Cisco Configuration Professional User Guide

Version 2.5

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

Customer Order Number:
Text Part Number: OL-20445-06

Cisco Configuration Professional User Guide

CONTENTS

Preface 65

Audience 1-65

Conventions 1-66

Related Documentation 1-67

Obtaining Documentation and Submitting a Service Request 1-68

PART 1 **Getting Started with Cisco Configuration Professional**

CHAPTER 1 **Getting Started** 1-1

Understanding Cisco CP 1-1

Understanding the Cisco CP User Interface 1-2

Window Layout 1-2

Menu Bar 1-3

Toolbar 1-4

Status Bar 1-6

Applications Menu Field Reference 1-7

Manage Community 1-7

Setting up a New Device 1-8

Managing Setup New Device 1-8

Setup New Device 1-9

User Profile 1-11

Options 1-12

Feature Use Tracking 1-14

Templates 1-15
Offline Mode 1-15
Additional Help Topics 1-18
USB Token PIN Settings 1-18
Deliver Configuration to Router 1-19
Communication Ports 1-20
Feature Unavailable 1-21

CHAPTER 2 **Device Communities** 2-1
Device Community Basic Workflow 2-1
Understanding Device Communities 2-2
Working with Communities 2-2
Adding Communities 2-4
Changing the Community Name 2-5
Deleting a Community 2-5
Exporting and Importing Communities 2-6
Managing the Devices in a Community 2-8
Working with Devices in a Community 2-8
Adding a Device to a Community 2-8
Editing Device Information 2-10
Deleting a Device from a Community 2-11
Discovering Devices 2-12
Displaying Discovery Process Details 2-14
Displaying Information About a Discovered Device 2-14
Device Community Reference 2-15
Manage Community Dialog Box 2-15
Change Default Credential Dialog Box 2-18
Community View Page 2-19
Manage Devices Dialog Box 2-22

Discovery Details Dialog Box 2-24
Router Status Dialog Box 2-26
Supplementary Information 2-28
Things to Know About Discovering Devices 2-28
Cisco CP Configuration Requirements 2-28
Wrong Secure Shell Version May Cause Discovery to Fail 2-30
Understanding Discovery Failed Error Messages 2-31
Cisco CP May Overwrite Existing Credentials 2-36
Proxy Server Settings Might Cause Discovery to Fail 2-37
Setting the Java Heap Size Value to -Xmx256m 2-37
Collecting Cisco CP Technical Support Logs 2-38

PART 2 **Managing Interfaces**

CHAPTER 3 **Creating a New Connection** 3-1
Creating a New Connection 3-1
New Connection Reference 3-2
Create Connection 3-2
Additional Procedures 3-3
How Do I Configure a Static Route? 3-4
How Do I View Activity on My LAN Interface? 3-4
How Do I Enable or Disable an Interface? 3-5
How Do I View the IOS Commands I Am Sending to the Router? 3-5
How Do I Launch the Wireless Application from Cisco CP? 3-6
How Do I Configure an Unsupported WAN Interface? 3-6
How Do I Enable or Disable an Interface? 3-6
How Do I View Activity on My WAN Interface? 3-7
How Do I Configure NAT on a WAN Interface? 3-7
How Do I Configure NAT on an Unsupported Interface? 3-8

How Do I Configure a Dynamic Routing Protocol? 3-8
How Do I Configure Dial-on-Demand Routing for My ISDN or Asynchronous Interface? 3-9
How Do I Edit a Radio Interface Configuration? 3-10

CHAPTER 4 **LAN Wizard** 4-1

Ethernet Configuration 4-2
LAN Wizard: Select an Interface 4-2
LAN Wizard: IP Address and Subnet Mask 4-3
LAN Wizard: Enable DHCP Server 4-3
LAN Wizard: DHCP Address Pool 4-4
DHCP Options 4-4
LAN Wizard: VLAN Mode 4-5
LAN Wizard: Switch Port 4-6
IRB Bridge 4-7
BVI Configuration 4-8
DHCP Pool for BVI 4-8
IRB for Ethernet 4-9
Layer 3 Ethernet Configuration 4-9
802.1Q Configuration 4-10
Trunking or Routing Configuration 4-10
Configure Switch Device Module 4-10
Configure Gigabit Ethernet Interface 4-11
Summary 4-11

CHAPTER 5 **Configuring WAN Connections** 5-1

Configuring an Ethernet WAN Connection 5-1
Ethernet WAN Connection Reference 5-2

WAN Wizard Interface Welcome Window 5-2
Select Controller 5-3
Select Interface - VDSL 5-3
Select Interface 5-3
IP Address: Ethernet without PPPoE 5-4
Encapsulation: PPPoE 5-5
Summary 5-5
Advanced Options 5-6
Configuring a VDSL Connection 5-7
VDSL WAN Connection Reference 5-8
Configuring a Serial Connection 5-8
Serial Connection Reference 5-9
IP Address: Serial with Point-to-Point Protocol 5-9
IP Address: Serial with HDLC or Frame Relay 5-10
Authentication 5-11
Configure LMI and DLCI 5-12
Configure Clock Settings 5-13
Configuring a DSL Connection 5-15
DSL Connection Reference 5-16
IP Address: ATM or Ethernet with PPPoE/PPPoA 5-16
IP Address: ATM with RFC 1483 Routing 5-17
Encapsulation Autodetect 5-18
PVC 5-19
Configuring a G.SHDSL Controller 5-21
G.SHDSL Controller Reference 5-21
SHDSL Configuration Mode Selection for HWIC-1SHDSL Controller 5-22
SHDSL Configuration Mode Selection for HWIC-2SHDSL Controller 5-22
SHDSL Configuration Mode Selection for HWIC-4SHDSL Controller 5-23
Configuring an ISDN Connection 5-25
ISDN Connection Reference 5-25

ISDN Wizard Welcome Window 5-26
IP Address: ISDN BRI or Analog Modem 5-26
Switch Type and SPIDs 5-26
Dial String 5-28
Configuring an Aux Backup Connection 5-29
Aux Backup Connection Reference 5-29
Aux Backup Welcome Window 5-30
Backup Configuration 5-30
Backup Configuration: Primary Interface and Next Hop IP Addresses 5-31
Backup Configuration: Hostname or IP Address to Be Tracked 5-32
Configuring an Analog Modem Connection 5-32
Analog Modem Connection Reference 5-33
Analog Modem Welcome 5-33
Configuring a Cable Modem Connection 5-33
Cable Modem Connection Reference 5-34
Cable Modem Connection Wizard Welcome 5-34
Select Interface 5-34
Summary 5-35

CHAPTER 6 **Edit Interface/Connection 6-1**
Connection: Ethernet for IRB 6-5
Connection: Ethernet for Routing 6-6
Existing Dynamic DNS Methods 6-7
Add Dynamic DNS Method 6-8
Media Type 6-9
Wireless 6-10
Association 6-10
NAT 6-12

Edit Switch Port 6-13
Application Service 6-14
General 6-16
Select Ethernet Configuration Type 6-18
Connection: VLAN 6-18
Subinterfaces List 6-19
Add or Edit BVI Interface 6-20
Add or Edit Loopback Interface 6-20
Connection: Virtual Template Interface 6-21
Connection: Ethernet LAN 6-21
Connection: Ethernet WAN 6-22
Connection: Ethernet Properties 6-24
Connection: Ethernet with No Encapsulation 6-26
Connection: ADSL 6-27
Connection: ADSL over ISDN 6-30
Connection: G.SHDSL 6-33
Connection: Cable Modem 6-36
Connection: Serial Interface, Frame Relay Encapsulation 6-37
Connection: Serial Interface, PPP Encapsulation 6-40
Connection: Serial Interface, HDLC Encapsulation 6-42
Add or Edit GRE Tunnel 6-43
Connection: ISDN BRI 6-45
Connection: Analog Modem 6-48
Connection: (AUX Backup) 6-50
Authentication 6-52
SPID Details 6-53
Dialer Options 6-54

Backup Configuration 6-56
Delete Connection 6-57
Connectivity Testing and Troubleshooting 6-59

CHAPTER 7 **Edit Controller/Connection 7-1**

Configuring a Cisco WIC-1SHDSL-V2 Controller 7-1
DSL Controller Screen Reference 7-2
Configure DSL Controller 7-2
Add a G.SHDSL Connection 7-4
Configuring a Cisco Multi-mode VDSL Router 7-7
Cisco Multi-mode VDSL Router Reference 7-8
Configure VDSL Controller dialog box 7-8
Add a VDSL Connection dialog box 7-8
Configuring a Cisco HWIC-SHDSL Controller 7-12
Cisco HWIC SHDSL Screen Reference 7-12
DSL Edit Controllers/Connection Tab 7-12
Add DSL Group for a 2SHDSL Controller 7-15
Edit DSL Group for a 2SHDSL Controller 7-15
Add DSL Group for a 4SHDSL Controller 7-16
Edit DSL Group for a 4SHDSL Controller 7-17

CHAPTER 8 **Wireless Support** 8-1

CHAPTER 9 **Cellular WAN Interface** 9-1

CHAPTER 10 **Module Configuration** 10-1

CHAPTER 11 **EnergyWise** 11-1

CHAPTER 12 **Trunks** 12-1

- Configuring Trunks 12-1
- Trunks Reference 12-2
  - Configure an Analog Trunk 12-3
  - Edit an Analog Trunk 12-4
    - Analog Trunks: General Settings Tab 12-4
    - Analog Trunks: Advanced Signal Settings Tab 12-5
    - Analog Trunks: Advanced Audio Settings Tab 12-6
    - Analog Trunks: Advanced Timer Settings Tab 12-8
  - Configure a Digital Trunk 12-9
  - Edit a Digital Trunk 12-10
    - Digital Trunks: T1/E1 Settings 12-11
    - Digital Trunks: PRI or BRI Settings Tab 12-13
    - Digital Trunks: PRI or BRI Audio Tab 12-14
- Configuring PSTN Trunk Groups 12-15
- Configuring SIP Trunks 12-15

PART 3 **Configuring Router Features**

CHAPTER 13 **Routing** 13-1

- Add or Edit IP Static Route 13-3

Add or Edit an RIP Route 13-5
Add or Edit an OSPF Route 13-5
Add or Edit EIGRP Route 13-7

CHAPTER 14 **Authentication, Authorization, and Accounting** 14-1
Configuring AAA 14-1
AAA Screen Reference 14-2
AAA Overview Screen 14-2
AAA Servers and Server Groups 14-3
AAA Servers 14-4
Add or Edit a TACACS+ Server 14-4
Add or Edit a RADIUS Server 14-5
Edit Global Settings 14-6
AAA Server Groups 14-7
Add or Edit AAA Server Group 14-8
Authentication, Authorization, and Accounting Policies 14-8
Authentication and Authorization 14-9
Authentication NAC 14-10
Authentication 802.1x 14-11
Add or Edit a Method List for Authentication or Authorization 14-12
Authorization Web Authentication 14-14
Accounting 802.1x 14-15
Accounting Web Authentication 14-16

CHAPTER 15 **ACL** 15-1
Useful Procedures for Access Rules and Firewalls 15-3
Rules Windows 15-3
Add or Edit a Rule 15-7
Associate with an Interface 15-10

Add a Standard Rule Entry 15-11
Add an Extended Rule Entry 15-13
Select a Rule 15-17

CHAPTER 16 **ACL Object Groups** 16-1

Understanding ACL Object Groups 16-1
ACL Object Groups Basic Workflow 16-2
Understanding Network Object Groups 16-3
Working with Network Object Groups 16-3
Creating Network Object Groups 16-3
Editing Network Object Groups 16-4
Deleting Network Object Groups 16-5
Understanding Service Object Groups 16-6
Working with Service Object Groups 16-7
Creating Service Object Groups 16-7
Editing Service Object Groups 16-8
Deleting Service Object Groups 16-9
Creating ACLs with Object Groups 16-10
ACL Object Groups Reference 16-11
Network Object Groups Summary Page 16-12
Create and Edit Network Object Groups Dialog Box 16-13
Create Network Object Group Dialog Box 16-13
Edit Network Object Groups Dialog Box 16-15
Service Object Groups Summary Page 16-17
Create and Edit Service Object Groups Dialog Box 16-18
Create Service Object Groups Dialog Box 16-18
Create Service Object Groups Dialog Box—TCP Service 16-21
Create Service Object Groups Dialog Box—UDP Service 16-24
Create Service Object Groups Dialog Box—TCP-UDP Service 16-27

Create Service Object Groups Dialog Box—ICMP Service 16-30
Create Service Object Groups Dialog Box—IP Protocol Service 16-31
Create Service Object Groups Dialog Box—Existing Service Object Groups 16-33
Edit Service Object Groups Dialog Box 16-34
Add an Extended Rule Entry Dialog Box 16-37
Select Network Object Groups Dialog Box 16-37
Select Service Object Groups Dialog Box 16-38

CHAPTER 17 **Router Properties** 17-1
Device Properties 17-1
Date and Time: Clock Properties 17-2
Date and Time Properties 17-3
Voice Timezone Configuration 17-4
NTP 17-6
Add or Edit NTP Server Details 17-7
Add an NTP Server 17-8
Logging 17-9
SNMP 17-10
Netflow 17-12
Netflow Talkers 17-12
Router Access 17-13
User Accounts/View 17-13
Add or Edit a Username 17-14
View Password 17-17
VTY Settings 17-17
Edit VTY Lines 17-18
Configure Management Access Policies 17-20
Add or Edit a Management Policy 17-21
Management Access Error Messages 17-23

SSH 17-25
DHCP Configuration 17-26
DHCP Pools 17-26
Add or Edit DHCP Pool 17-27
DHCP Bindings 17-28
Add or Edit DHCP Binding 17-29
DNS Properties 17-30
Dynamic DNS Methods 17-31
Add or Edit Dynamic DNS Method 17-32

CHAPTER 18 **Network Address Translation** 18-1
Network Address Translation Wizards 18-1
Basic NAT Wizard: Welcome 18-2
Basic NAT Wizard: Connection 18-2
Summary 18-3
Advanced NAT Wizard: Welcome 18-3
Advanced NAT Wizard: Connection 18-4
Add IP Address 18-4
Advanced NAT Wizard: Networks 18-4
Add Network 18-5
Advanced NAT Wizard: Server Public IP Addresses 18-5
Add or Edit Address Translation Rule 18-6
Advanced NAT Wizard: ACL Conflict 18-7
Details 18-8
Network Address Translation Rules 18-8
Designate NAT Interfaces 18-12
Translation Timeout Settings 18-12
Edit Route Map 18-13
Edit Route Map Entry 18-14

Address Pools 18-15
Add or Edit Address Pool 18-16
Add or Edit Static Address Translation Rule: Inside to Outside 18-17
Add or Edit Static Address Translation Rule: Outside to Inside 18-20
Add or Edit Dynamic Address Translation Rule: Inside to Outside 18-23
Add or Edit Dynamic Address Translation Rule: Outside to Inside 18-26
How Do I . . . 18-28
How do I Configure Address Translation for Outside to Inside 18-28
How Do I Configure NAT With One LAN and Multiple WANs? 18-29

CHAPTER 19 **Quality of Service** 19-1
Understanding QoS 19-1
QoS Policy Terms 19-2
Working with QoS Policies 19-3
Creating QoS Policies 19-3
Creating QoS Policies on a WAN Interface 19-3
Creating QoS Policies on a DMVPN Spoke Tunnel Interface 19-5
Editing QoS Policies 19-7
Associating and Disassociating QoS Policies 19-8
Adding Service Policy to a Class 19-9
Adding a QoS Class 19-10
Editing the QoS Class Information 19-11
Deleting a QoS Class 19-12
Editing DSCP, Protocols, and ACL Classification Values 19-13
Adding Custom Protocols 19-14
Editing Queuing, Policing, and Shaping Action Parameters 19-15
Viewing Associated QoS Policies 19-16
Create QoS Policy Reference 19-17
Create QoS Configuration Wizard 19-17
QoS Configuration Wizard Page 19-18

Interface Selection Page 19-18
QoS Group Name Page—Appears for DMVPN Spoke Tunnel Interface 19-20
Classification Page 19-21
Queuing With Shaping for Outbound Traffic Page 19-22
Add a New Traffic Class Dialog Box 19-24
Policing for Outbound Traffic Page 19-26
Bandwidth Allocation Dialog Box 19-29
QoS Configuration Summary Page 19-29
Edit QoS Policy Reference 19-30
Edit QoS Policy Page 19-31
Add Class for the New Service Policy Dialog Box 19-37
Add Service Policy to Class Dialog Box 19-38
Associate a Policy Map to Interface Dialog Box 19-39
Associate or Disassociate the QoS Policy Dialog Box 19-39
Add or Edit a QoS Class Dialog Box 19-40
Edit Match DSCP Values Dialog Box 19-42
Edit Match Protocol Values Dialog Box 19-43
Add Custom Protocols Dialog Box 19-44
Edit Match ACL Dialog Box 19-45
Configure Policing Dialog Box 19-46
Configure Shaping Dialog Box 19-48
Configure Queuing Dialog Box 19-49
Policies Associated Details Dialog Box 19-51
Configure QoS Group Name Dialog Box—Appears for DMVPN Spoke Tunnel Interface 19-51
Add or Edit QoS Group Name Dialog Box—Appears for DMVPN Hub Tunnel Interface 19-52

CHAPTER 20 **Router Provisioning** 20-1

Secure Device Provisioning 20-1

Router Provisioning from USB 20-2

Router Provisioning from USB (Load File) 20-2

SDP Troubleshooting Tips 20-2

CHAPTER 21 **Performance Routing** 21-1

PART 4 **Configuring Security Features**

CHAPTER 22 **Create Firewall** 22-1

Basic Firewall Configuration Wizard 22-5

Basic Firewall Interface Configuration 22-5

Configuring Firewall for Remote Access 22-6

Advanced Firewall Configuration Wizard 22-6

Advanced Firewall Interface Configuration 22-6

Advanced Firewall DMZ Service Configuration 22-7

DMZ Service Configuration 22-8

Application Security Configuration 22-9

Domain Name Server Configuration 22-10

URL Filter Server Configuration 22-10

Select Interface Zone 22-11

ZPF Inside Zones 22-11

Voice Configuration 22-11

Summary 22-12

Cisco CP Warning: Cisco CP Access 22-14

How Do I... 22-16

How Do I View Activity on My Firewall? 22-16

How Do I Configure a Firewall on an Unsupported Interface? 22-18

How Do I Configure a Firewall After I Have Configured a VPN? 22-18
How Do I Permit Specific Traffic Through a DMZ Interface? 22-19
How Do I Modify an Existing Firewall to Permit Traffic from a New Network or Host? 22-20
How Do I Configure NAT on an Unsupported Interface? 22-20
How Do I Configure NAT Passthrough for a Firewall? 22-21
How Do I Permit Traffic Through a Firewall to My Easy VPN Concentrator? 22-21
How Do I Associate a Rule with an Interface? 22-23
How Do I Disassociate an Access Rule from an Interface 22-23
How Do I Delete a Rule That Is Associated with an Interface? 22-24
How Do I Create an Access Rule for a Java List? 22-24
How Do I Permit Specific Traffic onto My Network if I Don't Have a DMZ Network? 22-25

CHAPTER 23 **Firewall Policy** 23-1

Edit Firewall Policy/ACL 23-1
Choose a Traffic Flow 23-3
Examine the Traffic Diagram and Choose a Traffic Direction 23-5
Make Changes to Access Rules 23-7
Make Changes to Inspection Rules 23-12
Add *App-Name* Application Entry 23-14
Add rpc Application Entry 23-14
Add Fragment application entry 23-15
Add or Edit http Application Entry 23-16
Java Applet Blocking 23-17
Cisco CP Warning: Inspection Rule 23-19
Cisco CP Warning: Firewall 23-20
Edit Firewall Policy 23-20
Add a New Rule 23-24

Add Traffic 23-25
Application Inspection Dialog Box 23-27
Configure Deep Packet Inspection - SIP Dialog Box 23-30
Configure SIP inspection based on header fields Dialog Box 23-32
Enable SIP inspection based on header fields Dialog Box 23-33
Configure SIP inspection based on status response patterns Dialog Box 23-34
Enable SIP inspection based on status response Dialog Box 23-35
Manage H323 Messages Inspection Dialog Box 23-36
URL Filter 23-37
Quality of Service 23-37
Inspect Parameter 23-37
Select Traffic 23-38
Delete Rule 23-38

CHAPTER 24 **Zone-Based Policy Firewall** 24-1

Zone List 24-3
Add or Edit a Zone 24-4
Zone-Based Policy General Rules 24-5
Zone Pairs 24-7
Add or Edit a Zone Pair 24-8
Add a Zone 24-10
Select a Zone 24-11

CHAPTER 25 **Site-to-Site VPN** 25-1

VPN Design Guide 25-1
Create Site to Site VPN 25-1
Site-to-Site VPN Wizard 25-4
View Defaults 25-5
VPN Connection Information 25-6

IKE Proposals 25-8
Transform Set 25-11
Traffic to Protect 25-13
Summary of the Configuration 25-14
Spoke Configuration 25-15
Secure GRE Tunnel (GRE-over-IPSec) 25-16
GRE Tunnel Information 25-16
VPN Authentication Information 25-17
Backup GRE Tunnel Information 25-18
Routing Information 25-19
Static Routing Information 25-20
Select Routing Protocol 25-22
Summary of Configuration 25-22
Edit Site-to-Site VPN 25-23
Add new connection 25-26
Add Additional Crypto Maps 25-26
Crypto Map Wizard: Welcome 25-27
Crypto Map Wizard: Summary of the configuration 25-28
Delete Connection 25-28
Generate Mirror... 25-29
Cisco CP Warning: NAT Rules with ACL 25-29
How Do I... 25-30
How Do I Create a VPN to More Than One Site? 25-30
After Configuring a VPN, How Do I Configure the VPN on the Peer Router? 25-33
How Do I Edit an Existing VPN Tunnel? 25-34
How Do I Confirm That My VPN Is Working? 25-34
How Do I Configure a Backup Peer for My VPN? 25-35
How Do I Accommodate Multiple Devices with Different Levels of VPN Support? 25-36

How Do I Configure a VPN on an Unsupported Interface? 25-37
How Do I Configure a VPN After I Have Configured a Firewall? 25-37
How Do I Configure NAT Passthrough for a VPN? 25-37

CHAPTER 26 **Easy VPN Remote** 26-1

Creating an Easy VPN Remote Connection 26-2
Create Easy VPN Remote Reference 26-3
Create Easy VPN Remote 26-4
Configure an Easy VPN Remote Client 26-4
Easy VPN Remote Wizard: Network Information 26-5
Easy VPN Remote Wizard: Identical Address Configuration 26-6
Easy VPN Remote Wizard: Interfaces and Connection Settings 26-7
Easy VPN Remote Wizard: Server Information 26-9
Easy VPN Remote Wizard: Authentication 26-11
Easy VPN Remote Wizard: Automatic Firewall Bypass 26-14
Easy VPN Remote Wizard: Summary of Configuration 26-15
Administering Easy VPN Remote Connections 26-16
Editing an Existing Easy VPN Remote Connection 26-16
Creating a New Easy VPN Remote Connection 26-17
Deleting an Easy VPN Remote Connection 26-17
Resetting an Established Easy VPN Remote Connection 26-17
Connecting to an Easy VPN Server 26-18
Connecting other Subnets to the VPN Tunnel 26-18
Editing CTCP Port Number and Keepalive Values 26-20
Administering Easy VPN Remote Reference 26-21
Edit Easy VPN Remote 26-21
Add or Edit Easy VPN Remote 26-26
Add or Edit Easy VPN Remote: General Settings 26-28
Network Extension Options 26-30
Add or Edit Easy VPN Remote: Easy VPN Settings 26-31

Add or Edit Easy VPN Remote: Authentication Information 26-33
Add or Edit Easy VPN Remote: Easy VPN Client Phase III Authentication 26-36
Add or Edit Easy VPN Remote: Interfaces and Connections 26-38
Add or Edit Easy VPN Remote: Firewall Bypass 26-40
Add or Edit Easy VPN Remote: Identical Addressing 26-41
Easy VPN Remote: Add a Device 26-43
Enter SSH Credentials 26-43
XAuth Login Window 26-44
Other Procedures 26-44
How Do I Edit an Existing Easy VPN Connection? 26-44
How Do I Configure a Backup for an Easy VPN Connection? 26-45

CHAPTER 27 **Easy VPN Server** 27-1
Creating an Easy VPN Server Connection 27-1
Create an Easy VPN Server Reference 27-2
Create an Easy VPN Server 27-3
Welcome to the Easy VPN Server Wizard 27-3
Interface and Authentication 27-4
Group Authorization and Group Policy Lookup 27-5
User Authentication (XAuth) 27-5
User Accounts for XAuth 27-6
Add RADIUS Server 27-7
Group Authorization: User Group Policies 27-7
General Group Information 27-8
DNS and WINS Configuration 27-9
Split Tunneling 27-10
Client Settings 27-11
Choose Browser Proxy Settings 27-14
Add or Edit Browser Proxy Settings 27-15

User Authentication (XAuth) 27-16
Client Update 27-17
Add or Edit Client Update Entry 27-17
Cisco Tunneling Control Protocol 27-19
Summary 27-20
Browser Proxy Settings 27-20
Editing Easy VPN Server Connections 27-21
Edit Easy VPN Server Reference 27-22
Edit Easy VPN Server 27-22
Add or Edit Easy VPN Server Connection 27-23
Restrict Access 27-24
Group Policies Configuration 27-25
IP Pools 27-27
Add or Edit IP Local Pool 27-27
Add IP Address Range 27-28

CHAPTER 28 **Enhanced Easy VPN** 28-1
Interface and Authentication 28-1
RADIUS Servers 28-2
Group Authorization and Group User Policies 28-4
Add or Edit Easy VPN Server: General Tab 28-5
Add or Edit Easy VPN Server: IKE Tab 28-6
Add or Edit Easy VPN Server: IPSec Tab 28-9
Create Virtual Tunnel Interface 28-10

CHAPTER 29 **Dynamic Multipoint VPN** 29-1
Dynamic Multipoint VPN 29-1
Dynamic Multipoint VPN Hub Wizard 29-2
Configuring a DMVPN Hub 29-3
DMVPN Hub Reference 29-5

Dynamic Multipoint VPN Page 29-6
DMVPN Hub Wizard—Configure a DMVPN Hub Page 29-7
DMVPN Hub Wizard—DMVPN Network Topology Page 29-7
DMVPN Hub Wizard—Type of Hub Page 29-8
DMVPN Hub Wizard—Multipoint GRE Tunnel Interface Configuration Page 29-9
Advanced Configuration for the Tunnel Interface Button 29-11
Cisco CP Warning Message Dialog Box 29-12
DMVPN Hub Wizard—Authentication Page 29-13
DMVPN Hub Wizard—IKE Proposals Page 29-14
Primary Hub Page 29-14
DMVPN Hub Wizard—Transform Set 29-15
DMVPN Hub Wizard—Select Routing Protocol Page 29-15
DMVPN Hub Wizard—Routing Information Page 29-16
DMVPN Hub Wizard—Summary of the Configuration Page 29-18
Dynamic Multipoint VPN Spoke Wizard 29-19
Configuring a DMVPN Spoke 29-20
DMVPN Spoke Reference 29-22
DMVPN Spoke Wizard—Configure a DMVPN spoke Page 29-22
DMVPN Spoke Wizard—DMVPN Network Topology Page 29-23
DMVPN Spoke Wizard—Specify Hub Information Page 29-24
DMVPN Spoke Wizard—GRE Tunnel Interface Configuration Page 29-24
DMVPN Spoke Wizard—Cisco CP Warning: DMVPN Dependency Page 29-26
DMVPN Spoke Wizard—Summary of the Configuration Page 29-27
Edit Dynamic Multipoint VPN (DMVPN) 29-28
General Panel 29-30
NHRP Panel 29-31
NHRP Map Configuration 29-32
Routing Panel 29-34

