery.
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).
meConfigParsingRegistry		string	List of handlers to be invoked at collect config time for Metro Ethernet services.
meDiscoverIntraPopVPWS	false	The valid values are true and false .	Set this to true if local switched VPWS services are to be discovered. Do this only if you wish to discover VPWS services switched at NPE. If not, set this to false for performance reasons.
/Discovery/NPCDiscovery			NPC discovery.
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).
/Discovery/RoleAssignment			

Table C-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).
/Discovery/Workflow			ISC auto discovery workflow.
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).
/Discovery/configs.location	<vpnsc_tmp>/Discovery/configs		The directory name where the temporary device configurations are stored during the collect config process.
/Discovery/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).
/Discovery/logLocation	vpnsc_tmp>/Discovery/logs	string	The directory name where discovery logs files are kept.
/Discovery/restart	false	The valid values are true and false .	With this property, you can clear out all network objects from the repository that was created by the Discovery process and you can restart the Discovery process. Be very cautious in setting this value to true .
/Discovery/tmpdir	<vpnsc_tmp>/Discovery	string	A directory to store the temporary results of the discovery process.
DistributionFramework Properties:			Distribution Framework. This component handles the distribution of work (jobs) between different servers in a ISC distributed installation.
/DistributionFramework/Dispatcher/			Service that dispatches jobs to workers.
DefaultUnitDuration	1000	integer	The unit duration (in milliseconds) used to estimate jobs without a profile.
PingInterval	1000	integer	The interval (in ms) dispatcher pings the workers to get the load.

Table C-1 *DCPL Properties (continued)*

ProcessorEpsilon	10	integer	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.
ProfileUpdateThreshold	10	integer	The percent change of a profile that triggers an update of the dispatcher.
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	<i><master_server></i>	string	The hostname or ip address of the name server.
/DistributionFramework/NamingPort	<i><naming_port></i>	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).

Table C-1 DCPL Properties (continued)

/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.
ThreadPoolSize	100	integer, 25-250	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 C-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 asynchronous 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/PAM/			
args		string	Invocation argument to be used.
className		string	PAM Class name.
usePAM	false	The valid values are true and false .	When the value is true , the selected PAM is used for device authentication. When the value is false , the standard authentication credentials are used in the ISC repository for each device.
/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.

Table C-1 DCPL Properties (continued)

/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. Setting ISC to run in echo mode allows ISC to perform Service provisioning tasks without downloading the resulting commands to the physical hardware. The resulting Service Provisioning is stored only in the Repository and no attempt is made to connect to the target devices. When echo mode is enabled (set to true), no attempt to audit the Service Request is performed. From a production environment, you are able to perform service provisioning on devices that are either temporarily offline or not yet commissioned. Once these devices become active, you can Force Deploy the already provisioned Service Requests and ISC downloads the configurations.
/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.
/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).
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 L2VPN.
logFileViewThreshold	10000000	integer	The maximum log file size in bytes that can be viewed in the GUI Log Viewer.

Table C-1 DCPL Properties (continued)

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/MPLSOAM/			The MPLS OAM component.
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).
/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).
/GUI/Performance/			For monitoring GUI performance.

Table C-1 DCPL Properties (continued)

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/Topology/			Component related to the web start topology application.
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 predefined workflow steps.
/GUI/workflows	<vpnsc_home>/etc/workflows.csv	string	The predefined workflows.

Table C-1 DCPL Properties (continued)

JavaWebStart Properties			Java Web Start components.
/JavaWebStart/InventoryManager/			Component to create and manage Devices.
MaxDevicesPerSaveTransaction	25	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	25	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.
/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.

Table C-1 DCPL Properties (continued)

/Logging/TaskLogs/			This contains logging properties for task logs.
logLocation	<vpnsd_tmp>/TaskLogs	string	The directory name where all the task logs are kept.
logMessageSize	100	integer, 100-300	This property sets the number of lines of message to be displayed for each log entry.
Provisioning Properties:			Contains properties and components for service provisioning like MPLS 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.
/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.
explicitlyRemoveRouteTargets	false	The valid values are true and false .	Normally (false), the “no ip vrfname” automatically cleans up all its subcommands in IOS. There is no need to clean up each one of the subcommands before taking away the parent command. By setting this value to true , ISC explicitly cleans up all router target subcommands before removing the “ip vrfname”.

Table C-1 DCPL Properties (continued)

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 .
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.

Table C-1 DCPL Properties (continued)

MaxNumberOfDevicesPerDownload	100	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.
ProvisioningBatchSize	10	integer, 0-2147483647	Provisioning Driver divides the requested Service Requests into batches while performing the deployment. This parameter specifies the number of Service Requests that will be processed as a batch.
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.
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.

Table C-1 DCPL Properties (continued)

TE/			Traffic Engineering Provisioning Service related properties section.
enableLogging	true	The valid values are true and false .	When the value is the default of true , debugging of logging is enabled for this service. When the value is false , debugging of logging is not enabled for this service.
platform/			Used by ProvDrv
CISCO_ROUTER/			Used by ProvDrv
serviceBladeClass	com.cisco.vpnsc. prov.te. ServiceBlade. TeServiceBlade	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.
Uds/			User defined services.
platform/			Service platform
CISCO_ROUTER/			Cisco router
serviceBladeClass	com.cisco.vpnsc. prov.uds.Uds ServiceBlade	string	Uds Service Blade.
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.L2VP NServiceBlade	string	ServiceBladeClass location.
CISCO_ROUTER/			
iosXRConfigType	XML		Config type for IOS XR devices for MPLS service blade

Table C-1 DCPL Properties (continued)

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.
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.
weightForMVRFCCE	0	integer	Download weight for MVRFCCE. The higher the weight the sooner we download to this device while deploying a service request.

Table C-1 *DCPL Properties (continued)*

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.
iosXRConfigType	XML		Config type for IOS XR devices for MPLS service blade
serviceBladeClass	com.cisco.vpnsc. prov.mpls.MplsS erviceBlade	string	ServiceBladeClass location
allowDuplicateIpAddressForPPPo ATM	false	The valid values are true and false .	Provision PPPoATM by allowing duplicate IP addresses for MPLS Service Requests. Ignore duplicate IP address on Loopback and Multilink interfaces.
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.
allowShared VLAN Modification	false	The valid values are true and false .	For residential services, if the flag is on, true , shared VLAN attributes are available for modify in edit mode. If the flag is off, false , attributes are in read only mode.
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 .	This property controls whether an audit will be run on the Max Route Threshold for a Service Request. This is needed to maintain backward compatibility.
auditPartialCommands	false	The valid values are true and false .	This property is set for the autodiscovered systems containing a superset of the commands that ISC supports.

Table C-1 DCPL Properties (continued)

dataFileSchema	l3vpnData.xsd	string	Specifies the schema for the data XML file for MPLS/BGP layer3 VPNs.
excludeNoKeepaliveConfigOnPort Channel	false	The valid values are true and false .	Exclude the no keepalive command on the port channel trunk port.
forceRemoveNonBroadcastStatic RouteOnPE	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.
ignoreLoopbackWhileRemovingVRF	false	The valid values are true and false .	Remove a VRF, even when some Loopback interfaces are still pointing to it.
ignoreMajorInterfaceCheck	false	The valid values are true and false .	This property controls the check for a proper major interface name in an unmanaged CE. If set to true , ISC bypasses the check for a proper major interface name. Note: This will work only for UnmanagedCE devices
ignoreStatusMessagesForUnmanaged CEs	false	The valid values are true and false .	If set to true , this property prevents the generation of status messages for unmanaged CEs
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.
passAuditForNonBroadcastStatic RouteOnPE	false	The valid values are true and false .	When this property is set to true , the ISC auditor does not generate an error message if the static route was found with a different format (such as, a PE interface name instead of a CE IP address).

Table C-1 DCPL Properties (continued)

passIpAddressAuditWhenNoAddress Detected	false	The valid values are true and false .	Pass the IP address command auditing if uploaded router config does not contain an IP address. This is to prevent the audit failure from appended template blob overwriting the provisioned IP address command.
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.
routeMapDeletedAfterLastLink Deletion	true	The valid values are true and false .	If this property is set to true , the route map configuration is automatically removed from the device after the last link is deleted. If false , the route map configuration is left as it is in the device.
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
skipIpAddressValidationOn UnmanagedCE	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 bypassed.
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.

Table C-1 DCPL Properties (continued)

useOnlyExtraCEloopbackForGreyAccessList	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).
IosXrVersionFilesDir		string	Path to IOS XR version XML files.
actionTakenOnUNIVlanList	prune	string	Action taken when switch port allowed vlan cmd is absent for ERS service.
leaveSystemMTUUnset	false	The valid values are true and false .	If this property is set as true : U-PE system MTU is not set as default, or set as value given by user; N-PE SVI MTU is set as 9216 for VPLS(EWS and ERS) and L2VPN(EWS). If this property is set as false : U-PE system MTU is set as minimum value 1522, or set as value given by user; N-PE SVI MTU is not set as default, or set as value given by user.
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 (Example: crypto map entries, gre Interfaces, and so on).
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.

Table C-1 DCPL Properties (continued)

useSRDescriptionToGenerateDebug Data	false	The valid values are true and false .	This property is used to generate more intuitive debug data for easy fixing of issues.
staging/			
platform/			Platform related classes.
CATOS/			Service blade parameters for CATOS.
serviceBladeClass	com.cisco.vpnsc. prov.staging. StagingService Blade	string	ServiceBladeClass location.
CISCO_ROUTER/			IOS.
serviceBladeClass	com.cisco.vpnsc. prov.staging. StagingService Blade	string	ServiceBladeClass location.
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.
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	stagingService. xml	string	Specifies the XML file containing the service definition for staging service. The schema for this file is specified by Provisioning.Engine.serviceSchema.
vpls/			Contains properties for Virtual Private LAN Service.

Table C-1 DCPL Properties (continued)

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.
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.

Table C-1 DCPL Properties (continued)

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.
/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/ciscoURL	http://www.cisco.com	string	The Cisco URL.
/SYSTEM/databaseServer	<db_server>	string	The database server fully qualified name.

Table C-1 DCPL Properties (continued)

/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.
auditableCommandsFileLocation		string	This property specifies the full path to the file containing the list of prefixes of auditable commands used in the Fully Managed feature.
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	The possible value is: master.
/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.
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.

Table C-1 DCPL Properties (continued)

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.
Services Properties:			Common services.
/Services/Common/			
allowForcePurge	true	The valid values are true and false .	With the default value of true , you can force purge a Service Request. If the value is false , you cannot force purge a Service Request.
disallowVlan1	true	The valid values are true and false .	This prevents allocating VLAN ID 1 for services configured by ISC. This is applicable for both auto allocation of VLAN from VLAN resource pool and manual allocation. Set this property to true to block ISC from deploying services with VLAN ID 1
pseudoWireVlanMode	false	The valid values are true and false .	This property is effective only for IOS XR L2VPN services. The default is false . When set to true , this configures pseudowire transport mode to VLANs.
SnmpService Properties:			The Snmp Service package provides APIs to perform SNMP get() and set() operations.
/SnmpService/misc			Advanced settings.

Table C-1 DCPL Properties (continued)

enableDebug	false	The valid values are true and false .	Enables the AdventNet SNMP stack debug messages. Messages are written to the TaskLogs directory in files stdout and stderr. Warning: These log files grow quickly and are NOT managed by the ISC logger. Requires WatchDog restart.
rcvPktBuffSize	96	integer, 64-512	Buffer size in K bytes, for SNMP stack receive buffer.
/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.
/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/maxTaskDuration	5	integer, 1-30	Maximum duration in minutes for collecting device interface information. A longer duration is required for devices with large numbers of interfaces. This period must be longer than $2^{(retries+1)}$ * timeout.
/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:			Traffic Engineering Management (TEM) Properties
/TE/Deployment			Control the operation of TEM Provisioning
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.

Table C-1 *DCPL Properties (continued)*

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.
tunnelMplsIp	true	The valid values are true and false .	When the value is the default of true , this indicates to deploy the mpls ip command when provisioning TE primary tunnels, which enables MPLS IP switching on the router. When the value is set to false , this indicates not to deploy the mpls ip command when provisioning TE primary tunnels.
/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:			TEM Topology-related 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.
Orange	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 orange.
Red	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 red. Greater than 100% is also displayed in red.
Yellow	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 yellow.

Table C-1 DCPL Properties (continued)

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/CollectConfig			The Collect Config task uploads the running configuration.
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).
/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	<vpncsc_home>/resources/AAgent/DMDFiles	string	File path and name.
input	<vpncsc_home>/resources/java/classes/common/AAgent/com/cisco/vpncscagent	string	File path and name.

Table C-1 DCPL Properties (continued)

working	<vpnsc_home>/resources/java/archives	string	File path and name.
cfr Properties:			The Command Flow Runner component. This currently runs within the Tomcat server (in the ISC web application) and is responsible for running MPLSOAM troubleshooting workflows.
/cfr/Diagnostics/			
disableTunnelDiagnostics	false	The valid values are true and false .	Set to true to disable tunnel diagnostics, in order to avoid errors when running MDE across networks with non-Cisco devices in the tunnel LSPs.
/cfr/LogHandler	com.cisco.mgmt.workflow.util.IscLogHandler		Set the CFR to use a custom handler for logging. The handler should log to a separate file and format the log messages using the <code>java.util.logging.SimpleFormatter</code> instead of the ISC default XML formatting.
/cfr/logLevel	INFO		The level of logging information the Command Flow Runner will log (it will log from the set level upwards). The logging levels are as defined in the <code>java.util.logging</code> package.
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/collectConfigLock	false	The valid values are true and false .	Determines if a software lock is to be applied to the devices in the CollectConfig task. If true , a software lock is applied to all devices prior to executing the CollectConfig operation, and is released upon completion of the CollectConfig operation. Note that a software lock is not applied to the optional device attributes and interfaces operations. This flag is read by the CollectConfig task upon execution.

Table C-1 DCPL Properties (continued)

/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).
/lockmanager/queueServicingInterval	100	integer, 10-2000 milliseconds	How often in milliseconds to service pending lock requests. A lower value decreases the average time it takes to get a lock at the expense of CPU processing overhead.
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.

Table C-1 DCPL Properties (continued)

/nbi/MetaDir	<vpnsc_home>/resources/java/xml/com/cisco/vpnsc/repository/meta/xml	string	Path to meta XML files. Do not change it or the meta XML will not be backed up.
/nbi/ProvidedReportMetaDir	<vpnsc_home>/resources/java/xml/com/cisco/vpnsc/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.vpnsc.nbi.io.NbiSoapReader	string	File path and name.
/nbi/RequestParserMgr	com.cisco.vpnsc.nbi.parser.NbiRequestParserMgr	string	File path and name.
/nbi/SSLfilepath	<vpnsc_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. A session is the socket connection between the client and the NBI server through the Tomcat server.
/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/WaitTimeout	1200	integer	The time in seconds to wait for a Service Request to deploy.
/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.

Table C-1 DCPL Properties (continued)

/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.NbiVpns cLogger	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.
/notification/logHandler	com.cisco.vpnsc. nbi.util.VpnscLo gHandler	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 username 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	Username for remote system authentication, if required, for example, when LDAP is in use.

Table C-1 DCPL Properties (continued)

/notification/username	admin	string	Both username and password are the same as the ones used for GUI login.
pal Properties:			The PAL Device interaction component. This runs within the Tomcat server and is responsible for running device interaction for the CFR to run the OAM troubleshooting workflows.
/pal/failureScenario			The system parameter that represents the current failure scenario. For use with the Canned Response mechanism for testing.
/pal/logHandler	com.cisco.mgmt.workflow.util.IscLogHandler		Set the PAL to use a custom handler for logging. The handler should log to a separate file and will format the log messages using the java.util.logging.SimpleFormatter instead of the ISC default XML formatting.
/pal/logLevel	INFO		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).
/pal/responseDir	/vob/ntg/dev/resources/pal/testnetwork		The base directory where the failure scenarios are held. Used by the canned response mechanism and transport for failure scenario testing.
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).

Table C-1 DCPL Properties (continued)

RecoverIPAddrSleepInterval	60	integer, 10 - 144000 minutes	The time in minutes for recovering Aged IP addresses recovery service to wait between recovery cycles. The default is 60 minutes. Changing this value initiates the recovery process.
releaseAndReuseAgedAddresses	true	The valid values are true and false .	The default value is false . When the value is set to true , the user wants a manual allocation of the address in the aged address to succeed. When the value is set to true , the address is released from the Aged Pool and moved to the Allocated pool when manually allocated.
/repository/common			Repository common constants.
MCAST_SUBSUME_ALL_SRS	true	The valid values are true and false .	This property set at true indicates that the user wants all the MPLS VPN links of a VPN to be subsumed when Multicast is enabled for that VPN.
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.
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.

Table C-1 *DCPL Properties (continued)*

schema	DBA	string	Schema.
slaur1	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.
cache/isEternal	false	The valid values are true and false .	Specifies whether the elements in the RBAC cache are eternal, never expire. The value true indicates the elements in the cache are eternal and never expire. The default value false indicates the elements in the cache can expire.
cache/maxElementsInMemory	5000	integer, 1000 to 10000	Specifies the maximum number of elements in cache memory. Default: 5000.
overflowToDisk	false	The valid values are true and false .	Specifies whether to use disk to store cache.
cache/timeToIdleSeconds	120	integer, 60 to 1800 seconds	Specifies the default number of seconds for an element to live in cache from its last accessed or modified date. Default: 120 seconds.
cache/timeToLiveSeconds	300	integer, 100 to 3600 seconds	Specifies the default number of seconds for an element to live in cache from its creation date. Default: 300 seconds.
/repository/rbac/checkCreatorPermission Enabled	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.
/repository/rbac/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 C-1 DCPL Properties (continued)

/repository/rbac/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.
/repository/rbac/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).
/repository/rbac/partialQueryResult Expected	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 .
/repository/rbac/webSessionTimeoutSec	1800	integer, 1 - 2,147,483,647	Timeout of inactive web client session in seconds. Default is 30 minutes.
/repository/uall/			User Access/Audit Log
cleanUALogs	true	The valid values are true and false .	Indicates whether to let the 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/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.

Table C-1 DCPL Properties (continued)

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.
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.
period_poller	60000	integer, 30000- 86400000 milliseconds	The minimum time between each heartbeat request for dbpoller and nspoller 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.

Table C-1 DCPL Properties (continued)

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.
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:+UseAltSig s	string	Any other flags to be passed on to java .
vmtype	-server	string	The flag to be passed on to java (-server or -client).

Table C-1 DCPL Properties (continued)

/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 cornerstonebridg e	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.
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).

Table C-1 DCPL Properties (continued)

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.
connectionextend	5	integer, 1-15	For Oracle RAC failover, increase this value to make sure the failover happens before dbpoller stops.
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).
select	select id from vpnsc_host	string	SQL select statement to issue when pinging the database.
discovery/			Handles various ISC Discovery workflow related tasks.
class	com.cisco.vpnsc. discovery.engine. server.Discovery Server	string	Heartbeat Handler.
cmd	java com.cisco.vpnsc. discovery.engine. server. DiscoveryImpl	string	Implementation of the Discovery work interface.
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, 1000-60000 milliseconds	The period of time before which response for heartbeat request should be received by the watchdog, in milliseconds. To discover large networks with a complex topology, we recommend you reset this property to 180000 milliseconds (3 minutes).
java/			Java attributes for this server

Table C-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. To discover large networks with a complex topology, we recommend you reset this property to -Xmx3072m -XX:PermSize=256m -XX:MaxPermSize=512m.
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.
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.

Table C-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).
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.
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, 1000-600000 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
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.

Table C-1 *DCPL Properties (continued)*

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.
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).
rgserver/			TEM server for the TEM tunnel generation algorithm.
heartbeat/			
rgport		string	The port on which rgserver should run.
startDelay	45000	integer, 0-60000 milliseconds	Time to wait before making the first heartbeat request in milliseconds.

Table C-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.
class	com.cisco.vpnsc. watchdog.servers .WDRGServer	string	Class.
cmd	rgserver.sh	string	Command to start the rgserver.
dependencies	httpd	string	Servers that must be functioning for this server to function normally.
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).