How Do I Configure a DMVPN Manually? 29-36

CHAPTER 30 **GETVPN** 30-1

CHAPTER 31 **Cisco IOS SSL VPN** 31-1

Creating an SSL VPN Connection 31-2
Create an SSL VPN Connection Reference 31-3
Create SSL VPN 31-4
Persistent Self-Signed Certificate 31-5
Welcome 31-6
SSL VPN Gateways 31-7
User Authentication 31-8
Configure Intranet Websites 31-9
Add or Edit URL 31-10
Customize SSL VPN Portal 31-10
SSL VPN Passthrough Configuration 31-11
User Policy 31-11
Details of SSL VPN Group Policy: Policyname 31-12
Select the SSL VPN User Group 31-12
Select Advanced Features 31-13
Thin Client (Port Forwarding) 31-13
Add or Edit a Server 31-14
Full Tunnel 31-14
Enable Cisco Secure Desktop 31-16
Common Internet File System 31-17
Enable Clientless Citrix 31-18
Summary 31-18
Editing SSL VPN Connections 31-18
Editing SSL VPN Connection Reference 31-19
Edit SSL VPN 31-20

SSL VPN Context 31-22
Designate Inside and Outside Interfaces 31-23
Select a Gateway 31-23
Context: Group Policies 31-24
Group Policy: General Tab 31-24
Group Policy: Clientless Tab 31-25
Group Policy: Thin Client Tab 31-27
Group Policy: SSL VPN Client (Full Tunnel) Tab 31-27
Advanced Tunnel Options 31-29
DNS and WINS Servers 31-31
Context: HTML Settings 31-31
Select Color 31-33
Context: NetBIOS Name Server Lists 31-33
Add or Edit a NBNS Server List 31-34
Add or Edit an NBNS Server 31-34
Context: Port Forward Lists 31-34
Add or Edit a Port Forward List 31-34
Context: URL Lists 31-35
Add or Edit a URL List 31-35
Context: Cisco Secure Desktop 31-35
Editing SSL VPN Gateways 31-36
Editing SSL VPN Gateway Reference 31-36
SSL VPN Gateways 31-36
Add or Edit a SSL VPN Gateway 31-38
Installing Software Packages 31-39
Packages Reference 31-39
Packages 31-39
Install Package 31-40
Locating the Install Bundle 31-41
Additional Help Topics 31-42

Cisco IOS SSL VPN Contexts, Gateways, and Policies 31-43
Learn More about Port Forwarding Servers 31-48
Learn More About Group Policies 31-49
Learn More About Split Tunneling 31-50
Cisco IOS SSL VPN Links on Cisco.com 31-51
How do I verify that my Cisco IOS SSL VPN is working? 31-51
How do I configure a Cisco IOS SSL VPN after I have configured a firewall? 31-52
How do I associate a VRF instance with a Cisco IOS SSL VPN context? 31-53

CHAPTER 32 **SSL VPN Enhancements** 32-1

SSL VPN Reference 32-1
SSL VPN Context: Access Control Lists 32-1
Add or Edit Application ACL 32-2
Add ACL Entry 32-3
Action URL Time Range 32-4
Add or Edit Action URL Time Range Dialog 32-5
Add or Edit Absolute Time Range Entry 32-6
Add or Edit Periodic Time Range Entry 32-7

CHAPTER 33 **IOS SSL VPN AnyConnect Client** 33-1

About Cisco AnyConnect 33-1
Installing AnyConnect Packages on the Router 33-1
Removing AnyConnect Packages from the Router 33-3
Changing the SSL VPN Package Priority 33-4
Installing the Cisco Secure Desktop Client on the Router 33-4
Anyconnect Client Screen Reference 33-5
Cisco SSL VPN Client Software 33-5
Change SSL VPN Package Priority 33-6

CHAPTER 34 **VPN Options and VPN Keys Encryption** 34-1

VPN Options 34-1

VPN Options Reference 34-1

VPN Options 34-1

VPN Global Settings: IKE 34-4

VPN Global Settings: IPSec 34-5

VPN Global Settings: Easy VPN Server 34-6

VPN Keys Encryption 34-7

VPN Keys Encryption Reference 34-7

VPN Key Encryption Settings 34-7

CHAPTER 35 **VPN Troubleshooting** 35-1

VPN Troubleshooting 35-1

VPN Troubleshooting: Specify Easy VPN Client 35-3

VPN Troubleshooting: Generate Traffic 35-4

VPN Troubleshooting: Generate GRE Traffic 35-5

Cisco CP Warning: Cisco CP will enable router debugs... 35-6

CHAPTER 36 **IP Security** 36-1

IPSec Policies 36-1

Add or Edit IPSec Policy 36-3

Add or Edit Crypto Map: General 36-5

Add or Edit Crypto Map: Peer Information 36-6

Add or Edit Crypto Map: Transform Sets 36-7

Add or Edit Crypto Map: Protecting Traffic 36-9

Dynamic Crypto Map Sets 36-11

Add or Edit Dynamic Crypto Map Set 36-11

Associate Crypto Map with this IPSec Policy 36-12

IPSec Profiles 36-12

Add or Edit IPSec Profile 36-13
Add or Edit IPSec Profile and Add Dynamic Crypto Map 36-14
Transform Set 36-15
Add or Edit Transform Set 36-18
IPSec Rules 36-20

CHAPTER 37 **Internet Key Exchange** 37-1
Internet Key Exchange (IKE) 37-1
IKE Policies 37-1
Add or Edit IKE Policy 37-2
IKE Pre-shared Keys 37-5
Add or Edit Pre Shared Key 37-5
IKE Profiles 37-7
Add or Edit an IKE Profile 37-7

CHAPTER 38 **Certificate Authority Server** 38-1
Create CA Server 38-1
Prerequisite Tasks for PKI Configurations 38-2
CA Server Wizard: Welcome 38-3
CA Server Wizard: Certificate Authority Information 38-3
Advanced Options 38-5
CA Server Wizard: RSA Keys 38-7
Open Firewall 38-8
CA Server Wizard: Summary 38-8
Manage CA Server 38-9
Backup CA Server 38-11
Manage CA Server Restore Window 38-11
Restore CA Server 38-11
Edit CA Server Settings: General Tab 38-12

Edit CA Server Settings: Advanced Tab 38-13
Manage CA Server: CA Server Not Configured 38-13
Manage Certificates 38-13
Pending Requests 38-13
Revoked Certificates 38-15
Revoke Certificate 38-16

CHAPTER 39 **Public Key Infrastructure** 39-1
Certificate Wizards 39-1
Welcome to the SCEP Wizard 39-2
Certificate Authority (CA) Information 39-3
Advanced Options 39-4
Certificate Subject Name Attributes 39-4
Other Subject Attributes 39-5
RSA Keys 39-6
Summary 39-7
Enrollment Status 39-8
Cut and Paste Wizard Welcome 39-8
Enrollment Task 39-9
Enrollment Request 39-9
Continue with Unfinished Enrollment 39-10
Import CA certificate 39-11
Import Router Certificate(s) 39-11
Digital Certificates 39-12
Trustpoint Information 39-14
Certificate Details 39-14
Revocation Check 39-14
Revocation Check, CRL Only 39-15

RSA Keys Window 39-15
Generate RSA Key Pair 39-16
USB Token Credentials 39-17
USB Tokens 39-18
Add or Edit USB Token 39-19
Open Firewall 39-20
Open Firewall Details 39-22

CHAPTER 40 **Content Filtering** 40-1
Cisco Configuration Professional Content Filtering 40-1
Creating a Content Filter 40-2
Creating Content Filter Reference 40-4
Content Filter Wizard: Create Content Filter Tab 40-4
Content Filter Wizard: Basic Content Filter Configuration Wizard 40-5
Content Filter Wizard: Basic Content Filter Interface Configuration 40-6
Content Filter Wizard: Content Filter Server Configuration 40-7
Content Filter Wizard and Edit Screen: Category Selection 40-8
Content Filter Wizard and Edit Screen: Reputation Selection 40-9
Content Filter Wizard: Choose Websense or Secure Computing 40-10
Content Filter Wizard: Content Filter Web Requests 40-11
Content Filter Wizard: Summary 40-11
Editing Content Filters 40-12
Using the Edit Content Filter Screens 40-13
Edit Screen Dialogs Reference 40-15
Policy Name 40-16
Clone Policy 40-16
Associate With Zone Pair 40-17
Edit Global Settings 40-18
Creating a Keyword Blocking Policy 40-21

Keyword Blocking Screen Reference 40-21
URL Filtering: Keyword Blocking 40-22
Add or Edit Keyword 40-23
Creating a Black and White Listing 40-23
Black and White Listing Screen Reference 40-24
Black and White List 40-25
Add Local URL 40-26
Registering With a Category Server 40-27
Category Server Registration Screen Reference 40-29
Category Server Registration 40-29
Edit Category Server 40-30
Filtering By URL Category 40-34
URL Category Screen Reference 40-34
Filtering By URL Reputation 40-35
URL Reputation Screen Reference 40-35
Configuring the Router To Use Websense or Secure Computing Servers 40-36
URL Filter Server Screen Reference 40-36
Server Filtering 40-37
Add Secure Computing or Websense Server 40-38
Configuring Content Filtering Components 40-38
Configuring or Editing URL Filter Policy Maps 40-39
URL Filter Policy Map Screen Reference 40-39
Policy Map Text Description 40-40
URL Filter Policy Map List 40-40
Add or Edit URL Filter Policy Map Entry 40-41
Add Action 40-44
Configuring URL Filter Class Maps 40-46
URL Filter Class Map Screen Reference 40-47
Class Map Text Description 40-47

Content Filter Local Class Map List 40-48
Add or Edit URL Filter Local Class Map Entry 40-49
Add Local Rule 40-51
URL Filter Websense Class Map List 40-52
Add or Edit Websense Class Map Entry 40-53
Content Filter N2H2 Class Map List 40-53
Add or Edit N2H2 Class Map Entry 40-54
Content Filter Trend Class Map List 40-55
Add or Edit Trend Class Map Entry 40-56
Add Trend Rule 40-58
Configuring or Editing URL Filter Parameter Maps 40-59
URL Filter Parameter Map Screen Reference 40-59
Parameter Map Text Description 40-60
Content Filtering Parameter Maps 40-61
Add Content Filtering: General Tab 40-62
Add Content Filtering: Content Filter Servers Tab 40-64
Add Content Filtering: URL List Tab 40-66
Content Filter Local Parameter Map List 40-67
Add or Edit URL Filtering Local Parameter Map 40-68
Content Filter Websense Parameter Map List 40-69
Add or Edit Websense Parameter Map 40-70
Content Filter N2H2 Parameter Map List 40-72
Add or Edit N2H2 Parameter Map 40-74
Content Filter Trend Global Parameter Map List 40-75
Add or Edit Trend Global Parameter Map 40-76
Content Filter Trend Parameter Map List 40-77
Add or Edit Trend Parameter Map 40-79
Content Filter Glob Parameter Map List 40-80
Add or Edit Regular Expression 40-82
Add or Edit Pattern 40-83

Additional Information 40-83
Content Filtering is Not Available 40-83

CHAPTER 41 **Cisco IOS IPS** 41-1

Create IPS 41-2
Create IPS: Welcome 41-3
Create IPS: Select Interfaces 41-3
Create IPS: SDF Location 41-3
Create IPS: Signature File 41-4
Create IPS: Configuration File Location and Category 41-6
Add or Edit a Config Location 41-6
Directory Selection 41-7
Signature File 41-7
Create IPS: Summary 41-8
Create IPS: Summary 41-9
Edit IPS 41-10
Edit IPS: IPS Policies 41-11
Enable or Edit IPS on an Interface 41-14
Edit IPS: Global Settings 41-15
Edit Global Settings 41-18
Add or Edit a Signature Location 41-19
Edit IPS: SDEE Messages 41-20
SDEE Message Text 41-22
Edit IPS: Global Settings 41-25
Edit Global Settings Dialog Box 41-26
Edit IPS Prerequisites Dialog Box 41-27
Add Public Key 41-28
Edit IPS: Download 41-29
Downloading Signature Package from Cisco.com 41-29
Downloading the Signature Package from Cisco.com Reference 41-31

Edit IPS: Auto Update 41-32
Automatically Updating IPS Signature Package from a Local Server 41-33
Automatically Update IPS Signature Package Reference 41-34
Automatically Update IPS Signature Package Page 41-34
Edit IPS: SEAP Configuration 41-35
Edit IPS: SEAP Configuration: Target Value Rating 41-35
Add Target Value Rating 41-36
Edit IPS: SEAP Configuration: Event Action Overrides 41-37
Add or Edit an Event Action Override 41-39
Edit IPS: SEAP Configuration: Event Action Filters 41-40
Add or Edit an Event Action Filter 41-42
Edit IPS: Signatures 41-44
Edit IPS: Signatures 41-50
Edit Signature 41-54
File Selection 41-57
Assign Actions 41-58
Import Signatures 41-59
Add, Edit, or Clone Signature 41-61
Cisco Security Center 41-63
IPS-Supplied Signature Definition Files 41-63
Security Dashboard 41-64
IPS Migration 41-67
Migration Wizard: Welcome 41-67
Migration Wizard: Choose the IOS IPS Backup Signature File 41-68
Signature File 41-68
Java Heap Size 41-68

CHAPTER 42 **Network Admission Control** 42-1
Create NAC Tab 42-2

Other Tasks in a NAC Implementation 42-2
Welcome 42-3
NAC Policy Servers 42-4
Interface Selection 42-6
NAC Exception List 42-7
Add or Edit an Exception List Entry 42-8
Choose an Exception Policy 42-8
Add Exception Policy 42-9
Agentless Host Policy 42-10
Configuring NAC for Remote Access 42-10
Modify Firewall 42-11
Details Window 42-12
Summary of the configuration 42-12
Edit NAC Tab 42-13
NAC Components 42-14
Exception Policies Window 42-14
NAC Timeouts 42-15
Configure a NAC Policy 42-16
How Do I... 42-17
How Do I Configure a NAC Policy Server? 42-17
How Do I Install and Configure a Posture Agent on a Host? 42-17

CHAPTER 43 **Cisco Common Classification Policy Language** 43-1
Policy Map 43-1
Policy Map Screens 43-1
Add or Edit a QoS Policy Map 43-3
Associate a Policy Map to Interface 43-3
Add an Inspection Policy Map 43-5
Layer 7 Policy Map 43-5
Application Inspection 43-5

Configure Deep Packet Inspection 43-6
Class Maps 43-6
Associate Class Map 43-7
Class Map Advanced Options 43-7
QoS Class Map 43-8
Add or Edit a QoS Class Map 43-9
Add or Edit a QoS Class Map 43-9
Select a Class Map 43-9
Deep Inspection 43-9
Class Map and Application Service Group Windows 43-9
Add or Edit an Inspect Class Map 43-12
Associate Parameter Map 43-12
Add an HTTP Inspection Class Map 43-13
HTTP Request Header 43-13
HTTP Request Header Fields 43-14
HTTP Request Body 43-15
HTTP Request Header Arguments 43-15
HTTP Method 43-16
Request Port Misuse 43-16
Request URI 43-16
Response Header 43-17
Response Header Fields 43-18
HTTP Response Body 43-19
HTTP Response Status Line 43-19
Request/Response Header Criteria 43-20
HTTP Request/Response Header Fields 43-20
Request/Response Body 43-21
Request/Response Protocol Violation 43-22
Add or Edit an IMAP Class Map 43-22
Add or Edit an SMTP Class Map 43-22

Add or Edit a SUNRPC Class Map 43-23
Add or Edit an Instant Messaging Class Map 43-23
Add or Edit a Point-to-Point Class Map 43-23
Add P2P Rule 43-24
Add or Edit a POP3 Class Map 43-24
Parameter Maps 43-25
Parameter Map Windows 43-25
Add or Edit a Parameter Map for Protocol Information 43-25
Add or Edit a Server Entry 43-26
Add or Edit Regular Expression 43-26
Add a Pattern 43-27
Build Regular Expression 43-28
Regular Expression Metacharacters 43-30

CHAPTER 44 802.1x Authentication 44-1
LAN Wizard: 802.1x Authentication (Switch Ports) 44-1
Advanced Options 44-2
LAN Wizard: RADIUS Servers for 802.1x Authentication 44-4
Edit 802.1x Authentication (Switch Ports) 44-6
LAN Wizard: 802.1x Authentication (VLAN or Ethernet) 44-7
802.1x Exception List 44-8
802.1x Authentication on Layer 3 Interfaces 44-9
Edit 802.1x Authentication 44-10
How Do I ... 44-11
How Do I Configure 802.1x Authentication on More Than One Ethernet Port? 44-11

CHAPTER 45 Port-to-Application Mapping 45-1
Port-to-Application Mapping Reference 45-1

Port-to-Application Mappings 45-1
Add or Edit Port Map Entry 45-3

CHAPTER 46 **Security Audit** 46-1

Welcome Page 46-4
Interface Selection Page 46-4
Report Card Page 46-5
Fix It Page 46-5
Disable Finger Service 46-6
Disable PAD Service 46-7
Disable TCP Small Servers Service 46-7
Disable UDP Small Servers Service 46-8
Disable IP BOOTP Server Service 46-8
Disable IP Identification Service 46-9
Disable CDP 46-9
Disable IP Source Route 46-10
Enable Password Encryption Service 46-10
Enable TCP Keepalives for Inbound Telnet Sessions 46-11
Enable TCP Keepalives for Outbound Telnet Sessions 46-11
Enable Sequence Numbers and Time Stamps on Debugs 46-11
Enable IP CEF 46-12
Disable IP Gratuitous ARPs 46-12
Set Minimum Password Length to Less Than 6 Characters 46-12
Set Authentication Failure Rate to Less Than 3 Retries 46-13
Set TCP Synwait Time 46-13
Set Banner 46-14
Enable Logging 46-14
Set Enable Secret Password 46-15
Disable SNMP 46-15
Set Scheduler Interval 46-16

Set Scheduler Allocate 46-16
Set Users 46-17
Enable Telnet Settings 46-17
Enable NetFlow Switching 46-17
Disable IP Redirects 46-18
Disable IP Proxy ARP 46-18
Disable IP Directed Broadcast 46-19
Disable MOP Service 46-20
Disable IP Unreachables 46-20
Disable IP Mask Reply 46-20
Disable IP Unreachables on NULL Interface 46-21
Enable Unicast RPF on Outside Interfaces 46-22
Enable Firewall on All of the Outside Interfaces 46-22
Set Access Class on HTTP Server Service 46-23
Set Access Class on VTY Lines 46-23
Enable SSH for Access to the Router 46-24
Enable AAA 46-24
Configuration Summary Screen 46-25
Cisco CP and Cisco IOS AutoSecure 46-25
Security Configurations Cisco CP Can Undo 46-27
Undoing Security Audit Fixes 46-28
Add or Edit Telnet/SSH Account Screen 46-28
Configure User Accounts for Telnet/SSH Page 46-29
Enable Secret and Banner Page 46-30
Logging Page 46-30

PART 5 Configuring Unified Communications Features

CHAPTER 47 **Unified Communications** 47-1

Understanding Unified Communications Features 47-2

Configuring Unified Communication Features 47-4

Features Available in Each Unified Communication Feature 47-5

Unified Communications Features Reference 47-7

Unified Communications Features Summary Page 47-8

Edit Unified Communications Features Page 47-8

CHAPTER 48 **CME as SRST** 48-1

CHAPTER 49 **SRST Settings** 49-1

Configuring SRST Settings 49-1

SRST Settings Reference 49-1

Configure SRST Settings 49-2

CHAPTER 50 **SRST Rerouting** 50-1

Configuring SRST Rerouting 50-1

SRST Rerouting Reference 50-2

Configure SRST Rerouting 50-2

Edit or Create SRST Rerouting 50-3

CHAPTER 51 **Gateway Settings** 51-1

Configuring Gateway Settings 51-1

Gateway Settings Reference 51-1

Gateway Settings 51-2

CHAPTER 52 **Unified Communication Security Audit** 52-1

Configuring Unified Communication Security Audit 52-1

Configuring CUE: Restriction Table 52-2

CHAPTER 53 **Telephony Settings 53-1**

Configuring Telephony Settings 53-1

Telephony Settings Reference 53-1

Telephony Settings page 53-2

Edit Telephony Settings dialog box 53-4

CHAPTER 54 **Advanced Telephony 54-1**

CHAPTER 55 **Importing Bulk Data 55-1**

Understanding the .CSV File 55-1

Downloading the .CSV Template 55-6

Using the Cisco Template to Create the .CSV File 55-6

Using Cisco CP to Import Bulk Data 55-8

Correcting Data Conflicts 55-9

Import Bulk Data Screen Reference 55-10

Bulk Import 55-10

Bulk Import Wizard—Select Bulk File 55-11

Bulk Import Wizard—Summary 55-12

Bulk Import Wizard—Enable Rollback 55-13

Bulk Import Wizard—Apply Data 55-14

Bulk Import Wizard—Finish 55-15

CHAPTER 56 **Users, Phones, and Extensions 56-1**

User, Phones, and Extensions Basic Workflow 56-1

Extensions 56-2

Creating, Editing, Deleting, and Cloning Extensions 56-4

Extensions Reference 56-7

Extensions Summary Page 56-7
Edit All Extensions Dialog Box 56-9
Create or Edit Extension Dialog Box 56-12
Create or Edit Extension Dialog Box 56-12
Phones and Users Settings 56-21
Creating, Editing, Deleting, Restarting, and Resetting Phones and Users 56-22
Phones and Users Reference 56-25
Configuring Line Types 56-26
Creating a Regular Line 56-26
Creating a Shared Extension 56-27
Creating a Monitor Line 56-30
Creating an Overlay or Call Waiting on Overlay Line 56-31
Changing an Overlay Line to Monitor or Regular Line 56-33
Creating a Watch Line 56-34
Phones and Users Reference 56-35
Phones and Users Summary Page 56-36
Edit All Users/Phones Dialog Box 56-38
Create or Edit Phone/User Dialog Box 56-41
Create or Edit Phone/User—Phone Tab 56-42
Create or Edit Phone/User—User Tab 56-47
Create or Edit Phone/User—Mailbox Tab 56-50
Create or Edit Phone/User—Phone Settings Tab 56-54

CHAPTER 57 **Dial Plans** 57-1
Configuring Incoming Dial Plan 57-2
Incoming Dial Plan Reference 57-3
Configure Incoming Dial Plan 57-3
Configuring Outgoing Calls 57-3
Outgoing Call Reference 57-4

Configuring Outgoing Dial Plan 57-4
Configure Incoming Dial Plan, Outgoing Dial Plan, Import Outgoing Dial Plan Template, and Create/Edit Dial Peer 57-4
Configuring International Dial Plan 57-5
Configuring Dial Peer 57-5
Dial Peer Reference 57-5
Create or Edit Dial Peer 57-5
Configuring VoIP Dial Peer 57-5
VoIP Dial Peer Reference 57-6
VoIP Dial Peer 57-6
Configuring Translation Rules and Profiles 57-6
Translation Rules and Profiles Reference 57-6
Create or Edit Translation Rules and Profiles 57-6
Configuring Calling Restrictions 57-7
Calling Restrictions Reference 57-7
Outgoing Call Types and Permissions 57-7
Create or Edit Outgoing Call Type 57-7
Create or Edit Permission 57-7
Configuring Codec Profiles 57-8
Creating, Editing, and Deleting Codec Profiles 57-8
Codec Profiles Reference 57-9
Codec Profiles Summary Page 57-10
Create or Edit Voice Class Codec Dialog Box 57-11

CHAPTER 58 **VoIP Settings** 58-1

VoIP Settings 58-1
Enabling or Disabling VoIP Settings 58-2
VoIP Settings Page 58-3
Edit VoIP Settings Page 58-4

VoIP Settings Feature Behavior 58-11

CHAPTER 59 **Telephony Features 59-1**

After-Hours Tollbar 59-2
After-Hour Tollbar Reference 59-3
Configure After-Hour Tollbar 59-3
Auto Attendant 59-7
Cisco Unified CME Basic Automatic Call Distribution 59-7
Cisco Unified CME Prompts and Scripts 59-7
Call Conferencing 59-8
Call Park 59-8
Call Park Reference 59-9
Configure Call Park page 59-9
Create or Edit Call-Park Parameters 59-10
Create or Edit Call-Park Parameters—General Tab 59-11
Create or Edit Call-Park Parameters—Advanced Tab 59-12
Call Pickup Groups 59-13
Call Pickup Group Reference 59-14
Configure Pickup Group 59-14
Create or Edit a Pickup Group 59-15
Directory Services 59-16
Directory Services Reference 59-16
Configure Directory Services 59-16
Create or Edit a Directory Entry 59-17
Hunt Groups 59-18
Working with Hunt Groups 59-19
Creating Hunt Groups 59-19
Editing Hunt Groups 59-20
Deleting Hunt Groups 59-20

Hunt Groups Reference 59-22
Hunt Groups Summary Page 59-22
Create or Edit a Hunt Group Dialog Box 59-24
Create or Edit a Hunt Group—General Tab 59-24
Set Extension Timeout Dialog Box 59-28
Create or Edit a Hunt Group—Advanced Tab 59-29
Intercom 59-31
Creating, Editing, and Deleting a Regular Intercom Line 59-33
Creating, Editing, and Deleting a Whisper Intercom Line 59-35
Intercom Reference 59-37
Intercom Summary Page 59-37
Setup New Intercom Line or Edit Intercom Dialog Box 59-38
Night Service Bell 59-44
Night Service Bell Reference 59-44
Configure Night Service Bell 59-45
Configuring Night Service Weekly Schedule 59-45
Configuring Night Service Annual Schedule 59-46
Configuring Night Service Daily Schedule 59-47
Configuring Night Service Code 59-48
Paging Numbers 59-49
Creating, Editing, and Deleting a Paging Number 59-49
Paging Numbers Reference 59-51
Paging Numbers Summary Page 59-51
Create or Edit Paging Number Dialog Box 59-53
Set Phones Paging Type Preference Dialog Box 59-55
Paging Groups 59-56
Creating, Editing, and Deleting Paging Groups 59-56
Paging Groups Reference 59-57
Paging Groups Summary Page 59-58
Create or Edit a Paging Group Dialog Box 59-59