Table C-1 DCPL Properties (continued)

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.
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.
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 C-1 DCPL Properties (continued)

flags	-Xmx512m -Xbootclasspath/ p:<vpnsc_home> /thirdparty/jar/ AdventNetSnmp 3_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 C-1 **DCPL Properties (continued)**

/xml/ValidatorRule			
filepath	<vpnsc_home>/resources/java/classes/common/com/cisco/vpnsc/util/validator/xml	string	Validator rules file path and name.
/xml/queries/			Properties for RepQueryLoader.
filepath	<vpnsc_home>/resources/java/xml/com/cisco/vpnsc/repository/Queries.xml	string	File path and name.



APPENDIX **D**

Template Usage

The following questions and answers can help you troubleshoot. The following topics are for Template Manager, which is explained in [Chapter 6, “Service Design”](#):

- [How do I split a string?, page D-1](#)
- [How do I obtain address information from the given IP address?, page D-2](#)
- [How do I obtain the octets from the given IP address?, page D-2](#)
- [How do I call a subtemplate in a template?, page D-2](#)
- [How do I concatenate two strings?, page D-3](#)
- [How can I convert a string to an integer and how can I increase the last octet of the IP address by one?, page D-3](#)
- [Can I use nested if statements?, page D-3](#)
- [How can I perform basic arithmetic operations?, page D-4](#)
- [How can I retrieve data from a two-dimensional array and what is the use of \\$velocityCount?, page D-4](#)
- [How can I print \\$a instead of its value?, page D-4](#)
- [What is the difference between #include\(\) and #parse\(\)?, page D-5](#)
- [What is a macro and how is it used?, page D-6](#)
- [What is a range operator and how can I use it?, page D-6](#)
- [How can I split strings containing special characters?, page D-7](#)
- [How can I use repository variables?, page D-7](#)
- [How can I use a variable as a dynamic URL?, page D-7](#)
- [Can I see more examples?, page D-7](#)

How do I split a string?

ISC provides a function `substringToDelim()`, which can split the given string and return the substring based on the given delimiter.

Syntax:

substringToDelim (srcString, delimChar, 0/1)

where:

0 returns the string before the delimiter.

1 returns the string after the delimiter.

Usage: **\$b=\$TMSystem.substringToDelim("10.11.230.145", ".230.145", "0")**

Result: The value of **\$b** is **10.11**. If **1** is specified instead of **0**, the value of **\$b** is **230.145**.

How do I obtain address information from the given IP address?

ISC provides the functions that can be used to get the address, mask, and reverse mask from the given IP address.

Usage:

\$TMSystem.getAddr ("10.33.4.5/30") returns 10.33.4.5

\$TMSystem.getMask ("10.33.4.5/30") returns 255.255.255.252

\$TMSystem.getReverseMask ("10.33.4.5/30") returns 0.0.0.3

\$TMSystem.getNetworkAddr ("10.33.4.5/30") returns 10.33.4.4

\$TMSystem.GetClassfulNetworkAddr ("10.33.4.5/30") returns 10.0.0.0

\$TMSystem.CurrentTimeInIOSFormat () returns hh:mm:ss day_of_month month_of_year year

How do I obtain the octets from the given IP address?

ISC provides the functions that can return the octets when called.

Usage:

\$TMSystem.getOctet1(\$ipAddr) returns the first octet of **ipAddr**

\$TMSystem.getOctet2(\$ipAddr) returns the second octet of **ipAddr**

\$TMSystem.getOctet3(\$ipAddr) returns the third octet of **ipAddr**

\$TMSystem.getOctet4(\$ipAddr) returns the fourth octet of **ipAddr**

How do I call a subtemplate in a template?

A subtemplate can be called in a main template. The subtemplate being called should be called with its datafile. The variable is declared as a subtemplate. The location of the subtemplate is specified in the datafile.

Usage: In the template body the subtemplate is declared as:

\$a. callWithDatafile("data1")

where:

the variable **a** is declared as a subtemplate in the variables

data1 is the name of the datafile of the subtemplate, and

in the datafile the path of the subtemplate path is specified.

How do I concatenate two strings?

Concatenation of strings is simple.

For example:

where: **\$a=vpnsc** and **\$b=properties**

then: **\${a}\${b}** concatenates these two strings and gives the result as **vpnscproperties**.

or, **\${a}_\${b}** gives the result as **vpnsc_properties**.

How can I convert a string to an integer and how can I increase the last octet of the IP address by one?

The last octet of the IP address can be increased by using the following code:

```
#set($d=$TMSsystem.getOctet1($c))
#set($e=$TMSsystem.getOctet2($c))
#set($f=$TMSsystem.getOctet3($c))
#set($g=$TMSsystem.getOctet4($c))
#set($valueOfString = $g)
#set($valueOfCharsCount = $valueOfString.length() - 1)
#set($valueOfVector = "0123456789")
#set($valueOfBase = 1)
#set($valueOfInt = 0)
#foreach($valueOfCharIterator in $valueOfCharsCount..0)
#set($valueOfChar=$valueOfString.charAt($valueOfCharIterator).toString())
#set($valueOfInt = $valueOfInt + $valueOfVector.indexOf($valueOfChar) * $valueOfBase)
#set($valueOfBase = $valueOfBase * 10)
#end
#set($valueOfInt = $valueOfInt+1)
```

The incremental value is **\$d.\$e.\$f.\$valueOfInt**

Can I use nested if statements?

If statements can be nested. Proper care must be taken for indentation when nesting **if** statements. The following code shows the usage of nested **if** statements, **elseif** statements, and the comparisons made in the **if** clause.

#if(\$a=="a") // here: string comparison is made

--

#if(\$b || \$d) // here: **\$b** and **\$d** are the Boolean expressions. **||** equals **OR** and **&&** equals **AND**

--

#if(!\$c) // here: **\$c** can be integer, string, or Boolean.

#if(\$p<10) // here: **\$p** is a integer.

#elseif(\$p==10)

#end

#end

#end

#end

How can I perform basic arithmetic operations?

Velocity Template Language (VTL) supports built-in mathematical functions that can be used in the templates with the set directives.

Usage:

```
#set($a = $b + 3)
#set($a = $b - 6)
#set($a = $b * 6)
#set($a = $b / 5)
#set($a = $b % 2)
```



Note

Only integers are valid for performing mathematical operations in the VTL.

How can I retrieve data from a two-dimensional array and what is the use of \$velocityCount?

The default name for the loop counter variable reference, which is specified in the velocity.properties file, is **\$velocityCount**. By default the counter starts at **1**, but this can be set to either **0** or **1** in the velocity.properties file at:

\$ISC_HOME/resources/webserver/tomcat/shared/lib/velocity-dep-VelocityVersion.jar (where the current *VelocityVersion* is 1.3.1-rc2). The associated settings are:

```
directive.foreach.counter.name=velocityCount
directive.foreach.counter.initial.value=1
```

Data from an array can be obtained by using **get(\$i)**

where: **\$i** is the \$velocityCount.

The following example illustrates the usage of the method **get()**:

```
Usage: #foreach ($Acl in $ACL-List)
      #set ($i = $velocityCount)
      #foreach ($protocol in $Protocol-Lists.get($i))
      #set ($j = $velocityCount)
          access-list $Acl permit $protocol $Source-IP.get($i).get($j)
      #end
      #end
```

where:

\$ACL-List is a one-dimensional array.

\$Protocol-Lists and **\$Source-IP** are two-dimensional arrays.

Here the \$velocityCount is set to **1** by default. It can be changed in velocity.properties, if desired.

How can I print \$a instead of its value?

Printing a value without processing is done by use of the character ****, even if the value of the variable for **a** is defined.

Usage:

`\$a` gives output as `$a` if `$a` is defined. If `$a` is not defined, it is printed as `\$a`.

What is the difference between #include() and #parse()?

The **#include("velocity.txt")** directive allows you to import a file and then include the file in the location where it is defined. The content of the file is made available to the template engine. The *.vm files can also be called by using **#include**. The name of the file can also be passed by a variable. For security reasons, the file should be included under **TEMPLATE_ROOT** (/vob/ntg/dev/resources/templatesystem).

The **#parse("velocity.vm")** directive allows you to import a local file that contains VTL. Velocity will parse the VTL and render the template specified. The template that **#parse** references must be included under **TEMPLATE_ROOT**. The **#parse** directive only takes a single argument. VTL templates can have **#parse** statements referring to templates that in turn have **#parse** statements. The default value of the **directive.parse.max.depth** property is set to 10, in the **velocity.properties** file at: **\$ISC_HOME/resources/webserver/tomcat/shared/lib/velocity-dep-VelocityVersion.jar** (where the current *VelocityVersion* is 1.3.1-rc2) and can be modified, if desired.



Note

If the **directive.parse.max.depth** property is not present in the **velocity.properties** file, the default is set to 10.

Example:

In **TEMPLATE_ROOT**, the file **velocity.vm** has the following content:

```
welcome to the parse file
The count is $count
#set($count = $count - 1)
#set($cl-list="cl1","cl2","cl3")
#foreach($i in $cl-list)
ipcommunity-list permit $i 30:20
#end
The count is $count
returning from parse
```

The template body contains the following:

```
#set($count=8)
#include("velocity.vm")
-----
#parse("velocity.vm")
-----
welcome back to template
The value of count is $count
```

The following O/P is obtained:

```
welcome to the parse file
The count is $count
#set($count = $count - 1)
#set($cl-list="cl1","cl2","cl3")
#foreach($i in $cl-list)
```

```
ipcommunity-list permit $i 30:20
#end
The count is $count
returning from parse
-----
welcome to the parse file
The count is 8
ipcommunity-list permit cl1 30:20
ipcommunity-list permit cl2 30:20
ipcommunity-list permit cl3 30:20
The count is 7
returning from parse
-----
welcome back to template
The value of count is 7.
```

**Note**

The previous examples clearly show that variables are parsed in the **#parse** directive and not in the **#include** directive.

What is a macro and how is it used?

The directive macro is almost similar to a function. This has a set of statements, which can be called repetitively.

Example:

```
#macro(community $CL $bgp-list)
  #foreach($bgp in $bgp-list)
    ip $CL standard permit $bgp
  #end
#end

#set($bgp_list = "20:10","30:10","40:10","50:10")
#set($CL = "community-list")

#community($CL $bgp_list)
```

Here, the macro name of **community** is defined. The macro takes two arguments **\$CL** and **\$bgp-list**. The macro is called at the end line.

The output of the previous template is:

```
ip community-list standard permit 20:10
ip community-list standard permit 30:10
ip community-list standard permit 40:10
ip community-list standard permit 50:10
```

What is a range operator and how can I use it?

The range operator can be used in conjunction with **#set** and **#foreach** statements. It is used to produce an object array containing integers. The range operator has the following construction **n..m**.

Example:

```
#set($a=0..2)
#foreach($b in $a)
  $b
#end
#foreach($c in -2..2)
  $c
#end
```

How can I split strings containing special characters?

```
#foreach ($i in $PE_Intf_Name.split('\.')) $i #end
```

here: In the first iteration, **\$i** contains the string before the period, and in the second iteration, **\$i** contains the string after the period.

How can I use repository variables?

Repository variables can be selected in the datafile. When a template along with a datafile is associated with a Service Request and the Service Request is deployed, then the value of the repository variable gets substituted.

How can I use a variable as a dynamic URL?

A variable declared as a dynamic URL can call the URL, by the method:

```
callUrl(String S)
```

For example: **\$a.callUrl("http://www.cisco.com")**

Can I see more examples?

Examples are given for:

- [Usage of Strings, page D-8](#)
- [Usage of a Macro, page D-9](#)
- [Usage of Subtemplates, page D-10](#)

Usage of Strings

The body of the template contains:

This example illustrates the usage of strings

```
#set($a="Fast")
#set($b="ethernet")
interface ${a}_${b}
```

```
#foreach ($i in $PE_Intf_Name.split('\.'))
$i
#end
```

```
#set($c="10.11.230.145")
#set($b=$TMSsystem.substringToDelim($c, ".230.145", "0"))
interface Loopback1
description By VPN-SC
ip vrf forwarding V31:eigrpfm
ip address ${b}.20.34 255.255.255.255
no ip directed-broadcast
```

```
#set($b=$TMSsystem.substringToDelim($c, ".230.145", "1"))
interface Loopback1
description By VPN-SC
ip vrf forwarding V31:eigrpfm
ip address 20.45.${b} 255.255.255.255
no ip directed-broadcast
```

```
#set($c="10.33.4.5/30")
#set($d=$TMSsystem.getAddr($c))
The Address of $c is $d
#set($d=$TMSsystem.getMask($c))
The mask of $c is $d
#set($d=$TMSsystem.getReverseMask($c))
The Reverse mask of $c is $d
#set($d=$TMSsystem.getNetworkAddr($c))
The network address of $c is $d
```

```
#set($e=$TMSsystem.currentTimeInIOSFormat())
The current time in IOS format is : $e
```

getting the octets from the ipaddress

```
#set($c="10.33.4.5")
#set($e=$TMSsystem.getOctet1($c))
The first Octet of $c is $e
#set($e=$TMSsystem.getOctet2($c))
The second Octet of $c is $e
#set($e=$TMSsystem.getOctet3($c))
The third Octet of $c is $e
#set($e=$TMSsystem.getOctet4($c))
The fourth Octet of $c is $e
```

The variables are declared as strings, integers, or sub-templates accordingly.

The Output of the above template body is:

```
interface Fast_ethernet

10
11
12
13

interface Loopback1
description By VPN-SC
ip vrf forwarding V31:eigrpfm
ip address 10.11.20.34 255.255.255.255
no ip directed-broadcast

interface Loopback1
description By VPN-SC
ip vrf forwarding V31:eigrpfm
ip address 20.45.230.145 255.255.255.255
no ip directed-broadcast
```

```
The Address of 10.33.4.5/30 is 10.33.4.5
The mask of 10.33.4.5/30 is 255.255.255.252
The Reverse mask of 10.33.4.5/30 is 0.0.0.3
The network address of 10.33.4.5/30 is 10.33.4.4
```

The current time in IOS format is: 00:17:01 21 Aug 2006

```
-----
getting the octets from the ipaddress
The first Octet of 10.33.4.5 is 10
The second Octet of 10.33.4.5 is 33
The third Octet of 10.33.4.5 is 4
The fourth Octet of 10.33.4.5 is 5
```

Usage of a Macro

The body of the template contains:

This example illustrates the usage of macro

```
#macro(community $CL $bgp-list)
#foreach($bgp in $bgp-list)
ip $CL standard permit $bgp
#end
#end

#set($bgp_list = "20:10","30:10","40:10","50:10")
#set($CL = "community-list")
```

```
#community($CL $bgp_list)
```

The Output is obtained as:

```
ip community-list standard permit 20:10
ip community-list standard permit 30:10
ip community-list standard permit 40:10
ip community-list standard permit 50:10
```

Usage of Subtemplates

The body of the template is as follows:

```
## This example illustrates the usage of the sub-template
```

```
$a.callWithDatafile("data1")
```

The screenshot shows a 'Template Editor' window. It contains the following fields:

- Template Name:** /demo/demo_subtemplate
- Description:** demonstrates the usage of subtemplate
- Body:**

```
## This example illustrates the usage of the sub-template

$a.callWithDatafile("data1")
```

At the bottom, there are two checkboxes: 'Required Fields' (checked) and 'Has User Section' (unchecked).

The variable **a** is declared as a subtemplate. The datafile provided here, **data**, must be a datafile for the template **a**, which must also exist. In the datafile of the main template, the path of the subtemplate is specified.

General	
Template:	/demo/demo_subtemplate
Data File Name:	data_file
Description:	sub-template
Variables	
a *	/sample/demo_strings (Sub-Template)
*Required Fields ☐ Display Optional Variables	
Save Configlet Close	

In the datafile of the main template, the specified path of the subtemplate might be the same directory or a different directory.

Can I see more examples?



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.
ATMoMPLS	Asynchronous Transfer Mode over Multi-Protocol Label Switching. A type of Layer 2 point-to-point connection running over an MPLS core.
AToM	Any Transport over MPLS.
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.

A

autonomous system See [AS](#).

autonomous system number See *ASN*.

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.

CDP Cisco Discovery Protocol. A protocol that is used to discover IOS devices in a network. One of the choices of method for performing device discovery in the ISC Discovery process.

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.

C

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.
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 <i>DLCI</i> .
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).
Device/Topology Based Discovery	One of the methods available for performing ISC device discovery. The Device/Topology Discovery method uses an XML file that provides device names and IP addresses and another XML file that provides information on the interface connections between devices in the network topology.
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.
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 BGP) communicate among different network domains.
egress	Traffic leaving the network or device.
E-LAN	An Ethernet LAN Service Type representing a multipoint-to-multipoint Ethernet service in a Metro Ethernet network.
E-Line	An Ethernet Line Service Type representing a point-to-point Ethernet service in a Metro Ethernet network.
EMS	Ethernet Multipoint Service is a port-based multipoint-to-multipoint E-LAN service that is used for transparent LAN applications.
EPL	Ethernet Private Line is a port-based point-to-point E-Line service that maps Layer 2 traffic directly on to a TDM circuit.
ERMS	Ethernet Relay Multipoint Service is a multipoint-to-multipoint VLAN-based E-LAN service that is used primarily for establishing a multipoint-to-multipoint connection between customer routers.
ERS	Ethernet Relay Service is a point-to-point LAN-based E-Line service that is used primarily for establishing a point-to-point connection between customer routers.
Ethernet LAN Service Type	See E-LAN .
Ethernet Line Service Type	See E-Line .
Ethernet Multipoint Service	See EMS .
Ethernet Private Line	See EPL .
Ethernet Relay Multipoint Service	See ERMS .
Ethernet Relay Service	See ERS .
Ethernet Virtual Connection	See EVC .
Ethernet Wire Service	See EWS .
EVC	An Ethernet Virtual Connection in Metro Ethernet with an association of two or more UNIs that limits the exchange of service frames to UNIs within the EVC.
EWS	Ethernet Wire Service is a point-to-point port-based E-Line service that is used primarily to connect geographically remote LANs over a service provider network.

E

Extensible Markup Language See [XML](#).

EWS An Ethernet Wire Service is a point-to-point-based E-Line service that is used primarily to connect geographically remote LANs over a Service Provider network.

exterior border gateway protocol See [EBGP](#).

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.

FRoMPLS Frame Relay over Multi-Protocol Label Switching. A type of Layer 2 point-to-point connection running over an MPLS core.

G

Gigabit Switch Router See [GSR](#).

global pool The bandwidth of TE enabled interfaces is assigned a number of nested bandwidth pools. The global pool represents the total bandwidth that can be reserved 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 [HTTP](#).

HTTP Hypertext 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.

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.
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.
ISC	Cisco IP Solution Center.
ISC Discovery	An automated process that allows ISC to discover the devices in a MPLS VPN network or a L2VPN Metro Ethernet network.
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.

label-switched path See *LSP*.

link speed factor TE multiplication factor to be applied to the link speed to determine the amount of bandwidth that must be protected.

LSP Sequence of routers that cooperatively perform MPLS operations for a packet stream. The first router in an LSP is called the ingress router, and the last router in the path is called the egress router. An LSP is a point-to-point, half-duplex connection from the ingress router to the egress router. (The ingress and egress routers cannot be the same router.)

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*.

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.

Metro Ethernet Metro Ethernet services use Ethernet technology to deliver cost-effective, high-speed connectivity for metropolitan-area network (MAN) and wide-area network (WAN) applications.

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.

M

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.
multilink point-to-point protocol	See MLPP.
multipoint-to-multipoint	In Metro Ethernet, a connection type consisting of single multipoint-to-multipoint Ethernet circuits provisioned between two or more UNIs.
multi protocol label switching	See <i>MPLS</i> .
multi protocol label switching virtual private network	See <i>MPLS VPN</i> .
Multi-VRF CE	multi-VPN routing and forwarding tables CE (MVRFCCE) is a feature that provides for Layer 3 aggregation. Multiple CEs can connect to a single Multi-VRF CE (typically in an enterprise network); then the Multi-VRF CE connects directly to a PE.

N

network	In MPLS VPN Solution, a collection of targets with unique names.
Network-facing Provider Edge	See <i>N-PE</i> .
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 TEM'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.
N-PE	Network-facing Provider Edge within the Edge layer in a Metro Ethernet network.