Phone Templates 59-62
Phone Template Reference 59-63
Phone Templates page 59-63
Creating or Editing a phone template 59-64
Create or Edit Phone Template dialog box 59-66
Associate Phones dialog box 59-71
Extension Templates 59-72

CHAPTER 60 **Phone Firmware** 60-1
Configuring Phone Firmware 60-2
Phone Firmware Reference 60-2
Phone Firmware Page 60-3
Edit Phone Firmware Settings dialog box 60-6
Registered Phones dialog box 60-6
Phone Firmware Wizard 60-7
Configure phone firmware available on the device flash radio button 60-7
Manual Phone Firmware Configuration dialog box 60-9
Upload phone firmware on the device flash and configure them radio button 60-11
Upload phone firmware on the device flash without configuring them radio button 60-13
FAQ 60-14

CHAPTER 61 **Voicemail** 61-1
Cisco Unity Express Initialization 61-1
Initialization Procedure 61-1
CUE Initialization Wizard Screen Reference 61-3
Service Engine Configuration 61-4
CUE Module Initialization 61-5
Initialization Confirmation 61-7

Cisco Unity Express Module Initialization 61-7
Complete 61-7
Discovery Details Messages 61-8
Configuring Module Settings 61-9
Configuring Voicemail 61-9
Voicemail Reference 61-9
Voicemail Settings 61-9
Configuring the Call-in Number 61-11
Call-in Number Reference 61-11
Configure the Call-in Numbers 61-12
Edit or Create Cisco Unity Express Call-in Numbers 61-12
Launching Cisco Unity Express 61-14
Cisco Unity Express Reference 61-14
Launch Cisco Unity Express 61-14

CHAPTER 62 **Media Resource Management and Transcoding** 62-1

PART 6 **Configuring Utilities**

CHAPTER 63 **Utilities** 63-1
Understanding Utilities 63-1
Utility Reference 63-2
Flash File Management 63-2
Software Upgrade 63-3
Managing Software Upgrade 63-3
Software Upgrade Page 63-4
Welcome Page 63-4
Download Image From CCO Page 63-5
Save Existing Image and Config Page 63-6

Select and Upload Image Page 63-7
Configuration Editor 63-8
Save Configuration to PC Page 63-9
Write to Startup Configuration Page 63-9
Telnet Page 63-10
Reload Device Page 63-11
Understanding Ping and Traceroute 63-11
Ping 63-12
Layer 2 Traceroute 63-12
Layer 3 Traceroute 63-12
Configuring Ping and Traceroute 63-14
Ping and Traceroute Dialog Box 63-15
Understanding the View Menu Options 63-16
View Reference 63-17
Running Configuration Page 63-17
IOS Show Commands Page 63-17
Default Rules Page 63-19
This Feature Not Supported 63-21

PART 7 Managing Modules

CHAPTER 64 WAN Optimization 64-1
Understanding WAAS 64-2
Configuring a WAN Optimization Module Interface 64-3
WAN Optimization Reference 64-4
WAN Optimization Module Setup Page 64-4
WAN Optimization Module Setup Wizard Page 64-5
Login Credentials Dialog Box 64-7
WAN Optimization Module Setup Wizard—Welcome Page 64-8

WAN Optimization Module Setup Wizard—Module Configuration page 64-9
WAN Optimization Module Setup Wizard—Configure Interception Method 64-11
WAN Optimization Module Setup Wizard—Select License 64-13
WAN Optimization Module Setup Wizard—Summary 64-15
WAAS Central Manager 64-16

CHAPTER 65 **WAAS Express Registration 65-1**
WAAS Express Registration Basic Workflow 65-1
Understanding WAAS Express 65-2
Registering WAAS Express 65-2
WAAS Express Registration Reference 65-4
Register with WCM page 65-5
EULA Confirmation dialog box 65-6
Status dialog box 65-6
WAAS Express Registration wizard 65-7
WAAS Express Registration wizard—Welcome page 65-8
WAAS Express Registration wizard—WAAS Central Manager page 65-8
WAAS Express Registration wizard—WCM Certificate page 65-8
WAAS Express Registration wizard—Domain Name Configuration page 65-9
WAAS Express Registration wizard—Digital Certificate page 65-9
WAAS Express Registration wizard—WCM Login Credentials page 65-10

CHAPTER 66 **Application Extension Platform 66-1**

CHAPTER 67 **Network Module Management 67-1**
AIM Module Management 67-1

AIM Sensor Interface IP Address 67-3
IP Address Determination 67-4
Configuration Checklist 67-5
Interface Monitoring Configuration 67-6
Network Module Login 67-7
Switch Module Interface Selection 67-7
Managing the IPS Sensor 67-8
IPS Sensor Reference 67-8
IPS Sensor 67-8
Sensor Failover Settings 67-10
IPS Sensor Configuration Checklist 67-11
Interface Monitoring Configuration 67-12
Monitoring Settings 67-12

CHAPTER 68 Video Surveillance 68-1
Video Management Initialization Wizard Screen Reference 68-1
Initialization Page 68-2
Module Initialization Wizard—Service Engine Configuration 68-2
Module Initialization Wizard—Module Configuration Page 68-3
Module Initialization Wizard—Confirmation Page 68-5
Module Initialization Wizard—Module Initialization Page 68-5
Module Initialization Wizard—Complete Page 68-6
Video Gateway Initialization Wizard Screen Reference 68-7
Initialization Page 68-7
Module Initialization Wizard—Service Engine Configuration 68-8
Module Initialization Wizard—Module Configuration Page 68-9
Module Initialization Wizard—Confirmation Page 68-11
Module Initialization Wizard—Module Initialization Page 68-11
Module Initialization Wizard—Complete Page 68-12

Integrated Storage System Initialization Wizard Screen Reference 68-12
Initialization Page 68-13
Module Initialization Wizard—Service Engine Configuration 68-13
Module Initialization Wizard—Module Configuration Page 68-14
Module Initialization Wizard—Confirmation Page 68-16
Module Initialization Wizard—Module Initialization Page 68-16
Module Initialization Wizard—Complete Page 68-17

PART 8 Managing Licenses

CHAPTER 69 License Management 69-1
License Dashboard Screencast 69-1

PART 8 Monitoring the Router

CHAPTER 70 Viewing Router Information 70-1
Overview 70-2
Interface Status 70-6
Environment 70-9
Logging 70-10
Syslog 70-10
Firewall Log 70-13
Application Security Log 70-15
SDEE Message Log 70-16
Traffic Status 70-17
Netflow Top Talkers 70-18
Top Protocols 70-18
Top Talkers 70-18
QoS 70-19

Application/Protocol Traffic 70-21
Firewall Status 70-22
Zone-Based Policy Firewall Status 70-23
VPN Status 70-25
IPSec Tunnels 70-25
DMVPN Tunnels 70-27
Easy VPN Server 70-28
IKE SAs 70-30
SSL VPN Components 70-31
SSL VPN Context 70-32
User Sessions 70-32
URL Mangling 70-33
Port Forwarding 70-33
CIFS 70-34
Full Tunnel 70-34
User List 70-35
IPS Status 70-36
IPS Signature Statistics 70-37
IPS Alert Statistics 70-38
NAC Status 70-39
802.1x Authentication Status 70-40
Traffic Monitoring 70-41
Traffic Volume 70-41

PART 10 Configuring Switches

CHAPTER 71 IP Address 71-1
Assign IP Address 71-2
IP Address Reference 71-3

IP Address Summary Page 71-3

CHAPTER 72 **Port** 72-1

Configuring Port 72-1

How to Edit a Port 72-2

Port Reference 72-4

Port Summary Page 72-4

Edit Port Dialog Box 72-7

Runtime Status 72-12

Refreshing the Runtime Status Page 72-12

Runtime Status Summary Page 72-13

CHAPTER 73 **EtherChannel** 73-1

EtherChannel Overview 73-1

Load Balancing and Forwarding Methods 73-2

Configuring EtherChannel 73-4

EtherChannel Configuration Guidelines 73-4

Creating, Editing and Deleting an EtherChannel 73-5

EtherChannel Reference 73-7

EtherChannel Summary Page 73-7

Create or Edit EtherChannel Dialog Box 73-9

CHAPTER 74 **Smartport** 74-1

Port Setup 74-2

Apply or Edit the Role for an interface 74-2

Port Setup Reference 74-3

Port Setup Summary Page 74-3

Edit Port Setup Dialog Box 74-4

Device Setup 74-7

How to Apply or Remove the Device role 74-7
Device Setup Reference 74-8
Device Setup Summary Page 74-8

CHAPTER 75 **VLAN Settings** 75-1
Configure VLANs 75-1
VLAN Configuration Guidelines 75-3
Creating, Editing, and Deleting a VLAN 75-4
VLAN Reference 75-6
Configure VLAN Summary Page 75-6
Create or Edit VLAN Dialog Box 75-7
Configure Port 75-9
How to Edit a Port Mode 75-11
Port Reference 75-12
Configure Port Summary Page 75-12
Edit Port Mode Dialog Box 75-14

CHAPTER 76 **PoE** 76-1
Understanding PoE 76-1
Supported Protocols and Standards 76-2
Power Management Modes 76-2
Configuring PoE 76-3
Managing PoE 76-4
PoE Reference 76-4
PoE Summary Page 76-5
Edit PoE Dialog Box 76-5

CHAPTER 77 **Device Alarm** 77-1
Configuring System Alarms 77-2

External Alarm Input 77-3
Power Supply Alarms 77-3
Applying Alarm Settings for the Device 77-4
Device Alarm Reference 77-5
Device Alarm Summary Page 77-5

CHAPTER 78 **ModBus** 78-1
Understanding ModBus 78-1
MODBUS and Security 78-2
Multiple Request Messages 78-2
Configuring MODBUS 78-2
ModBus Reference 78-3
ModBus Dialog Box 78-3

CHAPTER 79 **Quality of Service Classes** 79-1
QoS Classes 79-3
Creating, Editing and Deleting a QoS Classes 79-3
QoS Class Reference 79-5
QoS Classes Summary Page 79-5
Create and Edit QoS Classes Dialog Box 79-6

CHAPTER 80 **QoS Policies** 80-1
Input and Output Policies 80-2
Ingress Policy 80-3
Creating, Editing, and Deleting the Ingress Policy 80-4
Ingress Policy Reference 80-7
Ingress Policy Summary Page 80-7
Create or Edit QoS Ingress Policy Dialog Box 80-8
Assign Class To Policy Dialog Box 80-11
Create, Edit, and Delete the parameters of QoS Class 80-11

Assign Class To Policy—Flat 80-16
Assign Class To Policy—Hierarchical 80-23
Egress Policy 80-24
Creating, Editing, and Deleting the Egress Policy 80-25
Egress Policy Reference 80-28
Egress Policy Summary Page 80-28
Create or Edit QoS Egress Policy 80-29
Assign Class To Policy Dialog Box 80-31
Create, Edit, and Delete the parameters of QoS Class for the QoS Policy 80-31
Assign Class to Policy—Flat 80-35
Attach 80-38
Attach Policy to an Interface 80-38
Attach Policy Reference 80-39
Attach Policy Summary Page 80-39
Edit QoS Policy Attach Dialog Box 80-40

CHAPTER 81 Quality of Service Report 81-1
DSCP Statistics 81-2
Refreshing the DSCP Statistic Page 81-2
DSCP Statistics Summary Page 81-2
Class of Service Statistics 81-3
Refreshing the CoS Statistics Page 81-3
CoS Statistics Summary Page 81-4
Policer Statistics 81-4
Refreshing the Policer Statistics Page 81-5
Policer Statistic Summary Page 81-5

CHAPTER 82 **STP Configuration** 82-1

STP Status 82-2
To Apply Global Spanning-Tree Protocol 82-2
STP Status Reference 82-3
STP Status Summary Page 82-3
Bridge Parameters 82-5
To Edit the STP Bridge Parameters 82-5
Bridge Parameters Reference 82-6
Bridge Parameters Summary Page 82-6
Edit STP Bridge Parameters Dialog Box 82-7
Port Parameters 82-9
To Enable BPDU Guard 82-9
To Edit the STP Port Parameters 82-10
Port Parameters Reference 82-11
Port Parameters Summary Page 82-11
Edit STP Port Parameters Dialog Box 82-12
Port State Tables 82-14
Port Role 82-15

CHAPTER 83 **STP Monitor** 83-1

STP Status 83-2
Enable or Disable STP on a VLAN 83-2
STP Status Reference 83-3
STP Status Summary Page 83-3
Edit STP Status Dialog Box 83-4
Current Roots 83-6
Refreshing the Current Roots Page 83-6
Current Roots Reference 83-7
Current Roots Summary Page 83-7

CHAPTER 84 **REP** 84-1

Configuring REP 84-2

Characteristics of REP segment 84-2

Limitations of REP segments 84-2

Create, Edit, or Delete REP Segment 84-4

REP Reference 84-6

REP Summary Page 84-6

Create or Edit REP Segment Dialog Box 84-7

Default REP Configuration 84-10

CHAPTER 85 **Media Access Control Address** 85-1

Managing MAC Address 85-1

Dynamic Address 85-2

Refreshing and Removing All the MAC Address 85-2

MAC Address Reference 85-2

MAC address Summary Page 85-3

Aging 85-3

Guidelines on Changing the Address Aging Time 85-4

To Set Aging Parameters 85-4

Aging Reference 85-5

Aging Summary Page 85-5

Static Address Page 85-6

Create Static Address Dialog Box 85-8

Secure Address Page 85-9

CHAPTER 86 **ACL** 86-1

Configuring ACL 86-2

Creating, Editing, and Deleting an ACL 86-3

Access Control List Reference 86-5

Access Control List Summary Page 86-5
Create or Edit Access Control List Window 86-6
Access Control Element 86-8
ACL with Standard IP 86-8
Creating, Editing, and Deleting an ACE with Standard IP 86-9
Create or Edit ACE with Standard IP 86-11
ACL with Extended IP 86-13
Creating, Editing, and Deleting an ACE with Extended IP 86-13
Create or Edit ACE with Extended IP 86-16
TCP Application and Port Number Table 86-21
UDP Application and Port Number Table 86-23
ACL with MAC Extended 86-25
Creating, Editing, and Deleting an ACE with MAC Extended 86-25
Create or Edit ACE with MAC Extended 86-27
Attach ACL 86-29
Attach or Detach ACL to an Interface 86-29
Attach ACL Reference 86-30
Attach ACL Summary Page 86-30
Attach or Detach ACL Dialog Box 86-31
Time Range 86-33
To Set Time Range for an ACL 86-33
Creating, Editing, and Deleting a Time Range for an ACL 86-34
Time Range Reference 86-35
Time Range Summary Page 86-36
Create or Edit Time Range window 86-37
Time Range Entry 86-38
Creating, Editing, and Deleting the Time Range Entries 86-38
Create or Edit Time Range Entry Window 86-40

CHAPTER 87 **Port Security** 87-1

Secure MAC Addresses 87-2
Security Violations 87-2
Configuring Port Security 87-3
Enable or Disable Port Security 87-4
Enabling and Configuring Port Security Aging 87-6
How to set the Aging Parameters 87-6
Port Security Reference 87-7
Port Security Summary Page 87-7
Edit Port Security Dialog Box 87-8
Set Default Configuration 87-11

CHAPTER 88 **802.1x** 88-1

802.1x 88-2
802.1x Configuration Guidelines 88-2
Configurational Guidelines 88-2
Assign 802.1x to an Interface 88-3
To Delete 802.1x Configuration from an Interface 88-6
802.1x References 88-6
802.1x Summary Page 88-7
802.1x Configuration For Interface Page 88-8
Welcome 88-8
802.1x Wizard Configuration 88-9
WEB-Authentication 88-9
Authentication with Wake-on-LAN 88-9
To Set 802.1x Parameters 88-10
802.1x Wizard Configuration Screen 88-12
Select Interface 88-17
To Assign 802.1x To an Interface 88-17
Select Interface Screen 88-18

CHAPTER 89 **Security Wizard** 89-1

Configuring Security Wizard 89-1

Security Wizard Reference 89-3

Security Wizard Page 89-3

Security Wizard: Welcome Page 89-4

Security Wizard: Select Restriction Type 89-5

Security Wizard: Specify Destination IP Addresses 89-6

Security Wizard: Select Interfaces 89-7

Security Wizard: Specify Source IP Addresses 89-8

Security Wizard: Select Interfaces to be Restricted 89-9

Security Wizard: Specify Source IP Addresses 89-10

Security Wizard: Specify Application 89-11

Security Wizard: Select Interfaces 89-12

PART 11 **Monitoring Switches**

CHAPTER 90 **Port Statistics** 90-1

Transmit Packets 90-1

Refreshing the Transmit Packet Page 90-1

Transmit Packets Summary Page 90-2

Receive Packets 90-3

Refreshing the Receive Packet Page 90-3

Receive Packets Summary Page 90-3

CHAPTER 91 **Resilient Ethernet Protocol Segment** 91-1

REP Segment Summary Page 91-2

CHAPTER 92 **Health** 92-1

Health Summary Page 92-1

CHAPTER 93 **Reload Device** 93-1

PART 12 **Additional Information**

CHAPTER 94 **Application Security** 94-1

- Application Security Windows 94-2
- No Application Security Policy 94-3
- E-mail 94-4
- Instant Messaging 94-5
- Peer-to-Peer Applications 94-6
- URL Filtering 94-7
- HTTP 94-8
  - Header Options 94-10
  - Content Options 94-10
- Applications/Protocols 94-12
  - Timeouts and Thresholds for Inspect Parameter Maps and CBAC 94-13
  - Associate Policy with an Interface 94-16
  - Edit Inspection Rule 94-16
  - Permit, Block, and Alarm Controls 94-18

CHAPTER 95 **Tools Menu Commands** 95-1

- Ping 95-1
- Telnet 95-2
- Internal Access Point Screens 95-2
  - IP Address 95-2
  - Warning Message 95-3
- Security Audit 95-5
- USB Token PIN Settings 95-5

Wireless Application 95-6
CCO Login 95-7

CHAPTER 96 URL Filtering 96-1
URL Filtering Window 96-2
Edit Global Settings 96-2
General Settings for URL Filtering 96-3
Local URL List 96-5
Add or Edit Local URL 96-6
Import URL List 96-7
URL Filter Servers 96-7
Add or Edit a URL Filter Server 96-8
URL Filtering Precedence 96-9

CHAPTER 97 More About.... 97-1
IP Addresses and Subnet Masks 97-1
Host and Network Fields 97-3
Available Interface Configurations 97-4
DHCP Address Pools 97-5
Meanings of the Permit and Deny Keywords 97-6
Services and Ports 97-6
More About NAT 97-13
Static Address Translation Scenarios 97-13
Dynamic Address Translation Scenarios 97-16
Reasons that Cisco CP Cannot Edit a NAT Rule 97-17
More About VPN 97-18
Cisco.com Resources 97-18
More about VPN Connections and IPSec Policies 97-19
More About IKE 97-21

More About IKE Policies **97-22**

Allowable Transform Combinations **97-23**

Reasons Why a Serial Interface or Subinterface Configuration May Be Read-Only **97-24**

Reasons Why an ATM Interface or Subinterface Configuration May Be Read-Only **97-25**

Reasons Why an Ethernet Interface Configuration May Be Read-Only **97-26**

Reasons Why an ISDN BRI Interface Configuration May Be Read-Only **97-27**

Reasons Why an Analog Modem Interface Configuration May Be Read-Only **97-28**

DMVPN Configuration Recommendations **97-29**

Routing and Security White Papers **97-30**

GLOSSARY

INDEX

Preface

This preface describes the audience and conventions of the *Cisco Configuration Professional User Guide*. It also describes the available product documentation and provides information on how to obtain documentation and technical assistance.

- Audience, page 65
- Conventions, page 66
- Related Documentation, page 67
- Obtaining Documentation and Submitting a Service Request, page 68

Audience

This guide is intended primarily for network administrators and channel partners.

Conventions

This guide uses the following conventions:

Item	Convention
Commands and keywords.	**boldface** font
Variables for which you supply values.	*italic* font
Optional command keywords. You do not have to select any options.	[enclosed in brackets]
Required command keyword to be selected from a set of options. You must choose one option.	{options enclosed in braces | separated by vertical bar}
Displayed session and system information.	`screen` font
Information you enter.	**`boldface screen`** `font`
Variables you enter.	*`italic screen`* font
Menu items and button names.	**boldface** font
Choosing a menu item.	**Option > Network Preferences**

Note Means *reader take note*.

Tip Means *the following information will help you solve a problem*.

Caution Means *reader be careful*. In this situation, you might perform an action that could result in equipment damage or loss of data.

Timesaver Means *the described action saves time*. You can save time by performing the action described in the paragraph.

Warning **Means *reader be warned*. In this situation, you might perform an action that could result in bodily injury.**

Related Documentation

Table 1 describes the related documentation available for Cisco Configuration Professional.

Table 1 Cisco Configuration Professional Documentation

Document Title	Available Formats
Readme First for Cisco Configuration Professional	This document is available in the following locations: • On Cisco.com. • On the product CD-ROM in the Documentation folder.
Cisco Configuration Professional Quick Start Guide	This guide is available in the following locations: • On Cisco.com. • On the product CD-ROM in the Documentation folder.
Cisco Configuration Professional Getting Started Guide	This guide is available in the following locations: • On Cisco.com. • On the product CD-ROM in the Documentation folder. • During the installation process, just before you have finished installing the product, you are provided the option to read the Getting Started guide.
Cisco Configuration Professional User Guide	This guide is available in the following locations: • On Cisco.com. • Accessible from Online help.
Cisco Configuration Professional Express User Guide	This guide is available in the following locations: • On Cisco. com. • Accessible from Online help.

Table 1 Cisco Configuration Professional Documentation (continued)

Document Title	Available Formats
Release Notes for Cisco Configuration Professional	This document is available in the following location: • On Cisco.com.
Release Notes for Cisco Configuration Professional Express	This document is available in the following location: • On Cisco.com.

Obtaining Documentation and Submitting a Service Request

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

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

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

PART 1

Getting Started with Cisco Configuration Professional

This section introduces Cisco Configuration Professional and provides getting started information.

CHAPTER 1

Getting Started

This chapter introduces Cisco Configuration Professional (Cisco CP) and provides information about the Cisco CP user interface. It contains the following sections:

- Understanding Cisco CP, page 1-1
- Understanding the Cisco CP User Interface, page 1-2
- Additional Help Topics, page 1-18

Understanding Cisco CP

Cisco CP is a GUI based device management tool for Cisco access routers. This tool simplifies routing, firewall, IPS, VPN, unified communications, and WAN, and LAN configurations through GUI-based wizards.

Cisco CP is a valuable productivity enhancing tool for network administrators and channel partners for deploying routers with increased confidence and ease. It offers a one-click router lock-down and an innovative voice and security auditing capability to check and recommend changes to router configurations. Cisco CP also monitors router status and troubleshoots WAN and VPN connectivity issues.

Cisco CP is free and you can download it from:

www.cisco.com/go/ciscocp

Understanding the Cisco CP User Interface

Cisco CP eliminates the need for multiple device managers by providing a single tool to configure and manage devices.

The following sections describe the Cisco CP user interface:

- Window Layout, page 1-2
- Menu Bar, page 1-3
- Toolbar, page 1-4
- Status Bar, page 1-6

Window Layout

The user interface makes it easy to manage networking features. These are the main parts that define the user interface:

- Menu Bar—Row of menus across the top of the window. It offers application services, a list of open windows, and online help.
- Toolbar—Row of icons directly below the menu bar. They represent the most often used application services and most often configured networking features.
- Left Navigation Pane—Scalable panel on the left side of the content pane in which you select the features to configure and monitor.
- Content Pane—Right side of the workspace, in which windows appear. You view reports here and enter information that configures networking features.
- Status Bar—Bar at the bottom of the window, where Cisco CP displays the status of the application.

Menu Bar

Table 1-1 describes the row of menus across the top of the window that offers application services.

Table 1-1 Menu Bar

Menu	Options
Application	Contains the following options: • Manage Community—Allows you to create a new community or choose an existing community. See Chapter 2, "Device Communities." • Setup New Device—Allows you to set up a new device. See the "Setup New Device" section on page 1-9. • Create User Profile—Allows you to restrict users from using all of the features that are available in the left navigation pane. See the "User Profile" section on page 1-11. • Import User Profile—Allows you to import a user profile. See the "User Profile" section on page 1-11. • Options—Allows you to set user preferences such as log level, show community at startup, and show CLI preview parameters. See the "Options" section on page 1-12. • Template—Allows you to create, edit, or apply a template. See the "Templates" section on page 1-15. • Work Offline—Allows you to work with Cisco CP in offline mode. See the "Offline Mode" section on page 1-15. • Exit—Exits the Cisco CP application.
Help	Contains the following options: • Help Contents—Displays the online help contents, which includes online help topics and links to screencasts. • Feedback—Displays a feedback form allowing you to provide feedback on Cisco CP. • About—Displays information about Cisco CP, such as the version number, and allows you to view the end-user licence agreement.

Toolbar

Table 1-2 describes the Cisco CP features that are available from the toolbar at the top of the window.

Table 1-2 Toolbar

Tool Icon	Description
	Home button. Click this button to display the Community View page, which summarizes the community information and allows you to add, edit, and discover devices, also to view the discovery and device status of each device.
	Configure button. Click this button to display the features that you can configure on a chosen device. The features are displayed in the left navigation pane. **Note** If a feature (router, security, or voice) is not supported on a device, that feature is not displayed in the left navigation pane. **Note** If the version of Cisco IOS that is installed on the device does not support a specific feature, but an upgrade does support it, that feature is disabled (grayed out) in the left navigation pane.
	Monitor button. Click this button to display the router and security features that you can monitor for a chosen device. The features are displayed in the left navigation pane. **Note** If a feature (router or security) is not supported on a device, that feature is not displayed in the left navigation pane. **Note** If the version of Cisco IOS that is installed on the device does not support a specific feature, but an upgrade does support it, that feature is disabled (grayed out) in the left navigation pane.
	Manage Community icon. Click this icon to open the Manage Community dialog box where you can add a new community or edit an existing community.

Table 1-2 Toolbar (continued)

Tool Icon	Description
	Refresh icon. Click this button to: • Rediscover the selected device in the Select Community Member drop-down menu. • Rediscover and reload the current feature. **Note** Refresh is not available for offline mode. **Note** Refresh is available only after successful discovery of one or more devices. **Note** Clicking the Refresh button refreshes the device selected in the Select Community Member drop-down menu. Selecting a device in the **Home > Dashboard** page and clicking Refresh does not refresh that device.
	Provide feedback to Cisco icon. Click this icon to open the Cisco Configuration Professional Feedback form, which you can use to send feedback about this product to Cisco.

Table 1-2 Toolbar (continued)

Tool Icon	Description
	Help icon. Click this button to open the help page for the active window.
	Search icon. Click the Search icon to search for supported features in Cisco CP. **a.** Type the first letter of the word in the Search text-box. A list of keywords beginning with that letter is displayed. **b.** Choose the desired keyword and click the Search button. The search results display the available features that match the keyword. **c.** Click the feature name. The feature is launched in the right pane. **d.** Click the Search icon to exit search. **Note** Only features supported on the device are displayed in the search results. **Note** The Search option is available when devices are in discovered state.

Status Bar

The status bar displays status information about Cisco CP and selected community members.

Note When you are in the **Home > Dashboard > Community View** page, the padlock icon in the status bar displays the connection mode of the device that is selected in the Select Community Member drop-down list.

Table 1-3 lists the Status Bar icons.

Table 1-3 Status Bar

Feature Icon	Feature Name	Description
	Secure Connection	The locked padlock icon indicates that Cisco CP has a secure connection with the chosen community member.
	Nonsecure Connection	The unlocked padlock icon indicates that Cisco CP has a nonsecure connection with the chosen community member.

Applications Menu Field Reference

- Manage Community, page 1-7
- User Profile, page 1-11
- Options, page 1-12
- Templates, page 1-15
- Offline Mode, page 1-15

Manage Community

See Chapter 2, “Device Communities.”

Setting up a New Device

Before you begin using Cisco CP to set up a new device, you must first ensure that the computer running Cisco CP is connected to the powered up device over the console port and the device baud is set to its default value.

From the Setup New Device wizard, you can set up a new device and manage the device. The setup wizard can also be used to manage a device with existing configuration.

Managing Setup New Device

To set up a new device, use the procedure in this section.

Before You Begin

Make sure that the computer running Cisco CP is connected to the powered up device over the console port and the device baud is set to its default value.

Procedure

Use this procedure to set up a new a device and manage the device.

Step 1 From the menu bar, choose **Application > Setup New Device**. The Introduction page opens.

Step 2 Click the **Next** button. The Testing Connection dialog box opens.

Step 3 In the Testing Connection dialog box, choose the Interface for configuring the IP address. Enter the IP address of the device, subnet mask, username, and password information for the device.

The default username is **ccpuser** and default password is **ccpasswd**. If you change the default credentials, you must confirm the new password in the confirmation field.

Note If you get a warning message that Cisco CP is unable to communicate with the device using baud rate 9600 on serial port COM1, make sure to check the connection to the device by answering the troubleshooting questions.

Step 4 To backup the running configuration, check the **Backup current running configuration on the device flash** check box.

Step 5 Click the **Next** button. The Configuration Summary page is displayed.

Step 6 In the Configuration Summary page, check the **Add this device to CCP's currently selected community** check box.

Step 7 Click **Finish** to complete device setup configuration and include the new device in the community page.

Step 8 Click **Cancel** to cancel the changes that you made.

Setup New Device

Use the Setup New Device wizard to setup a new device and manage the device. In the Introduction page, click the **Next** button to set up the new device.

How to Get to This Dialog Box

From the menu bar, choose **Application > Setup New Device**.

Related Links

- Menu Bar, page 1-3
- Setting up a New Device, page 1-8
- Managing Setup New Device, page 1-8

Setup New Device: Testing Connection

In the Testing Connection dialog box, choose the Interface for configuring the IP address. Enter the IP address of the device, subnet mask, username, and password information for the device.

Note If you get a warning message that the Cisco CP is unable to communicate with the device using baud rate 9600 on serial port COM1, make sure to check the connection to the device by answering the troubleshooting questions.

How to Get to This Dialog Box

From the menu bar, choose **Application > Setup New Device**. Click next to until you get to this page.

Related Links

- Setup New Device, page 1-9
- Setup New Device: Configuration Summary, page 1-11
- Setting up a New Device, page 1-8
- Managing Setup New Device, page 1-8

Field Reference

Table 1-4 lists the fields in the Testing Connection dialog box.

Table 1-4 Testing Connection Dialog Box

Element	Description
Interface for configuring the IP Address	Choose the interface from the drop-down list.
IP Address	Enter the IP address
Subnet Mask	Enter the subnet mask.
Username	Enter the username.
Password	Enter the password.
Backup current running configuration on the device flash	Check this check box to back up the current running configuration on the device flash.
Next	Click the **Next** button to go to next page.
Cancel	Click **Cancel** to discard the configuration change.

Setup New Device: Configuration Summary

The Configuration Summary page displays a summary of the configuration.You can review this information, and if you need to change anything, you can click the **Cancel** button to cancel the configuration that you have entered.

Related Links

- Setup New Device, page 1-9
- Setup New Device: Testing Connection, page 1-9
- Setting up a New Device, page 1-8
- Managing Setup New Device, page 1-8

Field Reference

Table 1-4 lists the fields in the Configuration Summary page.

Table 1-5 Configuration Summary

Element	Description
Add this device to CCP's currently selected community	Check this check box to add the device to the community page.
Finish	Click the **Finish** button to complete the configuration.
Cancel	Click **Cancel** to discard the configuration change.

User Profile

For information about how to use Cisco Configuration Professional (Cisco CP) to create or import user profiles, see the screencast at: http://www.cisco.com/en/US/docs/net_mgmt/cisco_configuration_professional/scrcst/ccpsc.html

You must have Internet access to view the screencast.

Options

Use the Options dialog box to set the user preferences such as log level, show community at startup, and show CLI preview parameters at run time.

How to Get to This Dialog Box

From the menu bar, choose **Application > Options**.

Related Links

- Menu Bar, page 1-3

Field Reference

Table 1-6 lists the fields in the Options Dialog Box.

Table 1-6 Options Dialog Box

Element	Description
Log Level	Choose the log level to display the log file from the drop-down list. The options are: • Error—Choose the Error option to display only error messages in the log file. This option is selected by default. • Debug—Choose the Debug option to display error and debug messages in the log file. Use this option to send the log files to Cisco TAC for assistance when you have experienced a problem with Cisco CP. After you choose the Debug option, recreate the problem to log, and use the Collect Data for TAC Support utility to send the log files to Cisco TAC. For information on this procedure, see Collecting Cisco CP Technical Support Logs, page 2-38. After the problem is fixed, we recommend that you change the log level back to Error.

Table 1-6 Options Dialog Box (continued)

Element	Description
Show Community at Startup check box	By default, the Show Community at Startup check box is checked. When this check box is checked, the Manage Community dialog box is automatically displayed when you start Cisco CP. See Manage Community Dialog Box, page 2-15. Uncheck the Show Community at Startup check box to avoid having Cisco CP display the Manage Community dialog box on startup.
Show CLI Previews check box	By default, the Show CLI Previews check box is checked. When this check box is checked, and you enter the parameters to configure a feature, the Deliver Configuration to Router dialog box opens displaying the CLI commands to be delivered to the router. Uncheck the Show CLI Previews check box to avoid having Cisco CP display the CLI commands in the Deliver Configuration to Router dialog box before configuring a feature.
Save device credentials on this machine check box	While adding device information to a community, you supply IP address and login credentials for the device. By default, this information is saved by the application so you do not have to provide it again the next time the application is launched. If you do not want the login credentials to be saved on the PC, uncheck the **Save device credentials on this machine** check box. If you uncheck the check box, the application prompts for login credentials every time it is launched.
Feature Use Tracking check box	By default, the Feature Use Tracking check box is checked. When this check box is checked, feature usage statistics are tracked. Uncheck the Feature Use Tracking check box to avoid tracking feature usage statistics. For more information, see Feature Use Tracking, page 1-14.

Feature Use Tracking

The usage activity collection feature is designed to automatically provide feedback on how Cisco CP is used to deploy Cisco devices. The data shared by the usage activity collection feature helps Cisco improve the quality of the software. Cisco Systems, Inc. and its subsidiaries are committed to protecting your privacy and ensuring you have a positive experience on our websites and in using our products and services. The Cisco Privacy statement may be accessed at: http://www.cisco.com/web/siteassets/legal/privacy.html.

Usage activity collection is enabled by default, as described in the Supplemental End User License Agreement (EULA) for Cisco CP. To view the EULA, choose **Help > About** from the Cisco CP main menu and click the End User License Agreement link.

Uncheck the Enable Usage Activity Collection option from **Application > Options** to disable collection and transmission of Cisco CP usage data to Cisco.

When this option is enabled, only the following usage activity statistics are collected:

- Cisco CP version and internationalization.
- Types of devices and phones being managed by Cisco CP.
- Software version for each managed device (for example, Cisco IOS version, CME version).
- User actions (which feature navigation folders are opened).
- When Cisco CP applies a configuration to a device, details of the configuration are not recorded, only that you applied a change to the configuration.
- Public IP address of the PC on which Cisco CP is installed and from which the data is sent. This is the WAN or Internet IP address maintained and allocated by your Internet Service Provider (ISP) to the router or firewall at your site.
- Timestamp for each event.

The following information is **not** collected:

- Customer names, addresses, or other identifying information.
- Product serial numbers or other unique identifiers.

- Hostnames or IP addresses for devices that are behind the router or firewall at your site.
- Phone numbers or any other information that could be used to uniquely identify a customer or VAR.
- Cisco.com usernames or passwords.
- Usernames or passwords configured on the device.

Usage activity data is stored in a text file on the PC running Cisco CP and is sent to a server hosted by Cisco on a per-session basis. After the information is sent, it is removed from the user's PC.

Templates

For information about how to use Cisco Configuration Professional (Cisco CP) to configure Templates, see the screencast at: http://www.cisco.com/en/US/docs/net_mgmt/cisco_configuration_professional/scrcst/ccpsc.html.

You must have Internet access to view the screencast.

Offline Mode

Information about how to use Cisco Configuration Professional (Cisco CP) to configure the Offline mode feature is provided in a screencast. Table 1-7 provides information about the dummy devices used in the screencast. It lists the hostnames, the corresponding hardware, and the mode used in the screencast. See Table 1-7 and then view the screencast at:

http://www.cisco.com/en/US/docs/net_mgmt/cisco_configuration_professional/scrcst/ccpsc.html

You must have Internet access to view the screencast.

Table 1-7 Dummy Device Information

Hostname	Hardware	Mode
CISCO-877M	NM-HDV2-1T1/E1	Security-Routing
CISCO-2821-2	WIC-2AM, WIC-2T, HWIC-CABLE-D-2, WIC-1DSU-T1-V2	Security-Routing
CISCO-2811-1	WIC-1B-S/T, VWIC-2MFT-T1-DI, WIC-1ADSL, AIM-IPS-K9	Security-Routing
CISCO-3845-1	HWIC-AP-G-J, WIC-1SHDSL, WIC-1DSU-T1, NM-CIDS-K9, AIM-VPN/HPII-PLUS	Security-Routing
CISCO-2851-2	HWIC-4A/S, HWIC-4SHDSL, HWIC-1T, HWIC-1ADSLI, NME-WAE-502-K9, AIM-VPN/EPII-PLUS	Security-Routing
CISCO-2811-2	FXS-DID,T1-E1	Gateway with SRST
CISCO-2821-3	Default interfaces, no modules	Gateway with SRST
CISCO-3845-2	NME-CUE, FXS-DID, FXS, FXO, DID, T1-PRI, PVDM-32	Cisco Manager Express
CISCO-2821-1	PVDM,VIC2-2FXS, NM-HDV2-1T1/E1	Cisco Manager Express
CISCO-2851-1	VIC2-2BRI-NT/TE	Voice Gateway
CISCO-3825-1	2BRI,CUE	Cisco Manager Express
C1861-SRST-FK9	1861, 4FXS, 4FXO, 8xPOE	Cisco Manager Express
CISCO-SRST-888	Default interfaces, no modules	Gateway with SRST
CISCO-891	8 FE switch ports, 1 FE layer 3, 1 GE layer 3, 1 async, 1 wireless AP, 1 wireless-GE	Security-Routing
C1861-UC-2BRI-K9	1861, BRI, 4FXS, CUE, 8xPOE	Cisco Manager Express
CISCO-3945	PVDM2-32, HWIC-AP-G-E, VIC2-2BRI-NT/TE, NM-HDV2-1T1/E1	Cisco Manger Express
CISCO-3925	PVDM3-64, VIC2-4FXO, NM-HDV2-1T1/E1, PVDM2-48	Cisco Manger Express
CISCO-3845	PVDM2-32, VIC2-2FXS, NM-CUE-EC	Cisco Manger Express

Table 1-7 Dummy Device Information (continued)

Hostname	Hardware	Mode
CISCO-3825	PVDM2-48, VWIC2-2MFT-, VIC2-4FXO, NM-16ESW	Gateway with Cisco Unified SRST
CISCO-2951/K9	PVDM2-64, VIC-4FXS/DID=, HWIC-2FE, WIC-1AM-V2, NME-IPS-K9	Cisco Manger Express
CISCO-2921-1	Default interface	Cisco Manger Express
CISCO-2911/K9	PVDM2-64, VIC2-4FXO, VIC3-4FXS/DID	Cisco Manger Express
CISCO-2901/K9	Default Interface	Cisco Manger Express
CISCO-2851	VIC2-2BRI-NT/TE, NME-APPRE-502-K9	Cisco Manger Express
CISCO-2821	HWIC-3G-CDMA-S, HWIC-3G-GSM, HWIC-3G-CDMA-V, EVM-HD-8FXS/DID, EM-4BRI-NT/TE, EM-HDA-6FXO	Cisco Manger Express
CISCO-2811	HWIC-4SHDSL, NM-HDV2-2T1/E1, PVDM2-48, AIM-CUE,	Gateway with Cisco Unified CME as SRST
CISCO-2801	AIM-VPN/EPII-PLUS, AIM-VPN/SSL-2	Security-Routing
CISCO-1941	EHWIC-D-8ESG	Security-Routing
CISCO-1861-W	PVDM2-32, VIC3-4FXS/DID, VIC2-4FXO	Cisco Manger Express
CISCO-1841	WIC-1SHDSL-V3	Security-Routing
CISCO876W-G-E-K9	No modules	Security Routing
CISCO1811W-AG-A/K9	2FE, Dual Band 802.11 A+B/G Radio Access Point	Security Routing
CISCO1805-D	HWIC-CABLE-E/J-2, HWIC-4ESW	Security Routing
CISCO1841	WIC-1SHDSL-V3, HWIC-16A	Security Routing
CISCO2801	AIM-VPN/EPII-PLUS, AIM-VPN/SSL-2	Security Routing
CISCO1801-M/K9	1FE ADSLoPOTS	Security Routing
CISCO877W-G-A-M-K9	No modules	Security Routing
CISCO887G-K9	No modules	Security Routing
CISCO1802/K9	1FE ADSLoISDN, ILPM-8, Dual Band 802.11 A+B/G Radio Access Point	Security Routing

Table 1-7 Dummy Device Information (continued)

Hostname	Hardware	Mode
CISCO1941	EHWIC-D-8ESG	Security Routing
CISCO2801	AIM-VPN/EPII-PLUS, AIM-VPN/SSL-2	Security Routing
CISCO1812/K9	No modules	Security Routing

Additional Help Topics

This section contains the following parts:

- USB Token PIN Settings, page 1-18
- Deliver Configuration to Router, page 1-19
- Communication Ports, page 1-20

USB Token PIN Settings

The USB Token PIN Settings dialog box allows you to set PINs for USB tokens connected to your router.

Select a PIN Type

Choose **User PIN** to set a user PIN, or choose **Admin PIN** to set an administrator PIN. A user PIN is used to log into a router.

If you connect a USB token to a router, and the token name and user PIN match an entry in the USB Tokens page (**Configure > Security > VPN Components > Public Key Infrastructure > USB Tokens**), you are automatically logged into that router.

An administrator PIN is used to manage USB token settings using the software of the manufacturer. Cisco CP allows you to change the administrator PIN for a USB token if you can supply the current administrator PIN.

Token Name

Enter the USB token name.

The token name is set by the manufacturer. For example, USB tokens manufactured by a company are named eToken.

You can also use the name "usbtoken*x*", where *x* is the number of the USB port to which the USB token is connected. For example, a USB token connected to USB port 0 is named usbtoken0.

Current PIN

Enter the existing user or administrator PIN. If you do not know the existing PIN, you must use the USB token manufacturer's software to find it.

New PIN

Enter a new PIN for the USB token. The existing PIN is replaced by the new PIN. The new PIN must be at least four digits long.

Confirm PIN

Reenter the new PIN to confirm it.

Save the New PIN to Router

Check the **Save the new PIN to router** check box to save the new PIN as an entry in **Configure > VPN Components > Public Key Infrastructure > USB Tokens**. If an entry with the same name already exists in **Configure > VPN Components > Public Key Infrastructure > USB Tokens**, it is replaced with the new one.

The Save the new PIN to router check box is available only for user PINs.

Deliver Configuration to Router

This window lets you deliver to the router any configuration changes that you have made using Cisco CP. Note that any changes to the configuration that you made using Cisco CP does not affect the router until you deliver the configuration.

Field Reference

Table 1-8 lists the fields in the Deliver Configuration to Router window.

Table 1-8 Deliver Configuration to Router

Element	Description
Save Running Config to Router's Startup Config	Check this check box to cause Cisco CP to save the configuration shown in the window to both the router running configuration file and the startup file. The running configuration file is temporary—it is erased when the router is rebooted. Saving the configuration to the router startup configuration causes the configuration changes to be retained after a reboot. If Cisco CP is being used to configure a Cisco 7000 router, the check box **Save running config. to router's startup config.** will be disabled if there are **boot network** or **boot host** commands present with **service config** commands in the running configuration.
Cancel	To discard the configuration change and close the Cisco CP Deliver to Router dialog box, click **Cancel**.
Save to File	To save the configuration changes shown in the window to a text file, click **Save to File**.

Communication Ports

Table 1-9 provides the communication ports that must be available on Cisco IOS devices or on your PC.

Table 1-9 Communication Ports

Accessible From	Port Number	Description
Cisco IOS devices	22	SSH
Cisco IOS devices	23	Telnet
Cisco IOS devices	80	HTTP
Cisco IOS devices	443	HTTPS
PC	2038	Flex FDS and RTMP
PC	Any free port between 5050 and 10000	SDM Applet

Table 1-9 Communication Ports (continued)

Accessible From	Port Number	Description
PC	One of the following ports: 8600, 8610, 8620, or 8630	Tomcat and Flex AMF
PC	One of the following ports: 61616, 5000, 5010, or 5020	ActiveMQ JMS
PC	9610	Licensing server port
PC	9710	Licensing event listener port
PC	9810	Licensing HTTP file server port

Feature Unavailable

This window appears when you try to configure a feature that the Cisco IOS image on your router does not support. To use this feature, obtain a Cisco IOS image from Cisco.com that supports it.

CHAPTER 2

Device Communities

Before you can configure devices using Cisco Configuration Professional (Cisco CP) you must enter the IP address or hostname, and the credentials information of the devices to manage. To do this, you must first create a community, and then add devices to that community.

The following sections provide more information:

- Device Community Basic Workflow, page 2-1
- Understanding Device Communities, page 2-2
- Managing the Devices in a Community, page 2-8
- Device Community Reference, page 2-15
- Supplementary Information, page 2-28

Device Community Basic Workflow

0. Create a community.
1. Add devices to that community.
2. Discover the devices in the community.

Understanding Device Communities

Before you begin using Cisco CP, you must first create a community and then add devices to that community. When you start Cisco CP for the first time, Cisco CP automatically creates a community for you, to which you can add devices.

A community is basically a group of devices (community members). A single community can contain a maximum of 10 devices. You can create a community and then add the devices to it based on some common parameters. For example, you can create communities based on the location of the devices. You can create a San Jose community and add devices to it, then you can create a Bangalore community and add devices to it, and so on.

When you add a device to a community, you must specify its IP address or hostname, credential information (username and password), and other optional parameters. Cisco CP uses this information to discover the device. After you discover the device, you can configure and monitor it.

You can create and manage communities from the Manage Community dialog box. This dialog box is automatically displayed when you start Cisco CP. From the Manage Community dialog box, you can create communities, change the community name, delete a community, add devices to a community, export and import community information, and discover all the devices in a community. See Working with Communities, page 2-2.

Note If you switch between communities, the status of the devices in the community from which you switched, changes to Not Discovered. To configure devices in that community, you must re-discover the devices.

Working with Communities

This section contains the following topics:

- Creating a Community and Adding Devices, page 2-3
- Adding Communities, page 2-4
- Changing the Community Name, page 2-5
- Deleting a Community, page 2-5
- Exporting and Importing Communities, page 2-6

Creating a Community and Adding Devices

Procedure

Use this procedure to create a community, add devices to it, and discover all the devices in a community.

Step 1 Use the Manage Community dialog box to create communities. The Manage Community dialog box automatically displays when you start Cisco CP, and a community called New Community is created by default. You can change the default community name. See Changing the Community Name, page 2-5.

You can also open the Manage Community dialog box in the following ways:

- From the toolbar, click the **Manage Community** icon.
- From the menu bar, choose **Application > Manage Community**.

See Manage Community Dialog Box, page 2-15.

Step 2 In the Manage Community dialog box, enter the IP address or hostname and the username and password information for the devices to configure.

If you enter the default username **cisco** and default password **cisco**, the Change Default Credentials dialog box opens. For security reasons, you must change the default credentials to new credentials. See Change Default Credential Dialog Box, page 2-18.

Step 3 To have Cisco CP connect securely with the device, check the **Connect Securely** check box. To view the port information, click the down-arrow next to the Connect Securely check box.

Step 4 To change the default port information, click it and enter a new port value.

Note Make sure that Cisco CP can access the device at the specified secure or non-secure ports.

Step 5 To have Cisco CP discover all the devices in a community, check the **Discover All Devices** check box. You can choose to discover the devices later, from the Community View page. See Discovering Devices, page 2-12.

Step 6 Click **OK**. The Community View page opens. It displays the information about the devices in the community. See Community View Page, page 2-19.

Related Topics

- Device Community Basic Workflow, page 2-1
- Understanding Device Communities, page 2-2
- Manage Community Dialog Box, page 2-15
- Change Default Credential Dialog Box, page 2-18
- Adding Communities, page 2-4
- Deleting a Community, page 2-5
- Exporting and Importing Communities, page 2-6

Adding Communities

Procedure

Use this procedure to add a new community.

Step 1 From the menu bar, choose **Application > Manage Community**. The Manage Community dialog box opens. See Manage Community Dialog Box, page 2-15.

Step 2 To add a community, do one of the following:

- Click the **Add** icon located on the top left corner. A community called, New Community, is created. You can change the name of the new community. See Changing the Community Name, page 2-5.
- Right-click an existing community, and choose **New Community** from the displayed menu options. A community called New Community is created. You can change the name of the new community. See Changing the Community Name, page 2-5.

Related Topics

- Device Community Basic Workflow, page 2-1
- Understanding Device Communities, page 2-2
- Creating a Community and Adding Devices, page 2-3
- Deleting a Community, page 2-5
- Exporting and Importing Communities, page 2-6

Changing the Community Name

Before You Begin

Make sure that you have created a community.

Procedure

Use this procedure to change the name of a community.

Step 1 From the menu bar, choose **Application > Manage Community**. The Manage Community dialog box opens. See Manage Community Dialog Box, page 2-15.

Step 2 To change the name of a community, do one of the following:

- Click the name of the community to change, the community name is highlighted and becomes editable. Enter a new name for the community.
- Choose the community with the name to change and click the **Edit** icon (pencil icon) located on the top left corner. The community name is highlighted and becomes editable. Enter a new name for the community.
- Right-click the community with the name to change and choose **Rename Community** from the displayed menu options. The community name is highlighted and becomes editable. Enter a new name for the community.

Related Topics

- Device Community Basic Workflow, page 2-1
- Understanding Device Communities, page 2-2
- Creating a Community and Adding Devices, page 2-3
- Exporting and Importing Communities, page 2-6

Deleting a Community

Before You Begin

Make sure that you have created a community.

Procedure

Use this procedure to delete a community.

Step 1 From the menu bar, choose **Application > Manage Community**. The Manage Community dialog box opens. See Manage Community Dialog Box, page 2-15.

Step 2 To delete a community, do one of the following:

- Choose the community to delete and click the **Delete** icon (trash icon) located on the top left corner. A confirmation dialog box opens. Click **Yes** in the confirmation dialog box to delete the community.
- Right-click the community to delete and choose **Delete Community** from the displayed menu options. A confirmation dialog box appears. Click **Yes** in the confirmation dialog box to delete the community.

Related Topics

- Device Community Basic Workflow, page 2-1
- Understanding Device Communities, page 2-2
- Creating a Community and Adding Devices, page 2-3
- Exporting and Importing Communities, page 2-6

Exporting and Importing Communities

Before You Begin

Make sure that you have created a community and added devices to it. See Creating a Community and Adding Devices, page 2-3 and Adding a Device to a Community, page 2-8.

Procedure

Use this procedure to save (export) the information about all the comminutes in Cisco CP to a file on your PC, and then import that information from your PC into Cisco CP.

Step 1 From the menu bar, choose **Application > Manage Community**. The Manage Community dialog box opens. See Manage Community Dialog Box, page 2-15.

Step 2 To save the information about all the comminutes in Cisco CP to a file on your PC, do the following:

a. From the Manage Community dialog box, click the **Export** (disc) icon located on the top left corner. Cisco CP performs the necessary validation.

b. If validation fails, the system reports the error, and then stops the save operation.

c. If validation succeeds, the **Save Location to Download from Local Host** page opens from which you can select a file or add a new file name to save the community information.

d. Select a file or add a new file name and click **Save**.

Step 3 To import the community information from your PC into Cisco CP, do the following:

a. From the Manage Community dialog box, click the **Import** icon located on the top left corner. Cisco CP validates the existing communities before importing them.

b. If validation fails, the system reports the error, and then stops the import operation.

c. If validation succeeds, the **Select File to Upload by Local Host** page opens from which you can select the file to import.

d. Select the file to import and click **Open**.

e. Cisco CP imports the selected file and displays the communities with all its community members (devices) in the Manage Community dialog box.

If the name of the community that you import is already used, Cisco CP appends the community name with an incremental number. For example, if the community that you import is called Colorado, and that name is already used, Cisco CP renames it to Colorado 1.

Note You can import a maximum of 25 communities.

f. If you want to change the community name, see Changing the Community Name, page 2-5.

Related Topics

- Device Community Basic Workflow, page 2-1
- Understanding Device Communities, page 2-2
- Creating a Community and Adding Devices, page 2-3
- Changing the Community Name, page 2-5

Managing the Devices in a Community

After you create a community and add devices to it, you can view the information for that community in the Community View page. From the Community View page, you can manage the devices (community members) in a community, such as add devices to a selected community, edit device information, delete devices, discover the devices, view information about the discovery process, and view hardware and software information about a selected device. See Working with Devices in a Community, page 2-8.

Working with Devices in a Community

This section contains the following topics:

- Adding a Device to a Community, page 2-8
- Editing Device Information, page 2-10
- Deleting a Device from a Community, page 2-11
- Discovering Devices, page 2-12
- Displaying Discovery Process Details, page 2-14
- Displaying Information About a Discovered Device, page 2-14

Adding a Device to a Community

You can add devices to a community when you create a community in the Manage Community dialog box, or you can add devices to a community later, from the Community View page.

To add devices to a community from the Manage Community dialog box, see Creating a Community and Adding Devices, page 2-3.

To add devices to a community from the Community View page, use the procedure in this section.

Before You Begin

Make sure that you have created a community.

Procedure

Use this procedure to add a device to a selected community from the Community View page.