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.

PE-AGG Provider edge aggregation (PE-AGG) within the Aggregation layer in a Metro Ethernet network.

permanent virtual circuit. See *PVC*.

Point-to-Point Ethernet A network architecture delivered with the Cisco Metro Ethernet offering. It supports both EWS and ERS services.

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 aggregation See *PE-AGG*.

provider edge router See *PE*.

P

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.
Residual Bandwidth Reservation	The discrepancy between bandwidth reservations discovered for each link and bandwidth reserved by tunnels that ISC is aware of.
response time reporter	Renamed to service assurance agent (SA Agent).
RG	The Route Generator is a placement tool used in ISC Traffic Engineering Management to achieve optimization and bandwidth protection in the network.
RIP	Routing Information Protocol. The simplest Interior Gateway Protocol (IGP) in the Internet.
round-trip time	See RTT .
route distinguisher	See RD .
Route Generator	See RG .
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.

R

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.
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.
Shared-Risk Link Group	See SRLG .
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.
SRLG	In Traffic Engineering, a Shared-Risk Link Group (SRLG) identifies links with common physical characteristics that could fail as a group during a single failure event.
Static route	Route that is explicitly configured and entered into the routing table. Static routes take precedence over routes chosen by dynamic routing protocols.
storm control	Interface configuration settings to help prevent a UNI port from being disrupted by a broadcast, multicast, or unicast storm.

S

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.
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.
TEM	Traffic Engineering Management is an ISC implementation of the Traffic Engineering (TE) technology.
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.

T

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.
U-PE	The User-facing Provider Edge within the Access layer in a Metro Ethernet network.
User Datagram Protocol	See UDP .
User-facing Provider Edge	See U-PE .
user role	A user role is a predefined or a user-specified role defining a set of permissions.

V

VCI	virtual channel identifier. Used in ATM networking concept.
virtual channel identifier	See VCI .
virtual LAN	See VLAN .
virtual path identifier	See VPI .
virtual private network	See VPN .
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.

V

VLAN Translation	A technique used to pass frames between subinterfaces with different VLAN IDs. This allows frames entering a device with one VLAN ID to exit with a different VLAN ID. VLAN translation provides flexibility in managing VLANs, as well as Metro Ethernet-related services. There are two types of VLAN translation—1 to 1 (1:1) and 2 to 1 (2:1).
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 VRF .
VRF definition	The configuration information for a VPN routing/forwarding instance (VRF) table for PEs that share a common route-target (RT) signature. In the VPN inventory repository, a VRF definition is a template by which to define a VRF table in a PE .
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).



INDEX

A

aagent properties [C-36](#)
access control list, defined [GL-1](#)
access domains
 creating [3-125, 4-51](#)
accessing
 reports [7-43](#)
 Topology Tool for ISC-VPN topology [3-44](#)
ACL, defined [GL-1](#)
administration, overview [9-1](#)
Administration tab [1-15](#)
Aggregate view [3-48](#)
antialiasing, defined [GL-1](#)
API, defined [GL-1](#)
appliances, Cisco CNS IE2100 [A-1](#)
Application Programming Interface, defined [GL-1](#)
area, defined [GL-1](#)
AS, defined [GL-1](#)
ASN, defined [GL-1](#)
assigning
 CE roles [4-44](#)
 device roles [4-40](#)
 devices [3-36](#)
 PE roles [4-41](#)
ATM, defined [GL-1](#)
ATMoMPLS, defined [GL-1](#)
AToM, defined [GL-1](#)
attributes
 general device attributes [3-9](#)
 XML [B-1](#)
auditing, tasks [7-5](#)
audit SR (TE), defined [GL-1](#)

auto bandwidth / auto-bw, defined [GL-1](#)
AutoDiscovery property [C-1](#)
autonomous system, defined [GL-2](#)
autonomous system number, defined [GL-2](#)

B

backing store, defined [GL-2](#)
baseline, defined [GL-2](#)
BECN, defined [GL-2](#)
BGP, defined [GL-2](#)
Border Gateway Protocol, defined [GL-2](#)
border router, defined [GL-2](#)

C

CAR, defined [GL-2](#)
CDP, defined [GL-2](#)
CDP discovery [4-17](#)
CE, defined [GL-2](#)
CEF, defined [GL-2](#)
CERC, defined [GL-3](#)
CERC membership, defined [GL-3](#)
CERCs
 accessing the CE Routing Communities
 window [3-137](#)
 creating [3-138](#)
 deleting [3-139](#)
CE routing communities (see CERCs) [3-136](#)
CE Routing Communities window [3-137](#)
CEs
 assigning the CE role [4-44](#)
 editing the CE role [4-46](#)

- opening and editing [3-26](#)
- saving role assignment information [4-49](#)
- cfr properties [C-37](#)
- CIM, defined [GL-3](#)
- CIM-CX, defined [GL-3](#)
- CIR, defined [GL-3](#)
- Cisco CNS IE2100 appliances [A-1](#)
 - creating [3-96, A-1](#)
 - plug-and-play [A-7](#)
- Cisco Service Management, defined [GL-3](#)
- Cleanup properties [C-1](#)
- CNS [A-3](#)
 - customer attributes [3-32](#)
 - device attributes [3-12](#)
 - provider attributes [3-22](#)
- collection zones [9-26](#)
- commands
 - download [5-2](#)
 - EXEC [5-10](#)
 - startdb [2-1](#)
 - startns [2-2](#)
 - startwd [2-2](#)
 - stopall [2-3](#)
 - stopdb [2-3](#)
 - stopns [2-4](#)
 - stopwd [2-4](#)
 - WatchDog [2-1](#)
 - wdclient [2-5](#)
 - wdclient disk [2-5](#)
 - wdclient group [2-6](#)
 - wdclient groups [2-6](#)
 - wdclient health [2-6](#)
 - wdclient restart [2-7](#)
 - wdclient start [2-7](#)
 - wdclient status [2-8](#)
 - wdclient stop [2-10](#)
- committed access rate, defined [GL-3](#)
- config button, used to view DCPL properties [9-23](#)
- configlet, defined [GL-3](#)

- config task, for discovered devices [4-79](#)
- configuring
 - SSH [3-72](#)
 - SSHv2 [3-72](#)
- conformant tunnel, defined [GL-3](#)
- Control Center, overview [9-21](#)
- conventions
 - Topology Tool [3-41](#)
- copying
 - devices [3-104](#)
 - templates [6-13](#)
 - user roles [9-13](#)
 - users [9-6](#)
- CORBA, defined [GL-3](#)
- CPE devices (see CPEs) [3-116](#)
- CPEs
 - creating [3-117](#)
 - customer attributes [3-34](#)
 - deleting [3-119](#)
 - editing [3-118](#)
- creating [3-124](#)
 - access domains [3-125, 4-51](#)
 - Catalyst switch devices [3-80](#)
 - CERCs [3-138](#)
 - Cisco CNS IE2100 appliances [A-1](#)
 - CiscoCNS IE2100 devices [3-96](#)
 - Cisco devices [3-85](#)
 - Cisco IOS devices [A-3](#)
 - CPEs [3-117](#)
 - customers [3-112](#)
 - customer sites [3-115](#)
 - custom reports [7-47](#)
 - data files [6-13](#)
 - device groups [3-106](#)
 - devices [3-79](#)
 - folders for templates [6-4](#)
 - IP address pools [3-128](#)
 - multicast pools [3-129](#)
 - NPC rings [3-150](#)

- NPCs [3-146](#)
- object groups [9-16](#)
- PEs [3-124](#)
- provider regions [3-123](#)
- providers [3-120](#)
- resource pools [4-51](#)
- route distinguisher and route target pools [3-130](#)
- site of origin pools [3-132](#)
- tasks [7-3](#)
- templates [6-5](#)
- terminal servers [3-91](#)
- user groups [9-8](#)
- user roles [9-11](#)
- users [9-3](#)
- VC ID pools [3-134](#)
- VLAN pools [3-134](#)
- VPNs [3-141](#), [4-62](#)
- CSM, defined [GL-3](#)
- customer, defined [GL-3](#)
- customer edge router, defined [GL-3](#)
- customer edge routing community, defined [GL-3](#)
- customer network, defined [GL-3](#)
- customers
 - accessing the Customers window [3-112](#)
 - CNS attributes [3-32](#)
 - CPE attributes [3-34](#)
 - creating [3-112](#)
 - creating customer sites [3-115](#)
 - deleting [3-114](#)
 - editing [3-113](#)
 - general attributes [3-29](#)
 - interfaces [3-35](#)
 - overview [3-111](#)
 - password attributes [3-30](#)
 - platform attributes [3-33](#)
 - SNMP attributes [3-31](#)
- customer site, defined [GL-3](#)

D

- data files, creating [6-13](#)
- data-link connection identifier, defined [GL-4](#)
- data model, defined [GL-4](#)
- dCEF, defined [GL-4](#)
- DCPL properties
 - aagent [C-36](#)
 - AutoDiscovery [C-1](#)
 - cfr [C-37](#)
 - Cleanup [C-1](#)
 - DCS [C-3](#)
 - DeploymentFlow [C-8](#)
 - Discovery [C-8](#)
 - DistributionFramework [C-12](#)
 - GSAM [C-14](#)
 - GTL [C-14](#)
 - GUI [C-16](#)
 - how to view [9-23](#)
 - JavaWebStart [C-19](#)
 - lockmanager [C-37](#)
 - Logging [C-19](#)
 - nbi [C-38](#)
 - notification [C-40](#)
 - pal [C-41](#)
 - Provisioning [C-20](#)
 - repository [C-41](#)
 - Scheduler [C-33](#)
 - Services [C-33](#)
 - SLA [C-31](#)
 - SnmpService [C-33](#)
 - SYSTEM [C-31](#)
 - TaskManager [C-36](#)
 - TE [C-34](#)
 - TE Topology [C-35](#)
 - VpnInvServer [C-36](#)
 - watchdog [C-44](#)
 - xml [C-54](#)
- DCS properties [C-3](#)

deleting

- CERCs [3-139](#)
- CPEs [3-119](#)
- customers [3-114](#)
- device groups [3-109](#)
- devices [3-100](#)
- devices from NPCs [4-56](#)
- NPC rings [3-154](#)
- NPCs [3-150](#)
- object groups [9-17](#)
- providers [3-122](#)
- resource pools [3-136](#)
- rings from NPCs [4-56](#)
- SLA probes [7-31](#)
- tasks [7-7](#)
- templates [6-20](#)
- user groups [9-9](#)
- user roles [9-14](#)
- users [9-6](#)
- VPNs [3-144](#)