Step 1 From the menu bar, choose **Application > Manage Community**. The Manage Community dialog box opens.

Step 2 From the Manage Community dialog box, choose the community in which to add the device and click **OK**. The Community View page opens. See Community View Page, page 2-19.

Step 3 Click **Manage Devices**. The Manage Devices dialog box opens. See Manage Devices Dialog Box, page 2-22.

Step 4 In the Manage Devices dialog box, enter the IP address or hostname; and the username and password information for the device.

If you enter the default username **cisco** and default password **cisco**, the Change Default Credentials dialog box opens. For security reasons, you must change the default credentials to new credentials. See Change Default Credential Dialog Box, page 2-18.

Step 5 If you want Cisco CP to connect securely with the device, check the **Connect Securely** check box.

When you check the **Connect Securely** check box, HTTPS port 443 and SSH port 22 information is automatically added for the device. To view the port information, click the down-arrow next to the Connect Securely check box.

If you did not check the Connect Securely check box, the HTTP port 80 and Telnet port 23 information is automatically added to the device. To view the port information, click the down-arrow next to the Connect Securely check box.

Step 6 If you want to change the default port information, click it and enter a new port value.

Note Make sure that Cisco CP can access the device at the specified secure or non-secure ports.

Step 7 Click **OK**. The Community View page appears and includes the new device that you added. See Community View Page, page 2-19.

Related Topics

- Understanding Device Communities, page 2-2
- Managing the Devices in a Community, page 2-8
- Editing Device Information, page 2-10
- Deleting a Device from a Community, page 2-11

Editing Device Information

Before You Begin

Make sure that you have created a community and added devices to it. See Creating a Community and Adding Devices, page 2-3 and Adding a Device to a Community, page 2-8.

Procedure

Use this procedure to edit the information of a selected device.

Step 1 From the menu bar, choose **Application > Manage Community**. The Manage Community dialog box opens.

Step 2 From the Manage Community dialog box, choose the community in which the device whose information to change resides and click **OK**. The Community View page opens. See Community View Page, page 2-19.

Step 3 To edit the information of a particular device, select it and click **Manage Devices**. The Manage Devices dialog box opens. See Manage Devices Dialog Box, page 2-22.

Step 4 In the Manage Devices dialog box, modify the information.

Step 5 Click **OK**.

Related Topics

- Understanding Device Communities, page 2-2
- Managing the Devices in a Community, page 2-8
- Adding a Device to a Community, page 2-8
- Deleting a Device from a Community, page 2-11

Deleting a Device from a Community

Before You Begin

Make sure that you have created a community and added devices to it. See Creating a Community and Adding Devices, page 2-3 and Adding a Device to a Community, page 2-8.

Procedure

Use this procedure to delete a device from a community.

Step 1 From the menu bar, choose **Application > Manage Community**. The Manage Community dialog box opens.

Step 2 From the Manage Community dialog box, choose the community in which the device to delete resides and click **OK**. The Community View page opens. See Community View Page, page 2-19.

Step 3 To delete a particular device, select it and click **Delete**. A confirmation dialog box opens.

Step 4 Click **Yes** in the confirmation dialog box to delete the device.

Related Topics

- Understanding Device Communities, page 2-2
- Managing the Devices in a Community, page 2-8
- Adding a Device to a Community, page 2-8
- Editing Device Information, page 2-10

Discovering Devices

In order to configure a device, you must choose the community the device belongs to, choose the device and discover it. Cisco CP uses the IP address or hostname, and the credential information that you specified to discover the device.

You can discover the devices in a community from the Manage Community dialog box or the Manage Devices dialog box; or you can discover the devices from the Community View page.

To discover all the devices from the Manage Community dialog box or the Manage Devices dialog box, click the **Discover All Devices** check box. All of the devices in the displayed community are discovered. See Manage Community Dialog Box, page 2-15 and Manage Devices Dialog Box, page 2-22.

To discover specific or all of the devices in a community from the Community View page, use the procedure in this section.

Before You Begin

Make sure that you have created a community and added devices to it.

Procedure

Use this procedure to discover devices in a community from the Community View page.

Step 1 From the menu bar, choose **Application > Manage Community**. The Manage Community dialog box opens.

Step 2 From the Manage Community dialog box, choose the community name in which the device to discover resides and click **OK**. The Community View page opens. See Community View Page, page 2-19.

Step 3 Do one of the following:

- To discover a particular device, select the row and click **Discover**. A confirmation dialog box opens informing that the discovery process can take up to three minutes.
- To discover all the devices, press the shift button on your keyboard and select multiple rows. Click **Discover**. A confirmation dialog box opens informing that the discovery process can take up to three minutes.

Step 4 Click **Yes** in the confirmation dialog box to continue with the discovery.

After the discovery is complete, the discovery status information is displayed in the Discover Status column. You will see one of the following:

- Discovered—The device has been discovered and is available.
- Discovering—Cisco CP is in the process of discovering the device.
- Discovery failed—Cisco CP could not discover the device. See Understanding Discovery Failed Error Messages, page 2-31 to determine the problem and fix it.
- Discovery scheduled—Cisco CP has queued the discovery of the device.
- Discovered with errors—The device has been discovered, but errors were generated during the discovery process. See Things to Know About Discovering Devices, page 2-28. Use the procedure in Collecting Cisco CP Technical Support Logs, page 2-38 to collect technical support information and send it to Cisco for analysis.
- Discovered with warnings—The device has been discovered, but some information about the device was not available. To see what warnings are given, select the row for the device and click **Discovery Details**.
- Not Discovered—No attempt has been made to discover the device.

Step 5 To view details about the discovery process, click **Discovery Details**. See Discovery Details Dialog Box, page 2-24.

Related Topics

- Things to Know About Discovering Devices, page 2-28
- Discovery Details Dialog Box, page 2-24

Displaying Discovery Process Details

Before You Begin

Make sure that the device whose discovery details you want to view has gone through the discovery process. See Discovering Devices, page 2-12.

Procedure

Use this procedure to display the discovery process information about a device.

Step 1 From the Community View page, choose the device for which to view discovery process information.

Step 2 Click **Discovery Details**. The Discovery Details dialog box opens. See Discovery Details Dialog Box, page 2-24.

Step 3 View the discovery details and click **Close** to close the dialog box.

Related Topics

- Discovering Devices, page 2-12
- Community View Page, page 2-19

Displaying Information About a Discovered Device

Before You Begin

Make sure the device whose information to view is discovered. See Discovering Devices, page 2-12.

Procedure

Use this procedure to display the hardware and software information and the features that are available on a discovered device.

Step 1 From the Community View page, choose the discovered device for which to view information.

Step 2 Click **Router Status**. The Router Status dialog box opens. See Router Status Dialog Box, page 2-26.

Step 3 View the router status information and click **Close** to close the dialog box.

Related Topics

- Discovering Devices, page 2-12
- Community View Page, page 2-19

Device Community Reference

The following topics describe the Device Community pages and dialog boxes used to configure device communities:

- Manage Community Dialog Box, page 2-15
- Change Default Credential Dialog Box, page 2-18
- Community View Page, page 2-19
- Manage Devices Dialog Box, page 2-22
- Discovery Details Dialog Box, page 2-24
- Router Status Dialog Box, page 2-26
- Supplementary Information, page 2-28

Manage Community Dialog Box

Use the Manage Community dialog box to create a community, add devices to it, and discover all of the devices in a community.

How to Get to This Dialog Box

From the menu bar, choose **Application > Manage Community**.

Related Topics

- Understanding Device Communities, page 2-2
- Creating a Community and Adding Devices, page 2-3
- Adding a Device to a Community, page 2-8

- Editing Device Information, page 2-10
- Deleting a Device from a Community, page 2-11
- Change Default Credential Dialog Box, page 2-18
- Community View Page, page 2-19

Field Reference

Table 2-1 Manage Community Dialog Box

Element	Description
	Add icon. Click this icon to add a new community. See Adding Communities, page 2-4.
	Delete icon. Click this icon to delete a selected community. See Deleting a Community, page 2-5.
	Edit icon. Click this icon to edit the name of a selected community. See Changing the Community Name, page 2-5.
	Export icon. Click this icon to save the community information from Cisco CP to a file on your PC. See Exporting and Importing Communities, page 2-6.
	Import icon. Click this icon to import the community information from a file on your PC into Cisco CP. After the file is imported, Cisco CP displays the community with all its community members (devices) in the Manage Community dialog box. See Exporting and Importing Communities, page 2-6.
IP Address/Hostname	The IP address or hostname of the device.

Table 2-1 Manage Community Dialog Box (continued)

Element	Description
Username	The username used to log into the device. If you enter the default username **cisco** and default password **cisco**, the Change Default Credentials dialog box opens. For security reasons, you must change the default credentials to new credentials. See Change Default Credential Dialog Box, page 2-18. Cisco CP uses the new credentials that you provide to create an administrative user with a privilege level of 15. If the credentials that you enter were already configured, Cisco CP overwrites them, and gives them a privilege level of 15 when it discovers the device. To prevent an existing user account from being overwritten for any reason, do not use its credentials to replace the default credentials.
Password	Enter the password associated with the username that you entered.
Connect Securely check box	Click this check box if you want Cisco CP to connect securely with the device. When you check the **Connect Securely** check box, HTTPS port 443 and SSH port 22 information is automatically added to the device. If you did not check the Connect Securely check box, the HTTP port 80 and Telnet port 23 information is automatically added to the device.

Table 2-1 Manage Community Dialog Box (continued)

Element	Description
Down arrow	Click the down-arrow to view the port information that Cisco CP uses to connect to the device: • HTTP—80 • Telnet—23 • HTTPS—443 • SSH—22 You can change the default port information. Click it and then enter a new port value. **Note** Make sure that Cisco CP can access the device at the specified secure or non-secure ports.
Discover All Devices check box	Click this check box to discover all the devices in the displayed community.
OK button	Click this button to save the changes and add the community and device information to Cisco CP. When you click this button, the Community View page opens where you can view the community information. See Community View Page, page 2-19.
Cancel button	Click this button to cancel the changes.

Change Default Credential Dialog Box

The Change Default Credential dialog box appears when you add the default username **cisco** and default password **cisco** for a device. For security reasons, you must change the default credentials to new credentials. Use the Change Default Credential dialog box to change the default credentials.

How to Get to This Dialog Box

Enter the default username **cisco** and default password **cisco** in the Manage Community or Manage Devices dialog boxes.

Related Topics

- Creating a Community and Adding Devices, page 2-3
- Adding a Device to a Community, page 2-8
- Manage Community Dialog Box, page 2-15
- Manage Devices Dialog Box, page 2-22

Field Reference

Table 2-2 Change Default Credential Dialog Box

Element	Description
New Username	The username used to log into the device.
New Password	The password associated with the username that you entered.
Confirm Password	The password that you entered in the New Password field.
OK button	Click this button to add the credential information to Cisco CP.

Community View Page

The Community View page summarizes the community information and allows you to add, edit, discover devices, and to view the discovery and router status of each device.

How to Get to This Page

From the menu bar, choose **Application > Manage Community >** *Community Name* **> OK**.

Related Links

- Managing the Devices in a Community
- Manage Devices Dialog Box
- Discovery Details Dialog Box
- Router Status Dialog Box

Field Reference

Table 2-3 Community View Page

Element	Description
Search feature—Left Pane	
	Search icon. Click the Search icon to search for supported features in Cisco CP. **a.** Type the first letter of the word in the Search text-box. A list of keywords beginning with that letter is displayed. **b.** Choose the desired keyword and click the Search button. The search results display the available features that match the keyword. **c.** Click the feature name. The feature is launched in the right pane. **d.** Click the Search icon to exit search. **Note** Only features supported on the device are displayed in the search results. **Note** The Search option is available when devices are in discovered state.
Cisco Configuration Professional News—Upper Pane	
Date	Date the Cisco CP news was published.
Title	Links to important information about Cisco CP. The updated information is provided through RSS feeds. **Note** To view the Cisco CP news, you must have access to the Internet.
Community Information—Lower Pane (Displays the name of the community and summarizes the information about all the devices in the community.)	
Filter	To display only entries that contain specified text, enter the text in the Filter box. The display is updated each time you enter a character.
IP Address/Hostname	The IP address or hostname of the community member.
Router Hostname	The hostname associated with the IP address.

Table 2-3 Community View Page (continued)

Element	Description
Connection Type	Displays one of the following: • Non secure—The device has not been discovered, or has been discovered without using a secure protocol. • Secure—The device has been discovered, using a secure protocol. To ensure that the device is discovered using a secure protocol, check the Connect Securely check box in the Manage Community dialog box or the Manage Devices dialog box.
Discovery Status	This column contains one of the following values: • Discovered—The device has been discovered and is available. • Discovering—Cisco CP is in the process of discovering the device. • Discovery failed—Cisco CP could not discover the device. See Understanding Discovery Failed Error Messages, page 2-31 to determine the problem and fix it. • Discovery scheduled—Cisco CP has queued the discovery of the device. • Discovered with errors—The device has been discovered, but errors were generated during the discovery process. See Things to Know About Discovering Devices, page 2-28. Use the procedure in Collecting Cisco CP Technical Support Logs, page 2-38 to collect technical support information and send it to Cisco for analysis. • Discovered with warnings—The device has been discovered, but some information about the device was not available. To see what warnings are given, select the row for the device and click **Discovery Details**. • Not Discovered—No attempt has been made to discover the device.
Buttons	
Manage Devices	Click the **Manage Devices** button to open the Manage Devices dialog box were you can add new devices or edit information of a specific device.

Table 2-3 Community View Page (continued)

Element	Description
Delete	To remove a member from the community, choose the community member entry and click **Delete**.
Discover	To discover one or more community members, select the entry for each member that you want to discover and click **Discover**.
Discovery Details	To display details about the discovery of the device, select the entry for the member and click **Discovery Details**.
Cancel Discovery	To cancel the discovery of a device, select the row of the device being discovered and click **Cancel Discovery**.
Router Status	To display hardware, software, and feature details about a community member, select the entry for the member and click **Router Status**.

Manage Devices Dialog Box

Use the Manage Devices dialog box to add a new device (community member) or to edit information about an existing device.

How to Get to This Dialog Box

1. From the menu bar, choose **Application > Manage Community >** *Community Name* **> OK**. The Community View page opens.
2. From the Community View page, click **Manage Devices**.

Related Links

- Managing the Devices in a Community, page 2-8
- Adding a Device to a Community, page 2-8
- Editing Device Information, page 2-10

Field Reference

Table 2-4 Manage Devices Dialog Box

Element	Description
IP Address/Hostname	The IP address or hostname of the device.
Username	The username used to log into the device. If you enter the default username **cisco** and default password **cisco**, the Change Default Credentials dialog box opens. For security reasons, you must change the default credentials to new credentials. See Change Default Credential Dialog Box, page 2-18. Cisco CP uses the new credentials that you provide to create an administrative user with a privilege level of 15. If the credentials that you enter were already configured, Cisco CP overwrites them, and gives them a privilege level of 15 when it discovers the device. If you do not want an existing user account overwritten for any reason, do not use its credentials to replace the default credentials.
Password	Enter the password associated with the username that you entered.
Connect Securely check box	Click this check box if you want Cisco CP to connect securely with the device. When you check the **Connect Securely** check box, HTTPS port 443 and SSH port 22 information is automatically added to the device. If you did not check the Connect Securely check box, the HTTP port 80 and Telnet port 23 information is automatically added to the device.

Table 2-4 Manage Devices Dialog Box (continued)

Element	Description
Down arrow	Click the down-arrow to view the port information that Cisco CP uses to connect to the device: • HTTP—80 • Telnet—23 • HTTPS—443 • SSH—22 You can change the default port information. Click it and enter a new port value. **Note** Make sure that Cisco CP can access the device at the specified secure or non-secure ports.
Discover All Devices check box	Click this check box to discover all of the devices in the displayed community.
OK button	Click this button to save the changes and add the community and device information to Cisco CP. When you click this button, the Community View page opens where you can view the community information. See Community View Page, page 2-19.
Cancel button	Click this button to discard the changes that you made.

Discovery Details Dialog Box

When device discovery succeeds, the Discovery Details dialog box displays performance information about the discovery process. When discovery is not successful, this page reports the reason for the failure.

How to Get to This Dialog Box

1. From the menu bar, choose **Application > Manage Community >** *Community Name* **> OK**. The Community View page opens.
2. From the Community View page, select a discovered device and click **Discovery Details**.

Related Links

- Managing the Devices in a Community, page 2-8
- Discovering Devices, page 2-12
- Displaying Information About a Discovered Device, page 2-14
- Things to Know About Discovering Devices, page 2-28

Field Reference

Table 2-5 Discovery Details Dialog Box

Element	Description
i icon (information icon)	When discovery succeeds, Cisco CP displays performance data on the discovery and information on the software features discovered. You might see some of the following messages: • Hardware Discovery—The method used to discover the devices are displayed. The methods are: – Telnet—The method used if you did not choose the Secure login option when discovering the device. – SSH—The method used if you chose the Secure option when discovering the device. • Hardware discovery total elapsed time—The amount of time that elapsed before the device hardware features, such as interfaces and network modules, were discovered. Time is shown in milliseconds. • All features total discovery elapsed time—The amount of time that elapsed before all Cisco CP features were ready for use. Time is shown in milliseconds. • Total discovery elapsed time—The total amount of time that elapsed before all hardware and software features were discovered. Time is shown in milliseconds. • Summary—If all hardware and software features have been successfully discovered, the text “Successful discovery of all features” is displayed.

Table 2-5 Discovery Details Dialog Box (continued)

Element	Description
Red X icon (discovery failed icon)	When discovery fails, Cisco CP reports the reason for the failure. See the Understanding Discovery Failed Error Messages, page 2-31.
Warning icon	The device is discovered, but some information about the device is not available. For example, when an interface is disabled, Cisco CP displays warnings, such as the following: • <*Interface*> Administratively Disabled—The interface is administratively disabled. Enable the interface and rediscover the device to continue.

Router Status Dialog Box

Use the Router Status dialog box to view hardware and software information and the features that are available on a discovered device.

How to Get to This Dialog Box

1. From the menu bar, choose **Application > Manage Community >** *Community Name* **> OK**. The Community View page opens.
2. From the Community View page, choose the discovered device to view information for and click **Router Status**.

Related Topics

- Managing the Devices in a Community, page 2-8
- Displaying Information About a Discovered Device, page 2-14

Field Reference

Table 2-6 Router Status Dialog Box

Element	Description
Hardware Details	
Model Type	The device model type, for example Cisco 3825.
Available / Total Memory	The number of available megabytes in memory and the total number of megabytes in memory, for example 109/256 MB.
Total Flash Capacity	The flash memory capacity, in megabytes, for example, 61 MB.
Software Details	
IOS Version	The Cisco IOS version, for example, 12.4(11)T.
IOS Image	The Cisco IOS image name, for example, c3825-adventerprisek9-mz.124-11.T.
Hostname	The hostname, if one has been configured. An example hostname is c3825-1.
Feature Availability	
IP	If the IP routing feature is available, Cisco CP displays a green icon. If the IP routing feature is not available, Cisco CP displays a red icon.
Firewall	If the Firewall feature is available, Cisco CP displays a green icon. If the Firewall feature is not available, Cisco CP displays a red icon.
VPN	If the VPN[1] feature is available, Cisco CP displays a green icon. If the VPN feature is not available, Cisco CP displays a red icon.
IPS	If the IPS[2] feature is available, Cisco CP displays a green icon. If the IPS feature is not available, Cisco CP displays a red icon.
NAC	If the NAC[3] feature is available, Cisco CP displays a green icon. If the NAC feature is not available, Cisco CP displays a red icon.

1. VPN = Virtual Private Network.
2. IPS = Intrusion Prevention System.
3. NAC = Network Access Control.

Supplementary Information

This section contains information that may help you use Cisco CP. It contains the following sections:

- Things to Know About Discovering Devices, page 2-28
- Collecting Cisco CP Technical Support Logs, page 2-38

Things to Know About Discovering Devices

This section gives you information to refer to if you are unable to discover a device. It contains the following sections:

- Cisco CP Configuration Requirements, page 2-28
- Wrong Secure Shell Version May Cause Discovery to Fail, page 2-30
- Understanding Discovery Failed Error Messages, page 2-31
- Cisco CP May Overwrite Existing Credentials, page 2-36
- Proxy Server Settings Might Cause Discovery to Fail, page 2-37
- Setting the Java Heap Size Value to -Xmx256m, page 2-37

Cisco CP Configuration Requirements

Proper router configuration is required for discovery to succeed. Check the following configuration items for problems:

- Supported device—The device you are attempting to discover must be a device that Cisco CP supports. See the *Release Notes for Cisco Configuration Professional* for a list of supported devices.
- Correct username and password—You must use a username and password configured on the device.
- Correct privilege level—The privilege level for the user account entered in the Add Community Member or Edit Community Member screen must be level 15.

- Cisco CP View—Cisco CP allows you to associate user accounts with CLI views, which restrict the associated user to specified actions within Cisco CP. If a user with a CLI view configured using Cisco Router and Security Device Manager (SDM) attempts to discover a device, discovery fails. To remove an SDM CLI view from a user account and replace it with a Cisco CP CLI view, click **Router > Router Access > User Accounts/View**. Next, choose the user account to update and click **Edit**. In the displayed dialog box, choose a Cisco CP CLI view.
- Minimum Java Runtime Environment (JRE) version—The minimum JRE version is 1.5.0_11.
- Correct Java heap size value—The correct Java heap size value is -Xmx256m. See "Setting the Java Heap Size Value to -Xmx256m" to learn how to set the Java heap size value.
- vty lines—A vty line must be available for each session Cisco CP establishes with the device. At least one vty line must be available for Cisco CP to connect to the device. If you use Cisco CP to launch additional applications on the device, a vty line must be available for each additional session. If a Cisco Unity Express Advanced Integration Module (AIM) is present on the device, two vty lines must be available to connect to the AIM.
- Transport input for vty lines—The vty transport input must be set to ssh for secure connections and to telnet for nonsecure connections.
- Security settings—The following security settings must be in place:
  - ip http server—for nonsecure access
  - ip http secure-server—for secure access
  - ip http authentication local
- Protocol and encryption settings—Verify that other settings, such as a firewall, Network Access Control, and other features designed to limit access to the network are not preventing discovery.

Cisco CP configuration requirements are provided in the *Release Notes for Cisco Configuration Professional*. Additionally, the default configuration file shipped on routers ordered with Cisco CP provides a basic configuration that allows discovery to succeed.

Wrong Secure Shell Version May Cause Discovery to Fail

If the device that you are trying to discover is not using Secure Shell (SSH) version 2.0 or higher, discovery may fail, and you must update the version in order to eliminate this problem. To determine which SSH version the device is using and, if necessary, update the version and regenerate an RSA key, complete these steps:

Step 1 Determine which SSH version the device is using by entering the **show ip ssh** EXEC mode command. An example command entry and output follows:

```
c3845-1(config)# show ip ssh
SSH Enabled - version 1.5
Authentication timeout: 120 secs; Authentication retries: 3
c3845-1(config)#
```

Note If the version shown is 1.99, there is no need to update the SSH version to 2.0.

Step 2 To update SSH to version 2, enter the Exec mode **ip ssh version 2** command, as shown in the following example:

```
c3845-1(config)# ip ssh version 2
```

Step 3 To generate a new RSA key, enter the Global configuration mode **crypto key generate rsa** command, as shown in the following example:

```
c3845-1(config)# crypto key generate rsa
The name for the keys will be name.domain.com
Choose the size of the key modulus in the range of 360 to 2048 for
your General Purpose Keys. Choosing a key modulus greater than 512 may
take a few minutes.

How many bits in the modulus [512]: 768
% Generating 768 bit RSA keys, keys will be non-exportable...[OK]
c3845-1(config)# end
c3845-1# wr
```

When you complete this procedure, the configuration change is made to the running configuration and stored in the startup configuration, and the SSH version is eliminated as a reason for discovery not succeeding.

Understanding Discovery Failed Error Messages

Table 2-7 provides the discovery failed error messages and the conditions under which you might see them.

Table 2-7 Discovery Failed Error Messages

Error Message	Condition

`The username or password is incorrect.`	This error message is displayed in one of the following conditions:
	• The username is wrong.
	• The password is wrong.
	• The CLI **ip http authentication local** is missing in the configuration.
	To configure local authentication for http server users, enter the following commands on the device:
	`Router> config terminal`
	`Router(config)# ip http authentication local`

Table 2-7 Discovery Failed Error Messages (continued)

Error Message	Condition

`Discovery could not be completed because the security certificate was rejected.`	This error message is displayed when:
	• Cisco CP connects to the device securely, but because you did not accept the security certificate, Cisco CP is unable to start discovery.
	• You are not prompted to accept the security certificate at all. In this case, perform the following steps:
	1. Clear the crypto keys using the command:
	`Router (config)# crypto key zeroize`
	2. Delete the trustpoint using the CLI. For example:
	`Router(config)# no crypto pki trustpoint TP-self-signed-3248306557`
	`% Removing an enrolled trustpoint will destroy all certificates received from the related Certificate Authority.`
	`Are you sure you want to do this? [yes/no]: yes`
	`% Be sure to ask the CA administrator to revoke your certificates.`
	`Router(config)#`
	3. Access the router through a browser using the URL: https://<ip address of the router>
	4. Click option 2:
	Continue to this website (not recommended).
	5. Launch Cisco CP and discover the device in Secure mode.
	The security certificate has to be accepted within the HTTP idle timeout specified. The default value for the idle timeout is 180 seconds. For example, If the idle timeout is set to 30 seconds, you have to accept the certificate within that time. The idle timeout on the router is configured as:
	`Router(config)# ip http timeout-policy idle 30`

Table 2-7 Discovery Failed Error Messages (continued)

Error Message	Condition
	If you accept the certificate after the configured time, discovery fails. However, rediscovery is successful. • The router does not have SSH configured. To configure SSH: `Router (config)# crypto key generate rsa modulus 1024`

`Connection to the device could not be established. Either the device is not reachable or the HTTP service is not enabled on the device.`	This error message is displayed in one of the following conditions:
	• The internet connection is down.
	• The IP address of the device is wrong or the device is not reachable.
	• The CLI **ip route** <*x.x.x.x*> <*x.x.x.x*> <*x.x.x.x*> is missing in the configuration.
	• The wrong HTTP port is provided to Cisco CP to connect to the device.
	• The CLI **ip http server** is missing in the configuration for non-secure connection.
	• The CLI **ip http secure-server** is missing in the configuration for secure connection.
	To configure the device as an HTTP or HTTPS server, enter the following commands:
	`Router> config terminal`
	`Router(config)# ip http server`
	`Router(config)# ip http secure-server`

Table 2-7 Discovery Failed Error Messages (continued)

Error Message	Condition

`Connection to the device could not be established. Telnet service might not be configured properly on the device.`	This error message is displayed in one of the following conditions:
	• The wrong Telnet port is provided to Cisco CP to connect to the device.
	• The CLI **login local** under vty lines is missing in the configuration.
	• The CLI **transport input telnet** under vty lines is missing in the configuration.
	To configure VTY lines on the device, enter the following commands:
	`Router> config terminal`
	`Router(config)# line vty 0 4`
	`Router(config-line)# login local`
	`Router(config-line)# transport input telnet`
	`Router(config-line)# exit`

`The hardware platform <platform name> is not supported.`	This error message is displayed if the device is not supported by Cisco CP. See *Release Notes for Cisco Configuration Professional* for a list of supported devices.

Cisco CP May Overwrite Existing Credentials

If you enter the default username cisco and password cisco when adding a device to the community, Cisco CP informs you that you must create new credentials to avoid causing a security problem. Cisco CP uses the new credentials that you provide to create an administrative user with a privilege level of 15. If the credentials that you enter are already configured, Cisco CP overwrites them, and gives them a privilege level of 15 when it discovers the device. If you do not want an existing user account overwritten or to have the cisco/cisco default credentials overwritten, enter different credentials for Cisco CP to use to log on.

Proxy Server Settings Might Cause Discovery to Fail

If you are using a proxy server for your Internet Explorer to connect to the Internet, make sure that the Internet Explorer is configured to bypass the proxy server for local addresses as well as the addresses of the devices that will be discovered by Cisco CP. Otherwise, device discovery will fail.

To resolve this issue, do the following in Internet Explorer 6.0:

Step 1 Choose **Tools > Internet Options … > Connections > LAN Settings** button. The Local Area Network (LAN) Settings dialog box opens.

Step 2 Check to see if the **Use the Proxy Server for Your LAN** check box is selected. If the Use the Proxy Server for Your LAN check box is selected, select the **Bypass Proxy Server for Local Addresses** check box also.

Step 3 Click the **Advanced…** button. The Proxy Settings dialog box opens.

Step 4 In the Exceptions pane, enter the addresses of all of the devices for which you do not want Internet Explorer to use the proxy server.

Step 5 Click **OK** in the Proxy Settings dialog box.

Step 6 Click **OK** in the Local Area Network (LAN) Settings dialog box.

Setting the Java Heap Size Value to -Xmx256m

Complete the following steps to set the Java heap size to the value -Xmx256m:

Step 1 Exit Cisco CP.

Step 2 Click **Start > Control Panel > Java**.

Step 3 Open the Java Runtime Settings dialog box. The location of this dialog box varies by release.

- **a.** Click the **Advanced** tab. Locate the Java Runtime Settings dialog box and proceed to Step 4. If the dialog box is not available from the Advanced tab, proceed to Step b.
- **b.** Click the **Java** tab. Locate the Java Runtime Settings dialog box. Click the **View** button to display the dialog box and proceed to Step 4.

Step 4 In the Java Runtime Parameters column, enter the value stated in the window. For example, if the window states that you must use the value `-Xmx256m`, enter that value in the Java Runtime Parameters column. The following table shows sample values.

Product Name	Version	Location	Java Runtime Parameters
JRE	1.5.0_11	C:\Program Files\java\jre1.5.0_11	-Xmx256m

Step 5 Click **OK** in the Java Runtime Settings dialog.

Step 6 Click **Apply** in the Java Control Panel and click **OK**.

Step 7 Restart Cisco CP.

Collecting Cisco CP Technical Support Logs

Cisco CP automates the collection of the technical support logs that it generates. Cisco CP need not be running when the technical support logs are collected. If you need to send Cisco CP technical support logs to Cisco, complete the following steps:

Step 1 Click **Start > Programs > Cisco Systems > Cisco Configuration Professional > Collect Data for Tech Support**. Cisco CP automatically archives the logs in a zip file named _ccptech.zip. Cisco CP saves that zip file in a folder that it places on the PC desktop. The folder is named using the convention **`CiscoCP Data for Tech Support YYY-MM-DD_hh-mm-sec`**. An example folder name is CiscoCP Data for Tech Support 2008-06-28_18-03-13.

Step 2 Send the folder along with a description of the problem to the Cisco Technical Assistance Center (TAC).

PART 2

Managing Interfaces

This section provides information about how to manage interfaces.

CHAPTER 3

Creating a New Connection

The Cisco CP connection wizards guide you LAN and WAN configurations, and check the information that you enter against the existing configuration, warning you of any problems.

This chapter contains the following sections:

- Creating a New Connection
- New Connection Reference
- Additional Procedures

Creating a New Connection

Complete these steps to create a new connection:

Step 1 Click **Configure > Interface Management > Interface and Connections.**

Step 2 In the Create New Connection box, choose the type of connection that you want to configure. Information about the type of connection you choose is displayed in the Information box, and the Use Case Scenario area displays a graphic showing the kind of connection that you chose.

Step 3 Click the **Create New Connection** button to get started. If you chose the Wireless connection option, click the **Launch Wireless Application** button to start the wireless application.

New Connection Reference

The following topic describes the screen referred to in this chapter:

- Create Connection

Create Connection

This window allows you to create new LAN and WAN connections.

Note You cannot use Cisco CP to create WAN connections for Cisco 7000 series routers.

Field Reference

Table 3-1 describes the fields in this screen.

Table 3-1 Create Connection Fields

Element	Description
Create New Connection	Choose a connection type to configure on the physical interfaces available on your router. Only interfaces that have not been configured are available. If all interfaces have been configured, this area of the window is not displayed.
	If the router has Asynchronous Transfer Mode (ATM) or serial interfaces, multiple connections can be configured from a single interface because Cisco Configuration Professional II (Cisco CP) configures subinterfaces for each interface of that type. The Other (Unsupported by Cisco CP) radio button appears if an unsupported logical or physical interface exists, or if a supported interface exists that has been given an unsupported configuration. When you click the Other (Unsupported by Cisco CP) radio button, the Create New Connection button is disabled. If the router has radio interfaces but you do not see a **Wireless** radio button, you are not logged on as an Cisco CP Administrator.

Table 3-1 Create Connection Fields

Element	Description
Use Case Scenario	When you click the radio button for a connection type, a network diagram appears illustrating that type of connection.
Information	The information area displays more information about the connection type you choose. For example, if you choose Ethernet LAN, the information area may display the text "Configure Ethernet LAN interface for straight routing and 802.1q trunking."
Create New Connection button	Click the **Create New Connection** button to start the wizard for the type of connection you chose.
Launch Wireless Application button	**Note** The Launch Wireless Application button appears when you choose the Wireless connection option. Click the **Launch Wireless Application** button to start the wireless application. You must provide your username and password credentials to start it.

Additional Procedures

This section contains procedures for tasks that the wizard does not help you complete.

This section contains the following topics:

- How Do I Configure a Static Route?
- How Do I View Activity on My LAN Interface?
- How Do I Enable or Disable an Interface?
- How Do I View the IOS Commands I Am Sending to the Router?
- How Do I Configure an Unsupported WAN Interface?
- How Do I Enable or Disable an Interface?
- How Do I View Activity on My WAN Interface?
- How Do I Configure NAT on a WAN Interface?
- How Do I Configure a Static Route?
- How Do I Configure a Dynamic Routing Protocol?

- How Do I Configure Dial-on-Demand Routing for My ISDN or Asynchronous Interface?

How Do I Configure a Static Route?

To configure a static route:

Step 1 Click **Configure > Router > Static and Dynamic Routing**.

Step 2 In the Static Routing group, click **Add...**.

The Add IP Static Route dialog box appears.

Step 3 In the Prefix field, enter the IP address of the static route destination network.

Step 4 In the Prefix Mask field, enter the subnet mask of the destination network.

Step 5 If you want this static route to be the default route, check the **Make this as the Default Route** check box.

Step 6 In the Forwarding group, select whether to identify a router interface or the destination router IP address as the method to forward data, and then choose either the forwarding router interface or enter the destination router IP address.

Step 7 Optionally, in the Distance Metric field, enter the distance metric to be stored in the routing table.

Step 8 If you want to configure this static route to be a permanent route, which means that it will not be deleted even if the interface is shut down or the router is unable to communicate with the next router, check the **Permanent Route** check box.

Step 9 Click **OK**.

How Do I View Activity on My LAN Interface?

You can view activity on a LAN interface by using the Monitor mode in Cisco CP. Monitor mode can display statistics about the LAN interface, including the number of packets and bytes that have been sent or received by the interface, and the number of send or receive errors that have occurred. To display statistics about about a LAN interface:

Step 1 Click **Monitor > Router > Interface Status**.

Step 2 In the Select an Interface field, select the LAN interface for which you want to view statistics.

Step 3 Select the data item(s) you want to view by checking the associated check box(es). You can view up to four statistics at a time.

Step 4 Click **Start Monitoring** to see statistics for all selected data items.

The Interface Details screen appears, displaying the statistics you selected. The screen defaults to showing real-time data, for which it polls the router every 10 seconds. If the interface is up and there is data transmitting across it, you should see an increase in the number of packets and bytes transferred across the interface.

How Do I Enable or Disable an Interface?

You can disable an interface without removing its configuration, and you can re-enable an interface that you have disabled.

Step 1 Click **Configure > Interface Management > Interface and Connections**.

Step 2 Click **Edit Interfaces and Connections**.

Step 3 Select the interface that you want to disable or enable.

Step 4 If the interface is enabled, the Disable button appears above the Interface List. Click that button to disable the interface. If the interface is currently disabled, the Enable button appears below the Interface List. Click that button to disable the interface.

How Do I View the IOS Commands I Am Sending to the Router?

When you click OK in a dialog box, or when you click Finish in a wizard summary screen, Cisco CP automatically shows you the Cisco IOS commands it will deliver to the router in the Deliver Configuration to Router screen.

To send the commands to the router, click **Deliver**.

To cancel command delivery, click **Cancel**. Cisco CP discards the changes and closes the dialog box or wizard.

How Do I Launch the Wireless Application from Cisco CP?

Use the following procedure to launch the wireless application from Cisco CP.

Step 1 From the Cisco CP Tools menu, select **Launch Wireless Application.** The Wireless Application launches in a separate browser window.

Step 2 In the left panel, click the title of the configuration screen that you want to work in. To obtain help for any screen, click the help icon in the upper right corner. This icon looks like an open book with a question mark.

How Do I Configure an Unsupported WAN Interface?

Cisco CP does not support configuration of every WAN interface that your router might support. If Cisco CP discovers an interface in your router that it does not support, or a supported interface with an unsupported configuration, Cisco CP displays a radio button labeled Other (Unsupported by Cisco CP). The unsupported interface is displayed in the Interfaces and Connections window, but it cannot be configured using Cisco CP.

To configure an unsupported interface, you must use the router command-line interface (CLI).

How Do I Enable or Disable an Interface?

You can disable an interface without removing its configuration, and you can re-enable an interface that you have disabled.

Step 1 Click **Configure > Interface Management > Interface and Connections**.

Step 2 Click the interface that you want to disable or enable.

Step 3 If the interface is enabled, the Disable button appears above the Interface List. Click it to disable the interface. If the interface is currently disabled, the Enable button appears in that location. Click that button to disable the interface.

How Do I View Activity on My WAN Interface?

You can view activity on a WAN interface by using the Monitor feature in Cisco CP. Monitor screens can display statistics about the WAN interface, including the number of packets and bytes that have been sent or received by the interface, and the number of send or receive errors that have occurred. To display statistics about a WAN interface:

Step 1 Click **Monitor > Router > Interface Status**.

Step 2 In the Select an Interface field, choose the WAN interface for which you want to view statistics.

Step 3 Choose the data item(s) you want to view by checking the associated check box(es). You can view up to four statistics at a time.

Step 4 Click **Show Details** to see statistics for all selected data items.

The Interface Details screen appears, displaying the statistics you selected. The screen defaults to showing real-time data, for which it polls the router every 10 seconds. If the interface is up and there is data transmitting across it, you should see an increase in the number of packets and bytes transferred across the interface.

How Do I Configure NAT on a WAN Interface?

Step 1 Click **Configure > Router > NAT**.

Step 2 In the NAT window, click **Designate NAT interfaces**.

Step 3 Find the interface for which you want to configure NAT.

Step 4 Check **inside (trusted)** next to the interface to designate the interface as an inside, or trusted interface. An inside designation is typically used to designate an interface serving a LAN whose resources. must be protected. Check **outside (untrusted)** to designate it as an outside interface. Outside interfaces typically connect to an untrusted network. Click **OK**.

The interface is added to the pool of interfaces using NAT.

Step 5 Review the Network Address Translation Rules in the NAT window. If you need to add, delete, or modify a rule, click the appropriate button on the NAT window to perform the configuration you need.

For more information, click the following links:

- Add or Edit Static Address Translation Rule: Inside to Outside
- Add or Edit Static Address Translation Rule: Outside to Inside
- Add or Edit Dynamic Address Translation Rule: Inside to Outside
- Add or Edit Dynamic Address Translation Rule: Outside to Inside

How Do I Configure NAT on an Unsupported Interface?

Cisco CP can configure Network Address Translation (NAT) on an interface type unsupported by Cisco CP. Before you can configure the firewall, you must first use the router CLI to configure the interface. The interface must have, at a minimum, an IP address configured, and it must be working. To verify that the connection is working, verify that the interface status is "Up."

After you have configured the unsupported interface using the CLI, you can configure NAT using Cisco CP. The unsupported interface will appear as "Other" on the router interface list.

How Do I Configure a Dynamic Routing Protocol?

To configure a dynamic routing protocol:

Step 1 Click **Configure > Router > Static and Dynamic Routing**.

Step 2 In the Dynamic Routing group, click the dynamic routing protocol that you want to configure.

Step 3 Click **Edit**.

The Dynamic Routing dialog box appears, displaying the tab for the dynamic routing protocol you selected.

Step 4 Using the fields in the Dynamic Routing dialog box, configure the dynamic routing protocol. If you need an explanation for any of the fields in the dialog box, click **Help**.

Step 5 When you have finished configuring the dynamic routing protocol, click **OK**.

How Do I Configure Dial-on-Demand Routing for My ISDN or Asynchronous Interface?

ISDN BRI and asynchronous connections are dial-up connections, meaning that in order to establish a connection, the router must dial a preconfigured phone number. Because the cost of these types of connections is usually determined by the amount of time that a connection was established, and in the case of an asynchronous connection, that a phone line will be tied up, it is often desirable to configure Dial-on-Demand Routing (DDR) for these connection types.

Cisco CP can help you configure DDR by:

- Letting you associate a rule (or ACL) with the connection, which causes the router to establish the connection only when it recognizes network traffic that you have identified as interesting with the associated rule.
- Setting idle timeouts, which cause the router to end a connection after a specified amount of time when there is no activity on the connection.
- Enabling multilink PPP, which causes an ISDN BRI connection to use only one of the two B channels unless a specified percentage of bandwidth is exceeded on the first B channel. This has the advantage of saving costs when network traffic is low and the second B channel is not needed, but letting you utilize the full bandwidth of your ISDN BRI connection when needed.

To configure DDR on an existing ISDN BRI or asynchronous connection:

Step 1 Click **Configure > Interface Management > Interface and Connections**.

Step 2 Click the ISDN or asynchronous interface on which you want to configure DDR.

Step 3 Click **Edit**.

The Connection tab appears.

Step 4 Click **Options**.

The Edit Dialer Option dialog box appears.

Step 5 If you want the router to establish the connection only when it recognizes specific IP traffic, click the **Filter traffic based on selected ACL** radio button, and either enter a rule (ACL) number that will identify which IP traffic should cause the router to dial out, or click the **...** button to browse the list of rules and choose the rule that you want to use to identify IP traffic from that list.

Step 6 If you want to configure the router to end the connection when the connection is idle, i.e., no traffic passes across it, for a specified amount of time, in the **Idle timeout** field, enter the number of seconds the connection can remain idle before the router ends the connection.

Step 7 If you are editing an ISDN connection, and you would like to use your second B channel only when the traffic on the first B channel exceeds a certain threshold, check the **Enable MultiLink PPP** check box, then in the **Load Threshold** field, enter a number between 1 and 255, where 255 equals 100% of bandwidth, that will determine the threshold on the first B channel. When traffic on that channel exceeds that threshold, it will cause the router to connect the second B channel. In addition, in the **Data direction** field, you can choose whether this threshold should apply to outbound or inbound traffic.

Step 8 Click **OK**.

How Do I Edit a Radio Interface Configuration?

You must use the Wireless Application to edit an existing radio interface configuration.

Step 1 Click **Configure > Interface Management > Interface and Connections**.

Step 2 Click **Edit Interface/Connection**.

Step 3 Choose the radio interface and click **Edit**. In the Connections tab, you can change the IP address or bridging information. If you want to change other wireless parameters, click **Launch Wireless** Application.

CHAPTER 4

LAN Wizard

The Cisco Configuration Professional (Cisco CP) LAN wizard guides you in the configuration of a LAN interface. The screen lists the LAN interfaces on the router. You can select any of the interfaces shown in the window, and click **Configure** to make the interface a LAN interface and configure it.

This window lists the router interfaces that were designated as inside interfaces in Startup configuration, and lists the Ethernet interfaces and switch ports that have not been configured as WAN interfaces. The list includes interfaces that have already been configured.

When you configure an interface as a LAN interface, Cisco CP inserts the description text $ETH-LAN$ in the configuration file so that it recognizes the interface as a LAN interface in the future.

You can return to this screen as often as necessary to configure additional LAN interfaces.

Field Reference

Table 4-1 IP Address and Subnet Mask

Element	Description
Interface	The name of the interface
Configure	To configure an interface you have selected, click **Configure**. If the interface has not been configured before, Cisco CP will take you through the LAN Wizard to help you configure it. If the interface has been given a configuration using Cisco CP, Cisco CP displays an Edit window enabling you to change configuration settings. The Configure button may be disabled if a LAN interface has been given a configuration that Cisco CP does not support. For a list of such configurations, see Reasons Why an Ethernet Interface Configuration May Be Read-Only.

Ethernet Configuration

The wizard guides you through the configuration of an Ethernet interface on the LAN. You must provide the following information:

- An IP address and subnet mask for the Ethernet interface
- A DHCP address pool if you decide to use DHCP on this interface
- The addresses of DNS and WINS servers on the WAN
- A domain name

LAN Wizard: Select an Interface

Select the interface on which you want to configure a LAN connection in this window. This window lists interfaces that can support Ethernet LAN configurations.

LAN Wizard: IP Address and Subnet Mask

This window lets you configure an IP address and subnet mask for the Ethernet interface that you chose in the first window.

Field Reference

Table 4-2 IP Address and Subnet Mask

Element	Description
IP Address	Enter the IP address for the interface in dotted decimal format. Your network administrator should determine the IP addresses of LAN interfaces. For more information, see IP Addresses and Subnet Masks.
Subnet Mask	Enter the subnet mask. Obtain this value from your network administrator. The subnet mask enables the router to determine how much of the IP address is used to define the network and host portions of the address. Alternatively, select the number of network bits. This value is used to calculate the subnet mask. Your network administrator can tell you the number of network bits to enter.

LAN Wizard: Enable DHCP Server

This screen lets you enable a DHCP server on your router. A DHCP server automatically assigns reusable IP addresses to the devices on the LAN. When a device becomes active on the network, the DHCP server grants it an IP address. When the device leaves the network, the IP address is returned to the pool for use by another device.

Field Reference

Table 4-3 IP Address and Subnet Mask

Element	Description
Enable DHCP Server	To configure the router as a DHCP server on this interface, click **Yes**.

LAN Wizard: DHCP Address Pool

This screen lets you configure the DHCP IP address pool. The IP addresses that the DHCP server assigns are drawn from a common pool that you configure by specifying the starting IP address in the range, and the ending address in the range.

For more information, see DHCP Address Pools.

Note If there are discontinuous address pools configured on the router, then the Starting IP and Ending IP address fields will be read-only.

Field Reference

Table 4-4 DHCP Address Pool

Element	Description
Starting IP	Enter the beginning of the range of IP addresses for the DHCP server to use in assigning addresses to devices on the LAN. This is the lowest-numbered IP address in the range.
Ending IP	Enter the highest-numbered IP address in the range of IP addresses.
DNS Server and WINS Server Fields	If this window displays DNS Server and WINS Server fields, you can click DHCP Options for information on them.

DHCP Options

Use this window to configure DHCP options that will be sent to hosts on the LAN that are requesting IP addresses from the router. These are not options for the router that you are configuring; these are parameters that will be sent to the requesting hosts on the LAN. To set these properties for the router, click **Additional Tasks** on the Cisco CP category bar, click **DHCP**, and configure these settings in the DHCP Pools window.

Field Reference

Table 4-5 IP Address and Subnet Mask

Element	Description
DNS Server 1	The DNS server is typically a server that maps a known device name with its IP address. If you have DNS server configured for your network, enter the IP address for that device here.
DNS Server 2	If there is an additional DNS server on the network, you can enter the IP address for that server in this field.
Domain Name	The DHCP server that you are configuring on this router will provide services to other devices within this domain. Enter the name of the domain.
WINS Server 1	Some clients may require Windows Internet Naming Service (WINS) to connect to devices on the Internet. If there is a WINS server on the network, enter the IP address for the server in this field.
WINS Server 2	If there is an additional WINS server on the network, enter the IP address for the server in this field.

LAN Wizard: VLAN Mode

This screen lets you determine the type of VLAN information that will be carried over the switch port. Switch ports can be designated either to be in access mode, in which case they will forward only data that is destined for the VLAN to which they are assigned, or they can be designated to be in trunking mode, in which case they will forward data destined for all VLANs including the VLAN to which they are assigned.

If this switch port will be connected to a single device, such as a single PC or IP phone, or if this device will be connected to a port on a networking device, such as another switch, that is an access mode port, then select **Single Device**.

If this switch port will be connected to a port on a network device, such as another switch, that is a trunking mode, select **Network Device**.

Field Reference

Table 4-6 IP Address and Subnet Mask

Element	Description
Single Device	If this switch port will be connected to a single device, such as a single PC or IP phone, or if this device will be connected to a port on a networking device, such as another switch, that is an access mode port, then choose **Single Device**.
Network Device	If this switch port will be connected to a port on a network device, such as another switch, that is a trunking mode, choose **Network Device**.

LAN Wizard: Switch Port

This screen lets you assign an existing VLAN number to the switch port or to create a new VLAN interface to be assigned to the VLAN switch port.

Field Reference

Table 4-7 IP Address and Subnet Mask

Element	Description
Existing VLAN	If you want to assign the switch port to a VLAN that has already been defined, such as the default VLAN (VLAN 1), enter the VLAN ID number in the Network (VLAN) Identifier field.
New VLAN	If you want to create a new VLAN interface to which the switch port will be assigned, enter the new VLAN ID number in the New VLAN field, and then enter the IP address and subnet mask of the new VLAN logical interface in the IP Address and Subnet Mask fields.
Include this VLAN in an IRB bridge...	If you want the switch port to form part of a bridge with your wireless network, check this box. The other part of the bridge must be configured using the Wireless Application. The IP address and Subnet mask fields under New VLAN are disabled when this box is checked.

Launching the Wireless Application

After completing this LAN configuration, do the following to launch the Wireless Application and complete the bridging configuration.

Step 1 Select **Wireless Application** from the Cisco CP Tools menu. The Wireless Application opens in a separate browser window.

Step 2 In the Wireless Application, click **Wireless Express Security**, and then click **Bridging** to provide the information to complete the bridging configuration.

IRB Bridge

If you are configuring a VLAN to be part of an IRB bridge, the bridge must be a member of a bridge group.

To create a new bridge group that this interface will be part of, click **Create a new bridge group** and enter a value in the range 1 through 255.

To have this VLAN be a member of an existing bridge group, click **Join an existing bridge group**, and select a bridge group.

Note When you complete the bridge configuration in the Wireless Application, you must use the same bridge group number entered in this screen.

Field Reference

Table 4-8 IP Address and Subnet Mask

Element	Description
Create a new bridge group	To create a new bridge group that this interface will be part of, click **Create a new bridge group** and enter a value in the range 1 through 255.
Join an existing bridge group	To have this VLAN be a member of an existing bridge group, click **Join an existing bridge group**, and select a bridge group.

BVI Configuration

Assign an IP address and subnet mask to the BVI interface. If you selected an existing bridge group in the previous screen, the IP address and subnet mask will appear in this screen. You can change it, or leave the values unchanged**.**

Field Reference

Table 4-9 BVI Configuration

Element	Description
IP Address	Enter the IP address for the interface in dotted decimal format. Your network administrator should determine the IP addresses of LAN interfaces. For more information, see IP Addresses and Subnet Masks.
Net Mask	Enter the subnet mask. Obtain this value from your network administrator. The subnet mask enables the router to determine how much of the IP address is used to define the network and host portions of the address.
Net Bits	Alternatively, select the number of network bits. This value is used to calculate the subnet mask. Your network administrator can tell you the number of network bits to enter.

DHCP Pool for BVI

When you configure the router as a DHCP server, you can create a pool of IP addresses that clients on the network can use. When a client logs off the network, the address it was using is returned to the pool for use by another host.

Field Reference

Table 4-10 DHCP Pool for BVI

Element	Description
DHCP Server Configuration	If you want to have the router function as a DHCP server, check **DHCP Server Configuration**.
Starting IP	Enter the starting IP address for the pool. Be sure to specify IP addresses in the same subnet as the IP address you gave the interface. For example, If you gave the interface an IP address of 10.10.22.1, with a subnet mask of 255.255.255.0, you have over 250 addresses available for the pool, and you might specify a start IP Address of 10.10.22.2.
Ending IP	Enter the ending IP address for the pool. Using the above example, the end IP address would be 10.10.22.254.

IRB for Ethernet

If your router has a wireless interface, you can use Integrated Routing and Bridging to have this interface form part of a bridge to the wireless LAN, and enable traffic destined for the wireless network to be routed through this interface. Click **Yes** if you want to configure this Layer 3 interface for Integrated Routing and Bridging.

If you do not want this interface to be used in bridge to the wireless interface, click **No**. You will still be able to configure it as a regular routing interface.

Layer 3 Ethernet Configuration

Cisco CP supports Layer 3 Ethernet configuration on routers with installed 3750 switch modules. You can create VLAN configurations and designate router Ethernet interfaces as DHCP servers.

802.1Q Configuration

You can configure a VLAN that does not use the 802.1Q encapsulation protocol used for trunking connections. Provide a VLAN ID number, and check **Native VLAN** if you do not want the VLAN to use 802.1Q tagging.

If you want to use the 802.1Q tagging, leave the Native VLAN box unchecked.

Field Reference

Table 4-11 IP Address and Subnet Mask

Element	Description
VLAN ID (1-4094)	Enter a VLAN ID number from 1 to 4094. Cisco CP displays a message telling you to enter a different VLAN ID if the ID that you enter is already in use.
Native VLAN	If you do not want the VLAN to use 802.1Q tagging, check **Native VLAN**. If you want the VLAN to use 802.1Q tagging, leave this box unchecked.

Trunking or Routing Configuration

You can configure Layer 3 Ethernet interfaces for 802.1Q trunking or for basic routing. If you configure the interface for 802.1Q trunking, you can configure VLANs on the interface, and you can configure a native VLAN that does not use the 802.1q encapsulation protocol. I f you configure the interface for routing, you cannot configure subinterfaces or additional VLANs on the interface.

Configure Switch Device Module

If you are configuring a Gigabit Ethernet interface for routing, you can provide information about the switch module in this window. It is not required that you provide this information.