DeploymentFlow property [C-8](#)

device.xml (file used in discovery) [4-22](#)

Device/Topology Based Discovery, defined [6L-4](#)

Device Console [5-1](#)

- device configuration manager [5-8](#)
- download commands [5-2](#)
- download template [5-3](#)
- EXEC commands [5-10](#)
- reload [5-13](#)

device groups

- accessing the Device Groups window [3-106](#)
- creating a device group [3-106](#)
- deleting [3-109](#)
- editing [3-109](#)
- e-mailing device groups [3-110](#)
- overview [3-105](#)

devices

- accessing the Devices window [3-77](#)
- adding to NPCs [4-54](#)

adding to rings [4-55](#)

assigning [3-36](#)

assigning device roles [4-40](#)

changing device assignments [4-40](#)

Cisco CNS IE2100 appliances [A-1](#)

CNS attributes [3-12](#)

CNS device access protocol [A-3](#)

collection zones for [9-26](#)

commit discovered devices to the ISC repository [4-78](#)

config task for discovered devices [4-79](#)

configuring SSH or SSHv2 [3-72](#)

copying [3-104](#)

creating [3-79](#)

creating a Catalyst switch [3-80](#)

creating a Cisco CNS IE2100 [3-96](#)

creating a Cisco device [3-85](#)

creating Cisco IOS devices [A-3](#)

creating terminal servers [3-91](#)

deleting [3-100](#)

deleting from NPCs [4-56](#)

determining device roles through discovery [4-41](#)

device configuration manager [5-8](#)

editing [3-97](#)

editing device configurations [3-101](#)

editing device configurations for discovery [4-31](#)

e-mailing a device owner [3-103](#)

enabling RTR responder [3-77](#)

general attributes [3-9](#)

importing [3-6](#)

initiating role assignment [4-38](#)

interfaces [3-14](#)

logical [3-57](#)

opening and editing [3-7](#)

password attributes [3-10](#)

physical [3-58](#)

platform attributes [3-13](#)

properties [3-57](#)

saving configurations for discovery [4-37](#)

setting general attributes for discovery [4-35](#)

- setting up SNMP [3-75](#)
 - SNMP attributes [3-11](#)
 - viewing properties [3-56](#)
 - working with [3-71](#)
- Devices window, accessing [3-77](#)
- DHCP, defined [GL-4](#)
- diagnostics, overview [8-1](#)
- Diagnostics tab [1-14, 8-1](#)
- disabling, SLA probes [7-34](#)
- discovery
 - assigning devices individually or in bulk [4-40](#)
 - assigning the CE role [4-44](#)
 - assigning the PE role [4-41](#)
 - CDP [4-17](#)
 - changing device assignments [4-40](#)
 - changing the device assignment display [4-39](#)
 - CNS attributes [4-36](#)
 - commit devices and services to the ISC repository [4-78](#)
 - config task for discovered devices [4-79](#)
 - data collection [4-37](#)
 - determine device roles [4-41](#)
 - device.xml file [4-22](#)
 - device role assignment [4-37](#)
 - editing device configurations [4-31](#)
 - editing the CE role [4-46](#)
 - editing the PE role [4-43](#)
 - edit services [4-79](#)
 - end-to-end wires, deleting [4-74](#)
 - end-to-end wires, editing [4-72](#)
 - end-to-end wires, joining [4-74](#)
 - end-to-end wires, splitting [4-73](#)
 - end-to-end wires, viewing discovered end-to-end wires [4-70](#)
 - general device attributes [4-35](#)
 - general notes [4-6](#)
 - initiating role assignment [4-38](#)
 - installing licenses [4-17](#)
 - issues in large networks [4-17](#)
 - L2VPNs [4-7, 4-66](#)
 - deleting discovered services by VPN [4-70](#)
 - editing discovered services by VPN [4-69](#)
 - saving policies and initiating service creation [4-78](#)
 - viewing discovered services by VPN [4-67](#)
 - MDE [4-7](#)
 - MPLS VPN, service creation [4-65](#)
 - MPLS VPNs [4-6](#)
 - MPLS VPNs, saving [4-65](#)
 - MPLS VPN service discovery [4-57](#)
 - NPC assignment [4-52](#)
 - NPCs [4-50](#)
 - overview [4-1](#)
 - password attributes [4-33](#)
 - performing [4-25](#)
 - policy.xml file [4-19](#)
 - preliminary steps [4-15](#)
 - saving device configurations [4-37](#)
 - saving role assignment information [4-49](#)
 - starting [4-26](#)
 - summary of tasks for MPLS VPN and L2VPN discovery [4-8](#)
 - summary tasks for MDE discovery [4-12](#)
 - system requirements [4-16](#)
 - technical notes [4-5](#)
 - TEM [4-8](#)
 - topology.xml file [4-23](#)
 - using the discovery log files [4-6](#)
 - view services [4-79](#)
 - VPLS links, deleting [4-77](#)
 - VPLS links, editing [4-76](#)
 - VPLS links, viewing [4-74](#)
 - XML file samples [4-19](#)
 - XML files required for [4-19](#)
- Discovery properties [C-8](#)
- DistributionFramework properties [C-12](#)
- DLCI, defined [GL-4](#)
- DMTF, defined [GL-4](#)

DNS, defined [GL-4](#)
 document type definition, defined [GL-4](#)
 Domain Naming System, defined [GL-4](#)
 double buffer, defined [GL-4](#)
 DRAM, defined [GL-4](#)
 DSCP, defined [GL-4](#)
 DTD, defined [GL-4](#)
 Dynamic Host Configuration Protocol, defined [GL-4](#)
 dynamic path, defined [GL-4](#)
 dynamic random-access memory, defined [GL-4](#)

E

EBGP, defined [GL-5](#)
 editing
 CEs [3-26](#)
 CPEs [3-118](#)
 customers [3-113](#)
 device configurations [3-101](#)
 device configurations for discovery [4-31](#)
 device groups [3-109](#)
 devices [3-7, 3-97](#)
 discovered services [4-79](#)
 inter-N-PE interfaces [4-51](#)
 NPC rings [3-154](#)
 object groups [9-17](#)
 PEs [3-16](#)
 providers [3-121](#)
 templates [6-18](#)
 user groups [9-8](#)
 user roles [9-14](#)
 users [9-6](#)
 egress, defined [GL-5](#)
 E-LAN, defined [GL-5](#)
 E-Line, defined [GL-5](#)
 e-mailing, reports [7-46](#)
 EMS, defined [GL-5](#)
 enabling
 RTR responder [3-77](#)

SLA probes [7-32](#)
 traps [7-33](#)
 end-to-end wires
 [4-70](#)
 deleting [4-74](#)
 editing [4-72](#)
 joining [4-74](#)
 splitting [4-73](#)
 EPL, defined [GL-5](#)
 ERMS, defined [GL-5](#)
 ERS, defined [GL-5](#)
 Ethernet LAN Service Type, defined [GL-5](#)
 Ethernet Line Service Type, defined [GL-5](#)
 Ethernet Multipoint Service, defined [GL-5](#)
 Ethernet Private Line, defined [GL-5](#)
 Ethernet Relay Multipoint Service, defined [GL-5](#)
 Ethernet Relay Service, defined [GL-5](#)
 Ethernet Virtual Connection, defined [GL-5](#)
 Ethernet Wire Service, defined [GL-5](#)
 EVC, defined [GL-5](#)
 EWS, defined [GL-5, GL-6](#)
 examples, templates [6-22](#)
 EXEC command [5-10](#)
 exporting
 reports [7-46](#)
 templates [6-36](#)
 Extensible Markup Language, defined [GL-6](#)
 exterior border gateway protocol, defined [GL-6](#)

F

Fast Re-Route (FRR) protection, defined [GL-6](#)
 filtering
 for reports [7-43](#)
 MPLS VPN view [4-59](#)
 topology views [3-63](#)
 filters [1-7](#)
 folders
 copying template folders [6-4](#)

creating [6-4](#)
 FRoMPLS, defined [GL-6](#)

G

getting started [1-1](#)
 Gigabit Switch Router, defined [GL-6](#)
 global pool, defined [GL-6](#)
 graphical user interface (see GUI elements) [1-1](#)
 grooming, defined [GL-6](#)
 GSAM property [C-14](#)
 GSR, defined [GL-6](#)
 GTL properties [C-14](#)
 GUI elements
 about [1-6](#)
 accounts [1-5](#)
 Administration tab [1-15, 9-1](#)
 auto refresh [1-8](#)
 color coding [1-8](#)
 common components [1-7](#)
 customer [1-6](#)
 Device Console [5-1](#)
 Diagnostics tab [1-14, 8-1](#)
 filters [1-7](#)
 go to page [1-7](#)
 header row check box [1-7](#)
 help [1-6](#)
 home [1-3](#)
 icons [1-10](#)
 index [1-5](#)
 introduction [1-1](#)
 links [1-3](#)
 logout [1-6](#)
 Monitoring tab [1-13](#)
 Product Category tabs [1-3](#)
 rows per page [1-7](#)
 Security window [9-1](#)
 Service Design tab [1-12, 6-1](#)
 Service Inventory tab [1-10](#)

shortcuts [1-3](#)
 structural overview [1-2](#)
 using the reports GUI [7-43](#)

GUI properties [C-16](#)

H

help, invoking help for reports [7-47](#)
 hold priority, defined [GL-6](#)
 hosts
 details [9-22](#)
 viewing status information [9-21](#)
 HTTP, defined [GL-6](#)
 HTTPS, defined [GL-6](#)
 Hyper text Transfer Protocol, defined [GL-6](#)

I

IANA, defined [GL-7](#)
 IBGP, defined [GL-7](#)
 ICMP, defined [GL-7](#)
 icons [1-10](#)
 IDL, defined [GL-7](#)
 importing
 devices [3-6](#)
 templates [6-36](#)
 information model, defined [GL-7](#)
 ingress, defined [GL-7](#)
 installing
 licences [4-17](#)
 license keys [9-28](#)
 Interface Definition Language, defined [GL-7](#)
 interfaces [3-59](#)
 customers [3-35](#)
 devices [3-14](#)
 provider [3-25](#)
 interior border gateway protocol, defined [GL-7](#)
 Internet Control Message Protocol, defined [GL-7](#)

internet-service provider, defined [GL-7](#)

inter-switch link, defined [GL-7](#)

Inventory and Connection Manager [3-1](#)

Inventory Manager [3-5](#)

Inventory Manager window [3-5](#)

IOS XR

 configuring SSH or SSHv2 on Cisco IOS XR
 routers [3-73](#)

IP address pools, creating [3-128](#)

IPv4, defined [GL-7](#)

IPv6, defined [GL-7](#)

ISC

 service discovery (see discovery) [4-1](#)

 XML reference [B-1](#)

ISC, defined [GL-7](#)

ISC Discovery, defined [GL-7](#)

ISC-VPN topology, accessing [3-44](#)

ISL, defined [GL-7](#)

ISP, defined [GL-7](#)

J

JavaWebStart properties [C-19](#)

L

L2TPv3, defined [GL-8](#)

L2VPN, defined [GL-8](#)

L2VPNs

 deleting discovered services by VPN [4-70](#)

 discovery [4-7, 4-8, 4-66](#)

 editing discovered services by VPN [4-69](#)

 saving policies and initiating service creation [4-78](#)

 viewing discovered services by VPN [4-67](#)

label-switched path, defined [GL-8](#)

launching, Topology Tool [3-39](#)

layers [3-69](#)

licenses

 installing license keys [9-28](#)

 required for discovery [4-17](#)

links

 properties [3-60](#)

 viewing [3-56](#)

 viewing VPN link details [4-64](#)

link speed factor, defined [GL-8](#)

lockmanager properties [C-37](#)

log files, using for discovery [4-6](#)

logging out [1-6](#)

Logging properties [C-19](#)

logical

 devices [3-57](#)

 view [3-52](#)

logs

 task logs [7-7](#)

 user access logs [9-31](#)

 viewing master server logs [9-26](#)

 watchdog [9-25](#)

LSP, defined [GL-8](#)

M

macros, using in templates [D-9](#)

managed tunnel, defined [GL-8](#)

manage lock, defined [GL-8](#)

management information base, defined [GL-8](#)

managing

 object groups [9-15](#)

 TIBCO rendezvous [9-33](#)

 user groups [9-7](#)

 user roles [9-9](#)

 users [9-2](#)

maps [3-67](#)

 adding new maps [3-71](#)

 data [3-70](#)

 loading [3-68](#)

master servers (see servers) [9-24](#)

MCE, defined [GL-8](#)

MDEdiscovery [4-12](#)MDE, discovery [4-7](#)Metro Ethernet, defined [GL-8](#)MIB, defined [GL-8](#)MLPPP, defined [GL-8](#)monitoring, overview [7-1](#)Monitoring tab [1-13](#)MPE, defined [GL-8](#)MPLS, defined [GL-8](#)MPLS Diagnostics Expert (see MDE) [4-7](#)MPLS TE tunnel, defined [GL-8](#)MPLS VPN, defined [GL-9](#)**MPLS VPNs**filtering the MPLS VPN view [4-59](#)properties [3-62](#)service discovery [4-57](#)MPLS VPNs (see also VPNs) [4-6](#)multicast pools, creating [3-129](#)multilink point-to-point protocol, defined [GL-9](#)multipoint-to-multipoint, defined [GL-9](#)multi protocol label switching, defined [GL-9](#)multi protocol label switching virtual private network,
defined [GL-9](#)Multi-VRF CE, defined [GL-9](#)

Nnamed physical circuits (see NPCs) [3-144](#)Named Physical Circuits Window [3-145](#)nbi properties [C-38](#)network, defined [GL-9](#)Network-facing Provider Edge, defined [GL-9](#)network management subnet, defined [GL-9](#)nodes, locations of [3-70](#)non-conformant tunnel, defined [GL-9](#)notification properties [C-40](#)**NPCs**accessing the Named Physical Circuits
Window [3-145](#)adding devices to [4-54](#)adding rings to [4-55](#)creating [3-146](#)creating NPC rings [3-150](#)deleting [3-150](#)deleting a device or a ring [4-56](#)deleting NPC rings [3-154](#)discovering [4-50](#)editing NPC rings [3-154](#)inserting a device [4-56](#)inserting a ring [4-56](#)saving configurations [4-57](#)starting assignment of NPCs for discovery [4-52](#)N-PE, defined [GL-9](#)N-PEs, editing inter-N-PE interfaces [4-51](#)

O**object groups**creating [9-16](#)deleting [9-17](#)editing [9-17](#)managing [9-15](#)operations support system, defined [GL-10](#)OSS, defined [GL-10](#)**output**reports fields [7-44](#)using output from reports [7-45](#)

PPAD, defined [GL-10](#)pal properties [C-41](#)**passwords**customer attributes [3-30](#)device attributes [3-10](#)

- provider attributes [3-19](#)
 - setting attributes for discovery [4-33](#)
- PE, defined [GL-10](#)
- PE-AGG, defined [GL-10](#)
- permanent virtual circuit, defined [GL-10](#)
- PEs [3-124](#)
 - assigning the PE role [4-41](#)
 - editing the PE role [4-43](#)
 - opening and editing [3-16](#)
 - provider attributes [3-24](#)
 - saving role assignment information [4-49](#)
- physical
 - devices [3-58](#)
 - view [3-55](#)
- ping [7-8](#)
- platform
 - customer attributes [3-33](#)
 - device attributes [3-13](#)
 - provider attributes [3-23](#)
- plug-and-play, for Cisco CNS IE2100 appliances [A-7](#)
- Point-to-Point Ethernet, defined [GL-10](#)
- policies [6-1](#)
- policy.xml (file used in discovery) [4-19](#)
- printing, reports [7-46](#)
- probes (see also SLA probes) [7-12](#)
- projection (topology map), defined [GL-10](#)
- propagation delay, defined [GL-10](#)
- properties [3-59](#)
 - aagent [C-36](#)
 - AutoDiscovery [C-1](#)
 - cfr [C-37](#)
 - Cleanup [C-1](#)
 - DCS [C-3](#)
 - DeploymentFlow [C-8](#)
 - devices [3-57](#)
 - Discovery [C-8](#)
 - DistributionFramework [C-12](#)
 - GSAM [C-14](#)
 - GTL [C-14](#)
 - GUI [C-16](#)
 - JavaWebStart [C-19](#)
 - links [3-60](#)
 - lockmanager [C-37](#)
 - Logging [C-19](#)
 - nbi [C-38](#)
 - notification [C-40](#)
 - pal [C-41](#)
 - Provisioning [C-20](#)
 - repository [C-41](#)
 - Scheduler [C-33](#)
 - Services [C-33](#)
 - SLA [C-31](#)
 - SnmpService [C-33](#)
 - SYSTEM [C-31](#)
 - TaskManager [C-36](#)
 - TE [C-34](#)
 - TE Topology [C-35](#)
 - VpnInvServer [C-36](#)
 - watchdog [C-44](#)
 - xml [C-54](#)
- properties (see DCPL properties) [C-1](#)
- provider, defined [GL-10](#)
- Provider Administrative Domain, defined [GL-10](#)
- Provider edge aggregation, defined [GL-10](#)
- provider edge router, defined [GL-10](#)
- provider network, defined [GL-11](#)
- providers
 - accessing the Providers window [3-120](#)
 - CNS attributes [3-22](#)
 - creating [3-120](#)
 - creating access domains [3-125](#)
 - creating PE devices [3-124](#)
 - creating provider regions [3-123](#)
 - deleting [3-122](#)
 - editing [3-121](#)
 - general attributes [3-18](#)
 - interfaces [3-25](#)
 - overview [3-119](#)

- password attributes [3-19](#)
- PE attributes [3-24](#)
- platform attributes [3-23](#)
- SNMP attributes [3-21](#)
- Providers window [3-120](#)
- Provisioning properties [C-20](#)
- PVC, defined [GL-11](#)

Q

- QoS, defined [GL-11](#)
- quality of Service, defined [GL-11](#)

R

- RD, defined [GL-11](#)
- region, defined [GL-11](#)
- regions, creating provider regions [3-123](#)
- reports
 - accessing [7-43](#)
 - CoS report [7-40](#)
 - custom reports, creating [7-47](#)
 - e-mailing [7-46](#)
 - exporting [7-46](#)
 - filters [7-43](#)
 - HTTP Cos [7-41](#)
 - HTTP report [7-39](#)
 - invoking help [7-47](#)
 - jitter CoS report [7-41](#)
 - jitter report [7-39](#)
 - layout [7-43](#)
 - output fields [7-44](#)
 - overview [7-41, 7-42](#)
 - printing [7-46](#)
 - running [7-44](#)
 - SLA probes [7-36](#)
 - sorting [7-44](#)
 - summary report [7-36](#)

- using output from [7-45](#)
 - using the reports GUI [7-43](#)
- repository properties [C-41](#)
- repository variables, summary [6-23](#)
- Residual Bandwidth Reservation, defined [GL-11](#)
- resource pools
 - accessing the Resource Pools window [3-127](#)
 - creating [4-51](#)
 - creating IP address pools [3-128](#)
 - creating multicast pools [3-129](#)
 - creating route distinguisher and route target pools [3-130](#)
 - creating site of origin pools [3-132](#)
 - creating VC ID pools [3-134](#)
 - creating VLAN pools [3-134](#)
 - deleting [3-136](#)
 - overview [3-126](#)
- Resource Pools window [3-127](#)
- response time reporter, defined [GL-11](#)
- RG, defined [GL-11](#)
- rings
 - deleting from NPCs [4-56](#)
 - inserting into NPCs [4-56](#)
- RIP, defined [GL-11](#)
- roles, assignment with discovery [4-37](#)
- round-trip time, defined [GL-11](#)
- route distinguisher, defined [GL-11](#)
- route distinguisher pools, creating [3-130](#)
- Route Generator, defined [GL-11](#)
- route target, defined [GL-11](#)
- route target pools, creating [3-130](#)
- Routing Information Protocol, defined [GL-11](#)
- RT, defined [GL-11](#)
- RTR, defined [GL-12](#)
- RTT, defined [GL-12](#)
- rules, XML [B-1](#)
- running, reports [7-44](#)