You can provide an IP address and subnet mask for the switch module, and login credentials required to log on to the switch module interface.

Check the box at the bottom of the screen if you want to log on to the switch module after providing the information in this wizard and delivering the configuration to the router.

Configure Gigabit Ethernet Interface

Provide IP address and subnet mask information for Gigabit Ethernet interfaces in this window. For more information on IP addresses and subnet masks, see LAN Wizard: IP Address and Subnet Mask.

Field Reference

Table 4-12 IP Address and Subnet Mask

Element	Description
IP Address of Physical Interface	Enter the IP address and subnet mask for the physical Gigabit Ethernet interface in these fields.
IP Address of VLAN Subinterface	Provide the IP address and subnet mask for the VLAN subinterface that you want to create on the physical interface. These fields appear if you are configuring this interface for routing. These fields do not appear if you are configuring this interface for Integrated Routing and Bridging (IRB).

Summary

This window provides a summary of the configuration changes that you made for the interface you selected.

To save this configuration to the router's running configuration and leave this wizard:

Click **Finish**. Cisco CP saves the configuration changes to the router's running configuration. Although the changes take effect immediately, they will be lost if the router is turned off.

CHAPTER 5

Configuring WAN Connections

The WAN wizards enable you to configure WAN connections for all Cisco CP-supported interfaces.

This chapter contains the following sections:

- Configuring an Ethernet WAN Connection, page 5-1
- Configuring a Serial Connection, page 5-8
- Configuring a DSL Connection, page 5-15
- Configuring an ISDN Connection, page 5-25
- Configuring an Aux Backup Connection, page 5-29
- Configuring an Analog Modem Connection, page 5-32
- Configuring a Cable Modem Connection, page 5-33

Configuring an Ethernet WAN Connection

Cisco CP enables you to configure Ethernet PPPoE or unencapsulated routing WAN connections. Complete these steps to configure an Ethernet WAN Connection.

Step 1 In the Cisco CP Feature bar, click **Configure > Interface Management > Interface and Connections**.

Step 2 In the Create Connection tab, click **Ethernet** (**PPPoE or unencapsulated routing**).

Step 3 Click **Create Connection** to start the wizard. The wizard Welcome screen describes the tasks to complete.

Step 4 Click **Next** to go to the subsequent screens to configure the connection. Cisco CP displays the Summary screen when you have completed the configuration.

Step 5 Review the configuration.

Step 6 To make changes, click **Back** to return to the screen in which you need to make changes, then return to the Summary screen.

Step 7 Check the **Test the connectivity after configuring** check box, to test the connection after sending the configuration to the router,. After you click **Finish**, Cisco CP tests the connection and displays the test results in another screen.

Step 8 Click **Finish** to send the configuration to the router.

The Ethernet WAN Connection Reference describes the screens that Cisco CP displays.

Ethernet WAN Connection Reference

- WAN Wizard Interface Welcome Window
- Select Interface
- Encapsulation: PPPoE
- IP Address: Ethernet without PPPoE
- IP Address: ATM or Ethernet with PPPoE/PPPoA
- Authentication
- Advanced Options
- Summary

WAN Wizard Interface Welcome Window

This window lists the types of connections you can configure for this interface using Cisco CP. To configure another type of connection for this interface, use the CLI.

Select Controller

Use this window to configure the VDSL Controller.

Field Reference

Table 5-1 Select Controller Field

Element	Description
Select Controller drop-down list	Choose the VDSL Controller from the list.

Select Interface - VDSL

Use this window to configure the interface for VDSL.

Field Reference

Table 5-2 Select Interface Field

Element	Description
Available Interfaces drop-down list	Choose ATM or Ethernet from the list.

Select Interface

This window appears if there is more than one interface of the type you selected in the Create Connection window. Choose the interface to use for this connection.

Field Reference

Table 5-3 Select Interface Fields

Element	Description
Check Boxes	Check the box next to the interface to use for this connection. If you are configuring an Ethernet interface, Cisco CP inserts the description text $ETH-WAN$ in the configuration file so that it will recognize the interface as a WAN interface in the future.
Enable Dynamic DNS	Click **Enable Dynamic DNS** to update your DNS servers automatically whenever the WAN interface IP address changes. Click the **Dynamic DNS** button to configure dynamic DNS. The Enable Dynamic DNS option is not shown for all connection types.

IP Address: Ethernet without PPPoE

Choose the method that the WAN interface will use to obtain an IP address.

Field Reference

Table 5-4 Ethernet without PPPoE IP Address Fields

Element	Description
Static IP Address	If you choose **Static IP Address**, enter the IP address and subnet mask or the network bits in the fields provided. For more information, see IP Addresses and Subnet Masks.
Dynamic (DHCP Client)	If you choose Dynamic, the router leases an IP address from a remote DHCP server. Enter the name of the DHCP server that will assign addresses.
Dynamic DNS	Choose dynamic DNS to update your DNS servers automatically whenever the WAN interface IP address changes. Click the **Dynamic DNS** button to configure dynamic DNS.

Encapsulation: PPPoE

This window lets you enable Point-to-Point-Protocol over Ethernet (PPPoE) encapsulation. This is necessary if your service provider or network administrator requires remote routers to communicate using PPPoE.

PPPoE is a protocol used by many asymmetric digital subscriber line (ADSL) service providers. Ask your service provider if PPPoE is used over your connection.

If you choose PPPoE encapsulation, Cisco CP automatically adds a dialer interface to the configuration, and this is shown in the Summary window.

Field Reference

Table 5-5 PPoE Encapsulation Fields

Element	Description
Enable PPPoE Encapsulation	If your service provider requires that the router use PPPoE, check this box to enable PPPoE encapsulation. Uncheck this box if your service provider does not use PPPoE. This check box will not be available if your router is running a version of Cisco IOS that does not support PPPoE encapsulation.

Summary

This screen displays a summary of the WAN link that you configured.You can review this information. If you need to change anything, click the **Back** button to return to the screen on which you need to make changes.

Button Reference

Table 5-6 WAN Summary Buttons

Element	Description
Test the connectivity after configuring	Check this box to have Cisco CP test the connection you have configured, after it delivers the commands to the router. Cisco CP tests the connection and reports results in another window.

To save this configuration to the running configuration of the router and leave this wizard:

Click **Finish**. Cisco CP saves the configuration changes to the running configuration of the router. The changes take effect immediately, but are lost if the router is turned off.

If you checked **Preview commands before delivering to router** in the Cisco CP Preferences window, the Deliver window appears. In this window, you can view the CLI commands that you are delivering to the router.

Advanced Options

There are two advanced options available, based on the router's configuration: Default static route and Port Address Translation (PAT).

If the Static Route option is not visible in the window, it means a static route has already been configured on the router.

If the PAT option is not visible, PAT has already been configured on an interface.

Field Reference

Table 5-7 Advanced Options Fields

Element	Description
Default Static Route	Check this box to configure a static route to the outside interface to which outgoing traffic will be routed. If a static route has already been configured on this router, this box does not appear.
Next Hop Address	If your service provider has given you a next-hop IP address to use, enter the IP address in this field. If you leave this field blank, Cisco CP will use the WAN interface that you are configuring as the next-hop interface.
Port Address Translation	If devices on the LAN have private addresses, you can allow them to share a single public IP address. You can ensure that traffic goes to its proper destination by using PAT, which represents hosts on a LAN with a single IP address and uses different port numbers to distinguish the hosts. If PAT has already been configured on an interface, the PAT option will not be visible.
Inside Interface to be Translated	Choose the inside interface connected to the network whose host IP addresses you want to be translated.

Configuring a VDSL Connection

Cisco CP enables you to configure VDSL PPPoE or unencapsulated routing WAN connections. Complete these steps to configure a VDSL WAN Connection:

Step 1 In the Cisco CP Feature bar, click **Configure > Interface Management > Interface and Connections**.

Step 2 In the Create Connection tab, click **VDSL** (**PPPoE or unencapsulated routing**).

Step 3 Click **Create Connection** to start the wizard. The wizard Welcome screen lists the VDSL WAN connections supported.

Step 4 Click **Next**.

Step 5 The Select Controller screen is displayed. Choose the VDSL Controller from the drop-down list.

Step 6 Click **Next**.

Step 7 The Select Interface window appears if there is more than one interface of the type you selected in the Create Connection window. Choose the interface to use for this connection.

Step 8 Click **Next**.

Step 9 The Encapsulation screen is displayed. Click the required encapsulation type.

Step 10 Click **Next**.

Step 11 The PVC screen is displayed. Enter the Virtual Path Identifier (VPI) and Virtual Circuit Identifier (VCI) values.

Step 12 Click **Next**.

Step 13 The IP Address screen is displayed. Enter the IP address for the connection.

Step 14 Click **Next**.

Step 15 The Authentication screen is displayed. Select authentication type and enter username and password.

Step 16 Click **Next**.

Step 17 The Advanced Options screen is displayed. Configure Port Address Translation (PAT).

Step 18 Click **Next.**

Step 19 The Summary screen is displayed. Review the configuration. To make changes, click **Back** to return to the screen in which you need to make changes, then return to the Summary screen.

Step 20 Check the **Test the connectivity after configuring** checkbox to test the connection after sending the configuration to the router. After you click **Finish**, Cisco CP tests the connection and displays the test results in another screen.

Step 21 Click **Finish** to send the configuration to the router.

The VDSL WAN Connection Reference describes the screens that Cisco CP displays.

VDSL WAN Connection Reference

- WAN Wizard Interface Welcome Window
- Select Controller
- Select Interface - VDSL
- Encapsulation Autodetect
- PVC
- IP Address: ATM or Ethernet with PPPoE/PPPoA
- Authentication
- Advanced Options
- Summary

Configuring a Serial Connection

Complete these steps to configure a Serial connection:

Step 1 In the Cisco CP Feature bar, click **Configure**.

Step 2 Click **Interfaces and Connections**.

Step 3 In the Create Connection tab, click **Serial**.

Step 4 Click **Create Connection** to start the wizard. The wizard Welcome screen describes the tasks to complete.

Step 5 Click **Next** to go to the next screens to configure the connection.

Step 6 Cisco CP displays the Summary screen when you have completed the configuration. Review the configuration. To make changes, click **Back** to return to the screen in which you need to make changes, then return to the Summary screen.

Step 7 Check the **Test the connectivity after configuring** checkbox, to test the connection after sending the configuration to the router. After you click **Finish**, Cisco CP tests the connection and displays the test results in another screen.

Step 8 Click **Finish** to send the configuration to the router.

The Serial Connection Reference describes the screens that Cisco CP displays.

Serial Connection Reference

- WAN Wizard Interface Welcome Window
- Select Interface
- IP Address: Serial with Point-to-Point Protocol
- IP Address: Serial with HDLC or Frame Relay
- Authentication
- Configure LMI and DLCI
- Configure Clock Settings
- Advanced Options
- Summary

IP Address: Serial with Point-to-Point Protocol

Choose the method that the point-to-point interface will use to obtain an IP address.

Field Reference

Table 5-8 Serial Connection with Point-to-Point Protocol

Element	Description
Static IP Address	If you choose **Static IP Address**, enter the IP address and subnet mask or the network bits in the fields provided. For more information, see IP Addresses and Subnet Masks.
IP Unnumbered	Choose **IP Unnumbered** to have the interface share an IP address that has already been assigned to another interface. Choose the interface whose IP address to use for the interface you are configuring.
Easy IP (IP Negotiated)	Choose **Easy IP (IP Negotiated)** if the router will obtain an IP address through PPP/IPCP address negotiation.
Dynamic DNS	Choose dynamic DNS to update your DNS servers automatically whenever the WAN interface IP address changes. Click the **Dynamic DNS** button to configure dynamic DNS.

IP Address: Serial with HDLC or Frame Relay

Choose the method that the WAN interface will use to obtain an IP address. If Frame Relay encapsulation is used, Cisco CP creates a subinterface, and the IP address is assigned to the subinterface Cisco CP creates.

Field Reference

Table 5-9 Serial Connection with HDLC or Frame Relay Fields

Element	Description
Static IP Address	If you choose **Static IP Address**, enter the IP address and subnet mask or the network bits in the fields provided. For more information, see IP Addresses and Subnet Masks.

Table 5-9 Serial Connection with HDLC or Frame Relay Fields (continued)

Element	Description
IP Unnumbered	Choose **IP Unnumbered** if you want the interface to share an IP address that has already been assigned to another interface. Then choose the interface whose IP address you want to use for the interface you are configuring.
Dynamic DNS	Choose dynamic DNS if you want to update your DNS servers automatically whenever the WAN interface IP address changes. Click the **Dynamic DNS** button to configure dynamic DNS.

Authentication

This page is displayed if you enabled or are configuring:

- PPP for a serial connection
- PPPoE or PPPoA encapsulation for an ATM connection
- PPPoE or PPPoA encapsulation for an Ethernet connection
- An ISDN BRI or analog modem connection

Your service provider or network administrator may use a Challenge Handshake Authentication Protocol (CHAP) password or a Password Authentication Protocol (PAP) password to secure the connection between the devices. This password secures both incoming and outgoing access.

Field Reference

Table 5-10 Authentication Fields

Element	Description
Authentication Type	Check the box for the type of authentication used by your service provider. If you do not know which type your service provider uses, you can check both boxes: the router will attempt both types of authentication, and one attempt will succeed. CHAP authentication is more secure than PAP authentication.
Username	The username is given to you by your Internet service provider or network administrator and is used as the username for CHAP or PAP authentication.

Table 5-10 Authentication Fields (continued)

Element	Description
Password	Enter the password exactly as given to you by your service provider. Passwords are case sensitive. For example, the password access is not the same as Access.
Confirm Password	Re-enter the same password that you entered in the previous box.

Configure LMI and DLCI

If you are configuring a connection with Frame Relay encapsulation, you must specify the protocol used to monitor the connection, called the Local Management Identifier (LMI), and provide a unique identifier for this particular connection, called a data link connection identifier (DLCI).

Field Reference

Table 5-11 LMI and DLCI Fields

Element	Description
LMI Type	
ANSI	Annex D defined by ANSI[1] standard T1.617.
Cisco	LMI type defined jointly by Cisco Systems and three other companies.
ITU-T Q.933	ITU-T Q.933 Annex A.
Autosense	Default. This setting allows the router to detect which LMI type is being used by communicating with the switch and to then use that type. If **autosense** fails, the router will use the Cisco LMI type.
DLCI	Enter the DLCI in this field. This number must be unique among all DLCIs used on this interface.
Use IETF Frame Relay Encapsulation	IETF[2] encapsulation. This option is used when connecting to non-Cisco routers. Check this box if you are connecting to a non-Cisco router on this interface.

1. ANSI - American National Standards Institute
2. IETF - Internet Engineering Task Force

Configure Clock Settings

The Clock Settings window is available when you are configuring a T1 or E1 link. The default Frame Relay clock settings are shown on this page. You should not change them unless you know you have different requirements.

Field Reference

Table 5-12 Clock Settings Fields

Element	Description
Clock Source	The clock synchronizes data transmission. Default is **line**. Internal specifies that the clock be generated internally. Line specifies that the clock source be taken from the network.
T1 Framing	This field configures the T1 or E1 link for operation with D4 Super Frame (sf) or Extended Superframe (esf). The default is **esf**.
Line Code	This field configures the router for operation on binary 8-zeros substitution (B8ZS) or alternate mark inversion (AMI) T1 lines. The b8zs setting ensures density on a T1 or E1 line by substituting intentional bipolar violations in bit positions 4 and 7 for a sequence of eight zero bits. When the router is configured with the AMI setting, you must use the data-coding inverted setting to ensure density on the T1 line. The default is **b8zs**.
Data Coding	Click **inverted** if you know that user data is inverted on this link, or if the Line Code field is set to AMI. Otherwise leave this set to the default value **normal**. Data inversion is used with bit-oriented protocols such as HDLC, PPP, and LAPB to ensure density on a T1 line with AMI encoding. These bit-oriented protocols perform "zero insertions" after every five "one" bits in the data stream. This has the effect of ensuring at least one zero in every eight bits. If the data stream is then inverted, it ensures that at least one out of every eight bits is a one. Cisco CP sets data coding to inverted if the line code is AMI and there are no time slots configured for 56 kbps. If you do not want to use inverted data coding with the AMI line code, you must use the CLI to configure all time slots to 56 kbps.

Table 5-12 Clock Settings Fields (continued)

Element	Description
Facilities Data Link (FDL)	This field configures the router behavior on the Facilities Data Link (FDL) of the Extended Superframe. When configured with **att**, the router implements AT&T TR 54016. When configured with **ansi**, it implements ANSI T1.403. When you choose both, the router implements both **att** and **ansi** choices.When you choose none, the router ignores the FDL. The default is **none. If T1 or E1 framing is set to sf,** Cisco CP will set FDL to **none** and make this field read-only.
Line Build Out (LBO)	This field is used to configure the line build out (LBO) of the T1 link. The LBO decreases the transmit strength of the signal by –7.5 or –15 decibels. It is not likely to be needed on actual T1 or E1 lines. The default is **none**.
Remote Loopback Requests	This field specifies whether the router will go into loopback mode when a loopback code is received on the line. Choosing **full** causes the router to accept full loopbacks, whereas choosing **payload-v54** will cause the router to choose payload loopbacks.
Enable Generation/Detection of Remote Alarms	Check this box to have the router T1 link generate remote alarms (yellow alarms) and to detect remote alarms being sent from the peer on the other end of the link. The remote alarm is transmitted by a router when it detects an alarm condition: either a red alarm (loss of signal) or a blue alarm (unframed 1s). The receiving channel service unit/data service unit (CSU/DSU) then knows that there is an error condition on the line. This setting should only be used when T1 framing is set to **esf**.

Configuring a DSL Connection

Complete these steps to configure an ADSL, or G.SHDSL connection:

Step 1 In the Cisco CP Feature bar, click **Configure**.

Step 2 Click **Interfaces and Connections**. The Create Connection tab displays the available DSL connection types, for example, ADSL (PPPoE or RFC 1483 routing or PPPoA).

Step 3 Choose an available connection type.

Step 4 Click **Create Connection** to start the wizard. The wizard Welcome screen describes the tasks you will complete.

Step 5 Click **Next** to go to the subsequent screens to configure the connection.

Step 6 Cisco CP displays the Summary screen when you have completed the configuration. Review the configuration. To make changes, click **Back** to return to the screen in which you need to make changes, then return to the Summary screen.

Step 7 Check the **Test the connectivity after configuring** checkbox to test the connection after sending the configuration to the router. After you click **Finish**, Cisco CP tests the connection and displays the test results in another screen.

Step 8 Click **Finish** to send the configuration to the router.

The following section describes the screens that Cisco CP displays:

- DSL Connection Reference

DSL Connection Reference

- WAN Wizard Interface Welcome Window
- Select Interface
- Encapsulation: PPPoE
- Encapsulation Autodetect
- IP Address: ATM or Ethernet with PPPoE/PPPoA
- IP Address: ATM with RFC 1483 Routing
- Authentication
- Advanced Options
- PVC
- Summary

IP Address: ATM or Ethernet with PPPoE/PPPoA

Choose the method that the WAN interface will use to obtain an IP address.

Field Reference

Table 5-13 ATM or Ethernet with PPPoE or PPPoA

Element	Description
Static IP Address	If you choose **Static IP Address**, enter the IP address and subnet mask or the network bits in the fields provided.
Dynamic (DHCP Client)	If you choose **Dynamic**, the router will lease an IP address from a remote DHCP server. Enter the name of the DHCP server that will assign addresses.
IP Unnumbered	Choose **IP Unnumbered** to have the interface share an IP address that has already been assigned to another interface. Choose the interface with the IP address you want to use for the interface you are configuring.

Table 5-13 ATM or Ethernet with PPPoE or PPPoA (continued)

Element	Description
Easy IP (IP Negotiated)	Choose **Easy IP (IP Negotiated)** if the router will obtain an IP address through PPP/IPCP address negotiation.
Dynamic DNS	Choose dynamic DNS if you want to update your DNS servers automatically whenever the WAN interface IP address changes. Click the **Dynamic DNS** button to configure dynamic DNS.

IP Address: ATM with RFC 1483 Routing

Choose the method that the WAN interface will use to obtain an IP address.

Field Reference

Table 5-14 ATM with RFC 1483 Routing

Element	Description
Static IP Address	If you choose **Static IP Address**, enter the IP address and subnet mask or the network bits in the fields provided. For more information, see IP Addresses and Subnet Masks.
Dynamic (DHCP Client)	If you choose Dynamic, the router will lease an IP address from a remote DHCP server. Enter the name of the DHCP server that will assign addresses.
IP Unnumbered	Click **IP Unnumbered** if you want the interface to share an IP address that has already been assigned to another interface. Then choose the interface whose IP address you want to use for the interface you are configuring.
Dynamic DNS	Choose dynamic DNS if you want to update your DNS servers automatically whenever the WAN interface IP address changes. Click the **Dynamic DNS** button to configure dynamic DNS.

Encapsulation Autodetect

In this window, choose the type of encapsulation that the WAN link will use. Ask your service provider or network administrator which type of encapsulation is used for this link. The interface type determines the types of encapsulation available.

Field Reference

Table 5-15 Encapsulation Fields

Element	Description
Autodetect	Click **Autodetect** to have Cisco CP discover the encapsulation type. If Cisco CP succeeds, it will automatically supply the encapsulation type and other configuration parameters it discovers.
Encapsulations Available for ADSL, G.SHDSL, or ADSL over ISDN	
PPPoE	Provides Point-to-Point Protocol over Ethernet encapsulation. This option is available when you have selected an Ethernet interface or an ATM interface. An ATM subinterface and a dialer interface will be created when you configure PPPoE over an ATM interface. The PPPoE radio button will be disabled if your router is running a version of Cisco IOS that does not support PPPoE encapsulation.
PPPoA	Point-to-Point protocol over ATM. This option is available when you have selected an ATM interface. An ATM subinterface and a dialer interface will be created when you configure PPPoA over an ATM interface. The PPPoA radio button will be disabled if your router is running a version of Cisco IOS that does not support PPPoA encapsulation.
RFC 1483 routing with AAL5-SNAP	This option is available when you have selected an ATM interface. An ATM subinterface will be created when you configure an RFC 1483 connection. This subinterface will be visible in the Summary window.
RFC 1483 routing with AAL5-MUX	This option is available when you have selected an ATM interface. An ATM subinterface will be created when you configure an RFC 1483 connection. This subinterface will be visible in the Summary window.
Encapsulations Available for Serial Interfaces	

Table 5-15 Encapsulation Fields (continued)

Element	Description
Frame Relay	Provides Frame Relay encapsulation. This option is available when you have selected a serial interface. A serial subinterface will be created when you create a Frame Relay connection. This subinterface will be visible in the Summary window. **Note** If a Frame Relay serial connection has been added to an interface, only Frame Relay encapsulation will be enabled in this window when subsequent serial connections are configured on the same interface.
Point-to-Point Protocol	Provides PPP encapsulation. This option is available when you have selected a serial interface.
High Level Data Link Control	Provides HDLC encapsulation. This option is available when you have selected a serial interface.

PVC

ATM routing uses a two-layer hierarchical scheme—virtual paths and virtual channels—denoted by the virtual path identifier (VPI) and virtual channel identifier (VCI), respectively. A particular virtual path may carry a number of different virtual channels corresponding to individual connections. When switching is performed based on the VPI, all cells on that particular virtual path are switched regardless of the VCI. An ATM switch can route according to VCI, VPI, or both VCI and VPI.

Field Reference

Table 5-16 PVC Fields

Element	Description
VPI	Enter the VPI value obtained from your service provider or system administrator. The virtual path identifier (VPI) is used in ATM switching and routing to identify the path used for a number of connections. Enter the VPI value given to you by your service provider.

Table 5-16 PVC Fields (continued)

Element	Description
VCI	Enter the VCI value obtained from your service provider or system administrator. The virtual circuit identifier (VCI) is used in ATM switching and routing to identify a particular connection within a path that it may share with other connections. Enter the VCI value given to you by your service provider.

Cisco IOS Default Values

The values shown in the following table are Cisco IOS defaults. Cisco CP will not overwrite these values if they have been changed during an earlier configuration, but if your router has not been previously configured, these are the values that will be used.

Table 5-17 Cisco IOS Default Values

Connection Type	Parameter	Value
ADSL	• Operating mode	• Auto
G.SHDSL	• Operating mode • Line rate • Equipment type	• Annex A (United States) • Auto • CPE
ADSL over ISDN	• Operating mode	• Auto

Configuring a G.SHDSL Controller

Complete these steps to configure an HWIC-4SHDSL or HWIC-2SHDSL controller.

Step 1 In the Cisco CP Feature bar, click **Configure**.

Step 2 In the Cisco CP taskbar, click **Interfaces and Connections**.

Step 3 In the Create Connection tab, click **G.SHDSL (PPPoE, RFC 1483, or PPPoA)**.

Step 4 Click **Create Connection** to start the wizard. The wizard Welcome screen describes the tasks to complete.

Step 5 Click **Next** to go to the subsequent screens to configure the connection. Cisco CP displays the Summary screen when you have completed the configuration. Review the configuration. If you need to make changes, click **Back** to return to the screen in which you need to make changes, then return to the Summary screen.

Step 6 If you want to test the connection after sending the configuration to the router, check **Test the connectivity after configuring**. After you click Finish, Cisco CP tests the connection and displays the test results in another screen.

Step 7 To send the configuration to the router, click **Finish**.

The G.SHDSL Controller Reference describes the screens that Cisco CP displays.

G.SHDSL Controller Reference

The following sections describe the Cisco CP G.SHDSL Controller wizard screens:

- SHDSL Configuration Mode Selection for HWIC-1SHDSL Controller, page 5-22
- SHDSL Configuration Mode Selection for HWIC-2SHDSL Controller, page 5-22
- SHDSL Configuration Mode Selection for HWIC-4SHDSL Controller, page 5-23

SHDSL Configuration Mode Selection for HWIC-1SHDSL Controller

This screen appears when you have chosen to configure an HWIC-1SHDSL controller.

Field Reference

Table 5-18 HWIC-1SHDSL Fields

Field	Description
Available Controllers	Choose the G.SHDSL controller that you want to configure. If you are configuring an HWIC-1SHDSL controller, no other fields appear. You can click **Next** to go to the next screen.

SHDSL Configuration Mode Selection for HWIC-2SHDSL Controller

This screen appears when you have chosen to configure an HWIC-2SHDSL controller. Use this screen to configure a DSL Group, or a DSL Interface.

Field Reference

Table 5-19 HWIC-2SHDSL Fields

Field	Description
Available Controllers	Choose the G.SHDSL controller that you want to configure.
Configure DSL Group	To create a DSL Group, click **Configure DSL Group**.
Configure DSL Interface	To configure the DSL interface, click **Configure DSL Interface** and click **Next**.
DSL Group Configuration	
Group Number	Choose the group number that you want to configure.
DSL Pairs	Choose the DSL pairs that you want to be included in the group. You can choose pair 0, or pair 0 and 1.