S

- SA Agent, defined [GL-12](#)
- saving, NPC configurations [4-57](#)
- Scheduler properties [C-33](#)
- scheduling, tasks [7-6](#)
- schema, defined [GL-12](#)
- searching, topology views [3-66](#)
- Security window [9-1](#)
- seed router, defined [GL-12](#)
- servers
 - collection zones [9-26](#)
 - creating terminal servers [3-91](#)
 - logs [9-26](#)
 - viewing status information [9-24](#)
- Service Assurance Agent, defined [GL-12](#)
- service design
 - policies [6-1](#)
 - templates [6-2](#)
- Service Design tab [1-12, 6-1](#)
- service discovery, overview [4-1](#)
- Service Inventory tab [1-10, 3-1](#)
- service level agreement (see SLAs) [7-11](#)
- service level agreement, defined [GL-12](#)
- service requests [3-2](#)
- Services property [C-33](#)
- setup priority, defined [GL-12](#)
- Shared-Risk Link Group, defined [GL-12](#)
- site, defined [GL-12](#)
- site of origin pools, creating [3-132](#)
- SLA, defined [GL-12](#)
- SLA probes
 - deleting [7-31](#)
 - disabling [7-34](#)
 - enabling [7-32](#)
 - HTTP CoS report [7-41](#)
 - HTTP report [7-39](#)
 - jitter CoS report [7-41](#)
 - jitter report [7-39](#)
 - protocols supported [7-24](#)
 - reports [7-36](#)
 - summary CoS report [7-40](#)
 - summary report [7-36](#)
 - traps, disabling [7-35](#)
 - traps, enabling [7-33](#)
 - viewing details [7-30](#)
- SLAs
 - overview [7-11](#)
 - probes (see SLA probes) [7-12](#)
 - properties of [C-31](#)
 - setup tasks [7-12](#)
- SNMP
 - customer attributes [3-31](#)
 - device attributes [3-11](#)
 - provider attributes [3-21](#)
 - setting up on devices [3-75](#)
- SNMP, defined [GL-12](#)
- SnmpService properties [C-33](#)
- SOAP, defined [GL-12](#)
- sorting, reports [7-44](#)
- SP, defined [GL-12](#)
- splitting, VPNs [4-59](#)
- SRLG, defined [GL-12](#)
- SSH, configuring [3-72](#)
- SSHv2, configuring [3-72](#)
- startdb command [2-1](#)
- starting, Task Manager [7-2](#)
- startns command [2-2](#)
- startwd command [2-2](#)
- Static route, defined [GL-12](#)
- status
 - viewing host status [9-21](#)
 - viewing server status [9-24](#)
- stopall command [2-3](#)
- stopdb command [2-3](#)
- stopns command [2-4](#)
- stopwd command [2-4](#)
- storm control, defined [GL-12](#)

sub pool, defined [GL-13](#)
 subtemplates, how to use [D-10](#)
 switch, creating Catalyst switch devices [3-80](#)
 system path, defined [GL-13](#)
 SYSTEM properties [C-31](#)
 system recommendations [1-1](#)
 system requirements, for discovery [4-16](#)

T

tags, XML [B-1](#)
 target, defined [GL-13](#)
 target language, defined [GL-13](#)
 Task Manager
 auditing tasks [7-5](#)
 creating tasks [7-3](#)
 deleting tasks [7-7](#)
 displaying task details [7-6](#)
 logs [7-7](#)
 overview [7-1](#)
 properties [C-36](#)
 scheduling tasks [7-6](#)
 starting [7-2](#)
 tasks [7-2](#)
 tasks [7-2](#)
 auditing [7-5](#)
 config task for discovered devices [4-79](#)
 creating [7-3](#)
 deleting [7-7](#)
 displaying task details [7-6](#)
 TCP, defined [GL-13](#)
 TE
 properties [C-34](#)
 Topology properties [C-35](#)
 TE, defined [GL-13](#)
 TE discovery, defined [GL-13](#)
 TE explicit path, defined [GL-13](#)
 TE functional audit, defined [GL-13](#)
 TE link, defined [GL-13](#)
 TEM, defined [GL-13](#)
 TEM, discovery [4-8](#)
 TE metric, defined [GL-13](#)
 Template Manager, troubleshooting [D-1](#)
 templates
 copying [6-13](#)
 copying folders [6-4](#)
 creating [6-5](#)
 creating folders [6-4](#)
 deleting [6-20](#)
 download [5-3](#)
 editing [6-18](#)
 examples [6-22](#)
 importing and exporting [6-36](#)
 listing associated service requests [6-21](#)
 overview [6-2](#)
 repository variables [6-23](#)
 templates tree and data pane [6-3](#)
 troubleshooting [D-1](#)
 using macros [D-9](#)
 using strings [D-8](#)
 using subtemplates [D-10](#)
 TE node, defined [GL-13](#)
 TE policy, defined [GL-13](#)
 TE provider, defined [GL-13](#)
 terminal servers, creating [3-91](#)
 TE topology, defined [GL-13](#)
 TE traffic admission, defined [GL-13](#)
 TE tunnel, defined [GL-13](#)
 TIBCO rendezvous, managing [9-33](#)
 tools, topology (see Topology Tool) [3-38](#)
 topology
 logical devices [3-57](#)
 tool (see Topology Tool) [3-38](#)
 VPLS [3-50](#)
 topology.xml (file used in discovery) [4-23](#)
 Topology Tool [3-38](#)
 adding new maps [3-71](#)
 Aggregate view [3-48](#)

- conventions [3-41](#)
- device and link properties [3-56](#)
- device properties [3-57](#)
- filtering views [3-63](#)
- interface properties [3-59](#)
- introduction [3-39](#)
- launching [3-39](#)
- layers [3-69](#)
- links properties [3-60](#)
- loading maps [3-68](#)
- logical view [3-52](#)
- map data [3-70](#)
- maps [3-67](#)
- MPLS VPN properties [3-62](#)
- node locations [3-70](#)
- physical devices [3-58](#)
- physical view [3-55](#)
- searching views [3-66](#)
- views [3-46](#)
- VPLS view [3-50](#)
- VPN view [3-47](#)
- traffic engineering, performance report [7-41](#)
- Traffic Engineering Management (see also TEM) [3-5](#)
- Transmission Control Protocol, defined [GL-14](#)
- traps
 - disabling [7-35](#)
 - enabling [7-33](#)
- troubleshooting, templates [D-1](#)
- tunnel audit, defined [GL-14](#)
- tunnel placement, defined [GL-14](#)
- tunnel repair, defined [GL-14](#)

U

- UDP, defined [GL-14](#)
- unmanaged tunnel, defined [GL-14](#)
- U-PE, defined [GL-14](#)
- User Datagram Protocol, defined [GL-14](#)
- User-facing Provider Edge, defined [GL-14](#)

- user groups
 - creating [9-8](#)
 - deleting [9-9](#)
 - editing [9-8](#)
 - managing [9-7](#)
- user role, defined [GL-14](#)
- user roles
 - copying [9-13](#)
 - creating [9-11](#)
 - deleting [9-14](#)
 - design example [9-18](#)
 - editing [9-14](#)
 - managing [9-9](#)
- users
 - communicating with active users [9-30](#)
 - copying [9-6](#)
 - creating [9-3](#)
 - deleting [9-6](#)
 - editing [9-6](#)
 - managing [9-2](#)
 - user access log [9-31](#)
 - viewing activity of [9-31](#)
 - viewing details of [9-3](#)

V

- VCI, defined [GL-14](#)
- VC ID pools, creating [3-134](#)
- view, VPN [3-47](#)
- viewing
 - details of SLA probes [7-30](#)
 - device and link properties [3-56](#)
 - discovered services [4-79](#)
 - user details [9-3](#)
- views
 - Aggregate [3-48](#)
 - logical [3-52](#)
 - physical [3-55](#)
 - types of views [3-46](#)

virtual channel identifier, defined [GL-14](#)

virtual LAN, defined [GL-14](#)

virtual path identifier, defined [GL-14](#)

virtual private network, defined [GL-14](#)

VLAN, defined [GL-14](#)

VLANs pools, creating [3-134](#)

VLAN Translation, defined [GL-15](#)

VoIP, defined [GL-15](#)

VPI, defined [GL-15](#)

VPIM, defined [GL-15](#)

VPLS, defined [GL-15](#)

VPLS, topology [3-50](#)

VPLS links

- deleting [4-77](#)
- editing [4-76](#)
- viewing [4-74](#)

VPN, defined [GL-15](#)

VPN customer, defined [GL-15](#)

VpnInvServer properties [C-36](#)

VPN routing/forwarding instance, defined [GL-15](#)

VPNs

- accessing the VPNs window [3-140](#)
- creating [3-141, 4-62](#)
- deleting [3-144](#)
- discovery [4-6, 4-8](#)
- MPLS VPN properties [3-62](#)
- overview [3-140](#)
- service discovery [4-57](#)
- splitting [4-59](#)
- using ping command to check connectivity [7-8](#)
- view [3-47](#)
- viewing VPN link details [4-64](#)

VPNs window [3-140](#)

VRF, defined [GL-15](#)

VRF definition, defined [GL-15](#)

watchdog [9-25](#)

watchdog properties [C-44](#)

wdclient command [2-5](#)

wdclient disk subcommand [2-5](#)

wdclient groups subcommand [2-6](#)

wdclient group subcommand [2-6](#)

wdclient health subcommand [2-6](#)

wdclient restart subcommand [2-7](#)

wdclient start subcommand [2-7](#)

wdclient status subcommand [2-8](#)

wdclient stop subcommand [2-10](#)

WSDL, defined [GL-15](#)

X

XML

- reference [B-1](#)
- rules, tags and attributes in ISC [B-1](#)

XML, defined [GL-16](#)

XML API, defined [GL-16](#)

xml properties [C-54](#)

XML Schema, defined [GL-16](#)

W

WatchDog [2-1](#)