Things to Know about this Screen

- A DSL group must be configured before the ATM interface can be configured. Thus, when there are no DSL groups configured on the G.SHDSL controller the Configure DSL Group and Configure DSL Interface radio buttons does not appear, and you are only allowed to configure a DSL group, and are not given the option of configuring a DSL interface.
- When a DSL group has been configured, both the Configure DSL Group and Configure DSL Interface radio buttons are displayed.
- Only the group numbers that have not been configured are displayed. For example, if you have already configured group 0, only the group 1 radio button is displayed.
- DSL pairs already configured in a DSL group are disabled.

SHDSL Configuration Mode Selection for HWIC-4SHDSL Controller

This screen appears when you have chosen to configure an HWIC-4SHDSL controller. Use this screen to configure a DSL Group, or a DSL Interface.

Field Reference

Table 5-20 HWIC-4SHDSL Fields

Field	Description
Available Controllers	Choose the G.SHDSL controller that you want to configure.
Configure DSL Group	To create a DSL Group, click **Configure DSL Group**.
DSL Group Configuration	
Group Number	Choose the group number that you want to configure.

Table 5-20 HWIC-4SHDSL Fields (continued)

Field	Description
DSL Pairs	Choose the DSL pairs that you want to be included in the group. The permitted combinations depend on the chosen group type. To learn more, see *Configuring Cisco G.SHDSL HWICs in Cisco Access Routers* at: http://www.cisco.com/en/US/docs/routers/access/interfaces/software/feature/guide/shdslfm.html When the web page appears, click the dsl-group link to display the permitted combinations.
Group Type	DSL pairs can be bundled in IMA groups or M-pair groups: • IMA—inverse multiplexing over ATM. IMA allows you to bundle communications lines to obtain speeds in excess of 3 Mbps. IMA provides a protocol that handles link failure and recovery, and also the addition and deletion of links. IMA bundling creates an ATM-IMA interface. • M-Pair—Multi-pair bundling allows you to group pairs to create an ATM interface without IMA features.

Things to know about this screen

- When you create a DSL group, an ATM interface is created, and a subinterface is also created. These will be visible in the Controller/Connections tab. See DSL Edit Controllers/Connection Tab for more information.
- A DSL group must be configured before the ATM interface can be configured. Thus, when there are no DSL groups configured on the G.SHDSL controller only the Configure DSL Group radio button appears.
- When a controller with a configured DSL group is chosen, both the Configure DSL Group and Configure DSL Interface radio buttons are displayed.
- Only the group numbers that have not been configured are displayed. For example, if you have already configured group 0, only the group 1 radio button is displayed.
- DSL pairs already configured in a DSL group are disabled.

Configuring an ISDN Connection

Complete these steps to configure an ISDN connection:

Step 1 In the Cisco CP Feature bar, click **Configure**.

Step 2 In the Cisco CP taskbar, click **Interfaces and Connections**.

Step 3 In the Create Connection tab, click **ISDN (PPP)**.

Step 4 Click **Create Connection** to start the wizard. The wizard Welcome screen describes the tasks you will complete.

Step 5 Click **Next** to go to the subsequent screens to configure the connection. Cisco CP displays the Summary screen when you have completed the configuration. Review the configuration. If you need to make changes, click **Back** to return to the screen in which you need to make changes, then return to the Summary screen.

Step 6 If you want to test the connection after sending the configuration to the router, check **Test the connectivity after configuring**. After you click **Finish**, Cisco CP tests the connection and displays the test results in another screen.

Step 7 To send the configuration to the router, click **Finish**.

The ISDN Connection Reference describes the screens that Cisco CP displays.

ISDN Connection Reference

The following sections describe the Cisco CP ISDN Connection screens:

- ISDN Wizard Welcome Window
- Select Interface
- IP Address: ISDN BRI or Analog Modem
- Switch Type and SPIDs
- Authentication
- Advanced Options
- Dial String
- Summary

ISDN Wizard Welcome Window

PPP is the only type of encoding supported over an ISDN BRI by Cisco CP.

IP Address: ISDN BRI or Analog Modem

Choose the method that the ISDN BRI or analog modem interface will use to obtain an IP address.

Field Reference

Table 5-21 IP Address for ISDN BRI or Analog Modem Fields

Element	Description
Static IP Address	If you choose **Static IP Address**, enter the IP address and subnet mask or the network bits in the fields provided. For more information, see IP Addresses and Subnet Masks.
IP Unnumbered	Choose **IP Unnumbered** if you want the interface to share an IP address that has already been assigned to another interface. Then, choose the interface that has the IP address that you want the interface that you are configuring to use.
Easy IP (IP Negotiated)	Choose **IP Negotiated** if the interface will obtain an IP address from your ISP through PPP/IPCP address negotiation whenever a connection is made.
Dynamic DNS	Choose **Dynamic DNS** if you want to update your DNS servers automatically whenever the WAN interface IP address changes. Click the **Dynamic DNS** button to configure dynamic DNS.

Switch Type and SPIDs

ISDN BRI connections require identification of the ISDN switch type, and in some cases, identification of the B channels using service profile ID (SPID) numbers. This information will be provided to you by your service provider.

Field Reference

Table 5-22 Switch Type and SPIDs Fields

Element	Description
ISDN Switch Type	Choose the ISDN switch type. Contact your ISDN service provider for the switch type for your connection. Cisco CP supports these BRI switch types: • For North America: – basic-5ess—Lucent (AT&T) basic rate 5ESS switch – basic-dms100—Northern Telecom DMS-100 basic rate switch – basic-ni—National ISDN switches • For Australia, Europe, and the UK: – basic-1tr6—German 1TR6 ISDN switch – basic-net3—NET3 ISDN BRI for Norway NET3, Australia NET3, and New Zealand NET3switch types; ETSI-compliant switch types for Euro-ISDN E-DSS1 signaling system – vn3—French ISDN BRI switches • For Japan: – ntt—Japanese NTT ISDN switches • For voice or PBX systems: – basic-qsig—PINX (PBX) switches with QSIG signaling per Q.931

Table 5-22 Switch Type and SPIDs Fields (continued)

Element	Description
I have SPIDS	Check this check box if your service provider requires SPIDs. Some service providers use SPIDs to define the services that are subscribed to by an ISDN device that is accessing the ISDN service provider. The service provider assigns the ISDN device one or more SPIDs when you first subscribe to the service. If you are using a service provider that requires SPIDs, your ISDN device cannot place or receive calls until it sends a valid, assigned SPID to the service provider when the device accesses the switch to initialize the connection. Currently, only the DMS-100 and NI switch types require SPIDs. The AT&T 5ESS switch type may support a SPID, but we recommend that you set up the ISDN service without SPIDs. In addition, SPIDs have significance only at the local access ISDN interface. Remote routers never receive the SPID. A SPID is usually a 7-digit telephone number with some optional numbers. However, service providers may use different numbering schemes. For the DMS-100 switch type, two SPIDs are assigned, one for each B channel.
Spid 1	Enter the SPID for the first BRI B channel provided to you by your ISP.
Spid 2	Enter the SPID for the second BRI B channel provided to you by your ISP.

Dial String

Enter the phone number of the remote end of the ISDN BRI or analog modem connection. This is the phone number that the ISDN BRI or analog modem interface will dial whenever a connection is made. The dial string is provided to you by your service provider.

Configuring an Aux Backup Connection

Complete these steps to configure an Aux Backup connection:

Step 1 In the Cisco CP Feature bar, click **Configure**.

Step 2 In the Cisco CP taskbar, click **Interfaces and Connections**.

Step 3 In the Create Connection tab, click **Aux Backup.**

Step 4 Click **Create Connection** to start the wizard. The wizard Welcome screen describes the tasks you will complete.

Step 5 Click **Next** to go to the subsequent screens to configure the connection. Cisco CP displays the Summary screen when you have completed the configuration. Review the configuration. If you need to make changes, click **Back** to return to the screen in which you need to make changes, then return to the Summary screen.

Step 6 If you want to test the connection after sending the configuration to the router, check **Test the connectivity after configuring**. After you click **Finish**, Cisco CP tests the connection and displays the test results in another screen.

Step 7 To send the configuration to the router, click **Finish**.

The Aux Backup Connection Reference describes the screens that Cisco CP displays.

Aux Backup Connection Reference

- Aux Backup Welcome Window
- Backup Configuration
- Backup Configuration: Primary Interface and Next Hop IP Addresses
- Backup Configuration: Hostname or IP Address to Be Tracked
- Summary

Aux Backup Welcome Window

The option to configure the AUX port as a dial-up connection only appears for the Cisco 831 and 837 routers.

The Aux dial-backup radio button is disabled if any of the following conditions exist:

- More than one default route exists.
- One default route exists and it is configured with an interface other than the primary WAN interface.

The Aux dial-backup option is not shown if any of the following conditions exist:

- Router is not using a Cisco IOS image that supports the Aux dial-backup feature.
- Primary WAN interface is not configured.
- Asynchronous interface is already configured.
- Asynchronous interface is not configurable by Cisco CP because of the presence of unsupported Cisco IOS commands in the existing configuration.

Backup Configuration

ISDN BRI and analog modem interfaces can be configured to work as backup interfaces to other, primary interfaces. In that case, an ISDN or analog modem connection will be made only if the primary interface goes down for some reason. If the primary interface and connection go down, the ISDN or analog modem interface will immediately dial out and try to establish a connection so that network services are not lost.

Choose whether this ISDN BRI or analog modem connection should act as a backup connection.

Field Reference

Table 5-23 Backup Configuration Fields

Element	Description
Configure this connection as backup	Check this option to designate this interface as backup.
Do not configure this connection as backup.	Check this option if you do not want to designate this interface as backup.

Prerequisites

Note the following prerequisites:

- The primary interface must be configured for site-to-site VPN.
- The Cisco IOS image on your router must support the SAA ICMP Echo Enhancement feature.

Backup Configuration: Primary Interface and Next Hop IP Addresses

For the ISDN BRI or analog modem connection to act as a backup connection, it must be associated with another interface on the router that will act as the primary connection. The ISDN BRI or analog modem connection will be made only if the connection on the primary interface goes down.

Field Reference

Table 5-24 Hostname or IP Address to Be Tracked Fields

Element	Description
Primary Interface	Enter the IP address or hostname of the destination host to which connectivity will be tracked. Specify an infrequently contacted destination as the site to be tracked.
Primary Next Hop IP Address	Choose the router interface that will maintain the primary connection.
Backup Next Hop IP Address	This field is optional. Enter the IP address to which the backup interface will connect when it is active, known as the *next hop IP address*.

Backup Configuration: Hostname or IP Address to Be Tracked

This screen lets you identify a specific host to which connectivity must be maintained. The router will track connectivity to that host, and if the router discovers that connectivity has been lost by the primary interface, a backup connection will be initiated over the ISDN BRI or analog modem interface.

Field Reference

Table 5-25 Hostname or IP Address to Be Tracked Fields

Element	Description
IP Address to Be Tracked	Enter the IP address or hostname of the destination host to which connectivity will be tracked. Specify an infrequently contacted destination as the site to be tracked.

Configuring an Analog Modem Connection

Complete these steps to configure an Analog Modem connection:

Step 1 In the Cisco CP Feature bar, click **Configure**.

Step 2 In the Cisco CP taskbar, click **Interfaces and Connections**.

Step 3 In the Create Connection tab, click **Analog Modem.**

Step 4 Click **Create Connection** to start the wizard. The wizard Welcome screen describes the tasks you will complete.

Step 5 Click **Next** to go to the subsequent screens to configure the connection. Cisco CP displays the Summary screen when you have completed the configuration. Review the configuration. If you need to make changes, click **Back** to return to the screen in which you need to make changes, then return to the Summary screen.

Step 6 If you want to test the connection after sending the configuration to the router, check **Test the connectivity after configuring**. After you click **Finish**, Cisco CP tests the connection and displays the test results in another screen.

Step 7 To send the configuration to the router, click **Finish**.

The Analog Modem Connection Reference describes the screens that Cisco CP displays.

Analog Modem Connection Reference

- Analog Modem Welcome
- IP Address: ISDN BRI or Analog Modem
- Authentication
- Dial String
- Summary

Analog Modem Welcome

This screen describes the tasks you will perform to configure an analog modem connection. PPP is the only type of encoding supported over an analog modem connection by Cisco CP.

Configuring a Cable Modem Connection

Complete these steps to configure a Cable Modem connection:

Step 1 In the Cisco CP Feature bar, click **Configure**.

Step 2 Click **Interfaces and Connections**.

Step 3 In the Create Connection tab, click **Cable Modem.**

Step 4 Click **Create Connection** to start the wizard. The wizard Welcome screen describes the tasks you will complete.

Step 5 Click **Next** to go to the subsequent screens to configure the connection.

Step 6 Cisco CP displays the Summary screen when you have completed the configuration. Review the configuration. If you need to make changes, click **Back** to return to the screen in which you need to make changes, then return to the Summary screen.

Step 7 If you want to test the connection after sending the configuration to the router, check **Test the connectivity after configuring**. After you click **Finish**, Cisco CP tests the connection and displays the test results in another screen.

Step 8 To send the configuration to the router, click **Finish**.

The Cable Modem Connection Reference describes the screens that Cisco CP displays.

Cable Modem Connection Reference

- Cable Modem Connection Wizard Welcome
- Select Interface
- Advanced Options
- Summary

Cable Modem Connection Wizard Welcome

The Welcome screen indicates that you are using the cable modem connection wizard, and describes the tasks you perform when you configure a Cable Modem connection.

Click **Next** to begin configuring the connection.

Select Interface

Select the cable modem interface to configure in this screen. The interface that you select will be configured as a DHCP client.

Field Reference

Table 5-26 Select Interface

Element	Description
Select an interface for the WAN connection	Choose the cable modem interface that you want to configure.
Enable Dynamic DNS	Check **Enable Dynamic DNS** if you want to update your DNS servers automatically whenever the WAN interface IP address changes.
Dynamic DNS	Click the Dynamic DNS button to configure a dynamic DNS method. See Add or Edit Dynamic DNS Method for more information.

Summary

The Summary screen shows the configuration you are sending to the router. Cisco CP configures a cable modem connection as a DHCP client. The following lines show cable modem connection with no NAT or static route configuration

```
Selected Interface: Cable Modem 0/1/0
IP Address: Dynamic (DHCP Client)
```

Field Reference

Table 5-27 Summary Buttons

Element	Description
Test the connectivity after configuring	Check this box if you want Cisco CP to test the connection you have configured after it delivers the commands to the router. Cisco CP will test the connection and report results in another window.

To save this configuration to the router's running configuration and leave this wizard:

Click **Finish**. Cisco CP saves the configuration changes to the router's running configuration. The changes will take effect immediately, but will be lost if the router is turned off.

If you checked **Preview commands before delivering to router** in the Cisco CP Preferences window, the Deliver window appears. In this window, you can view the CLI commands that you are delivering to the router.

CHAPTER 6

Edit Interface/Connection

This window displays the router interfaces and connections. The window also enables you to add, edit, and delete connections, and to enable or disable connections.

Add

When you choose an unconfigured physical interface and click **Add**, the menu contains choices for adding a connection on that interface. Click **Add** to create a new loopback or tunnel interface. If the Cisco IOS image on the router supports Virtual Template Interfaces (VTI), the context menu contains an option to add a VTI. If there are switch ports present on the router, you can add a new VLAN.

To reconfigure an interface, if you see no choices except Loopback and Tunnel when you click **Add**, choose the interface and click **Delete**. All the types of connections available for that kind of interface appears in the Add menu. Click **Available Interface Configurations** to see what configurations are available for an interface.

Edit

When you choose an interface and click **Edit**, the Interface Feature Edit dialog box appears. If the interface is a supported and configured interface and is not a switch port, the dialog box has the following tabs:

- Connection
- Media Type. The Media Type tab is displayed if the chosen interface is a small form-factor pluggable (SFP) interface.
- Association
- NAT
- Application Service
- General

If the interface is not supported, the dialog box will *not* have a Connection tab. If you choose a switch port, the Edit Switch Port dialog appears. The Edit button is disabled if the interface is supported and unconfigured.

Delete

Choose a connection and click **Delete.** A dialog box is displayed listing the associations this connection has and giving the option to remove the associations along with the connection. You can delete just the connection or the connection and all of its associations.

Summary

Click the **Summary** button to hide details about the connection, restricting information to the IP address, Type, Slot, Status, and Description.

Details

Click **Details** to display the Details About Interface area. Details about the interface are shown by default.

Enable or Disable

When the chosen interface or connection is down, this appears as the **Enable** button. Click the **Enable** button to bring up the chosen interface or connection. When the chosen interface or connection is up, this appears as the **Disable** button.

Click the **Disable** button to administratively shut down the interface or connection. This button cannot be used with an interface whose configuration was not delivered to the router.

Test Connection

Click **Test Connection** to test the chosen connection. A dialog box is displayed that enables you to specify a remote host to ping through this connection. The dialog box then reports on the success or failure of the test. If the test fails, information about why the test may have failed is given, along with the steps to take to correct the problem.

Interface List

The interface list displays the physical interfaces and the logical connections to which they are configured.

Interfaces

The Interfaces column lists the physical and logical interfaces by name. If a logical interface is configured for a physical interface, the logical interface is shown under the physical interface.

If Cisco CP is running on a Cisco 7000 family router, you can create a connection only on Ethernet and Fast Ethernet interfaces.

IP Address

The IP Address column can contain the following types of IP addresses:

- Configured IP address of the interface.
- DHCP Client—Interface receives an IP address from a Dynamic Host Configuration Protocol (DHCP) server.
- IP address negotiated—Interface receives an IP address through negotiation with the remote device.
- IP unnumbered—Router uses one of a pool of IP addresses supplied by your service provider for your router, and for the devices on the LAN.
- Not Applicable—Interface type cannot be assigned an IP address.

Type

The Type column displays the interface type, such as Ethernet, serial, or ATM.

Slot

The Slot column displays the number of the physical slot in the router that the interface is installed in. If Cisco CP is running on a Cisco 1710 router, the slot field is empty.

Status

This column shows whether this interface is up or down. The green icon with the upward-pointing arrowhead indicates the interface is up. The red icon with the downward-pointing arrowhead indicates that the interface is down.

Description

This column contains any descriptions provided for this connection.

Details About Interface

The Details About Interface area of the window displays association and, if applicable, connection details about the interface chosen in the interface list. Association details include such information as Network Address Translation (NAT), access, inspection rules, IPsec policies, and Easy VPN configurations. Connection details include IP address, encapsulation type, and DHCP options.

Item Name

The Item Name column displays the name of the configuration item, such as IP address/Subnet mask, or IPsec policy. The actual items listed in this column depend on the type of interface chosen.

Item Value

If the named item has a configured value, it is displayed in this column.

Why Are Some Interfaces or Connections Read-Only?

There are many conditions that can prevent Cisco CP from modifying a previously configured interface or subinterface.

- Serial interface or subinterface appears as read-only in the interface list, see "Reasons Why a Serial Interface or Subinterface Configuration May Be Read-Only" section on page 97-24.

- ATM interface or subinterface appears as read-only in the interface list, see "Reasons Why an ATM Interface or Subinterface Configuration May Be Read-Only" section on page 97-25.
- Ethernet LAN or WAN interface appears as read-only in the interface list, see "Reasons Why an Ethernet Interface Configuration May Be Read-Only" section on page 97-26.
- ISDN BRI interface appears as read-only in the interface list, see "Reasons Why an ISDN BRI Interface Configuration May Be Read-Only" section on page 97-27.

Connection: Ethernet for IRB

The Connection dialog box contains the following fields if you chose **Ethernet for IRB** in the Configure list.

Current Bridge Group/Associated BVI

These read-only fields contain the current bridge group value and the current Bridge-Group Virtual Interface (BVI) name.

Create a new Bridge Group/Join an existing Bridge Group

Choose whether to make this interface a member of a new bridge group, or join an existing bridge group. To create a new bridge group, enter a number from range 1 to 255. To have the interface join an existing bridge group, choose the BVI interface that is already a member of that group.

IP Address

Enter the IP address and subnet mask in the fields provided.

Dynamic DNS

Enable dynamic DNS if you want to update your DNS servers automatically whenever the WAN interface IP address changes.

Note This feature appears only if it is supported by the Cisco IOS release on your router.

To choose a dynamic DNS method to use, do one of the following:

- Enter the name of an existing dynamic DNS method.

  Enter the name in the **Dynamic DNS Method** field exactly as it appears in the list in **Configure > Router > DNS> Dynamic DNS Methods**.

- Choose an existing dynamic DNS method from a list.

  Click the drop-down menu and choose an existing method. A window with a list of existing dynamic DNS methods opens. This menu choice is available only if there are existing dynamic DNS methods.

- Create a new dynamic DNS method.

  Click the drop-down menu and choose to create a new dynamic DNS method.

To clear an associated dynamic DNS method from the interface, choose **None** from the drop-down menu.

Connection: Ethernet for Routing

The Connection dialog box contains the following fields if you chose **Ethernet for Routing** in the Configure list.

IP Address

Enter an IP address and subnet mask in the IP Address fields. This address is the source IP address for traffic originating from this interface, and the destination IP address for traffic destined for hosts connected to this interface.

DHCP Relay

Click to enable the router to act as a DHCP relay. A device acting as a DHCP relay forwards DHCP requests to a DHCP server. When a device needs to have an IP address dynamically assigned, it broadcasts a DHCP request. A DHCP server replies to this request with an IP address. You can have a maximum of one DHCP relay or one DHCP server per subnetwork.

Note If the router was configured to be a DHCP relay and to have more than one remote DHCP server IP address, these fields are disabled.

IP Address of Remote DHCP Server

Enter the IP address of the DHCP server that will provide addresses to devices on the LAN.

Dynamic DNS

Enable dynamic DNS to update your DNS servers automatically whenever the WAN interface IP address changes.

Note This feature appears only if supported by the Cisco IOS release on your router.

To choose a dynamic DNS method to use, do one of the following:

- Enter the name of an existing dynamic DNS method.

  Enter the name in the **Dynamic DNS Method** field exactly as it appears in the list in **Configure > Router > DNS > Dynamic DNS Methods**.

- Choose an existing dynamic DNS method from a list.

  Click the drop-down menu and choose an existing method. A window with a list of existing dynamic DNS methods opens. This menu choice is available only if there are existing dynamic DNS methods.

- Create a new dynamic DNS method.

  Click the drop-down menu and choose to create a new dynamic DNS method.

To clear an associated dynamic DNS method from the interface, choose **None** from the drop-down menu.

Existing Dynamic DNS Methods

The Existing Dynamic DNS Methods window allows you to choose a dynamic DNS method to associate with a WAN interface.

The list of existing dynamic DNS methods shows the name of each method and the associated parameters. Choose a method from the list, and click **OK** to associate it to the WAN interface.

To add, edit, or delete dynamic DNS methods, go to **Configure > Router > DNS > Dynamic DNS Methods**.

Add Dynamic DNS Method

This window allows you to add a dynamic DNS method. Choose the type of method, HTTP or IETF, and configure it.

HTTP

HTTP is a dynamic DNS method that updates a DNS service provider with changes to the associated interface's IP address.

Server

If using HTTP, choose the domain address of the DNS service provider from the drop-down menu.

Username

If using HTTP, enter a username for accessing the DNS service provider.

Password

If using HTTP, enter a password for accessing the DNS service provider.

IETF

IETF is a dynamic DNS method that updates a DNS server with changes to the associated interface's IP address.

DNS Server

If using IETF, and no DNS server is configured for the router in **Configure > Router > DNS**, then enter the IP address of your DNS server.

Hostname

Enter a hostname if one is not configured in **Configure > Router > Router Options > Edit > Host**, or to override the configured hostname. When updating the interface IP address, the dynamic DNS method sends the hostname along with the interface's new IP address.

Domain Name

Enter a domain name if one is not configured in **Configure > Router Options > Edit > Domain**, or if you want to override the configured domain name. When updating the interface IP address, the dynamic DNS method sends the domain name along with the interface's new IP address.

Media Type

Use this window to change the media type of the SFP interface.

Media-type

Choose RJ45 or Pluggable Media (SFP) from the media-type drop-down menu. Select the Enable Auto-failover check box if you want to activate automatic fail-over - if the selected media-type does not work, the other media-type will automatically be used.

Speed

Choose Auto, 10 Mbps, 100 Mbps, or 1000 Mbps as the speed of the interface from the Speed drop-down menu.

Duplex

Choose Auto, Full, or Half from the Duplex drop-down menu.

Click OK after making changes. A message is displayed informing you that the media-type is changed and that you may need to change the speed and duplex settings of the interface.

Wireless

If the router has a wireless interface, you can launch the wireless application from this tab. You can also launch the wireless application from the Tools menu by choosing **Tools > Launch Wireless Application**.

Association

Use this window to view, create, edit, or delete associations between interfaces and rules or VPN connections.

Interface

The Interface column displays the name of the interface you selected in the Interfaces and Connections window.

Zone

If this interface is a member of a security zone, the name of the zone is displayed in this field. To include this interface in a security zone, click the button to the right of the field, choose **Select a Zone**, and specify the zone in the displayed dialog. To create a new zone, choose **Create a Zone**, enter a name for the zone in the displayed dialog box, and click **OK**. The name of the zone you created appears in the Zone field.

Access Rule

The names or numbers of any access rules associated with this interface. Access rules permit or deny traffic that matches the IP address and service criteria specified in the rule.

Inbound

The name or number of an access rule applied to inbound traffic on this interface. To apply a rule, click the **...** button and either choose an existing rule or create a rule and choose it.

When a rule is applied to inbound traffic on an interface, the rule filters traffic before it enters the router. Any packet that the rule does not permit is dropped and is not routed to another interface. When you apply a rule to the inbound direction on an interface, you are not only preventing it from entering a trusted network connected to the router, you are also preventing it from being routed anywhere else by the local router.

Outbound

The name or number of an access rule applied to outbound traffic on this interface. To apply a rule, click the **...** button and either choose an existing rule or create a rule and choose it.

When a rule is applied to outbound traffic on an interface, the rule filters traffic after it enters the router and before it exits the interface. Any packet that the rule does not permit is dropped before it leaves the interface.

Inspect Rule

The names of inspection rules associated with this interface. Inspection rules create temporary holes in firewalls so that hosts inside the firewall that started sessions of a certain type can receive return traffic of the same type.

Inbound

The name or number of an inspection rule applied to inbound traffic on this interface. To apply an inbound rule, click the **Inbound** drop-down menu and choose a rule.

Outbound

The name or number of an inspection rule applied to outbound traffic on this interface. To apply an outbound rule, click the **Outbound** drop-down menu and choose a rule.

VPN

VPNs protect traffic that may flow over lines that your organization does not control. You can use the chosen interface in a VPN by associating it with an IPsec policy.

IPsec Policy

The configured IPsec policy associated with this interface. To associate the interface with an IPsec policy, choose the policy from this list.

Note An interface can be associated with only one IPsec policy.

Note To create a GRE-over-IPsec Tunnel, you must first associate the policy with the tunnel interface, and then associate it with the source interface for the tunnel. For example, if you wanted to associate a policy with Tunnel3, whose source interface is Serial0/0, you would first choose Tunnel3 in the Interfaces and Connections window, click **Edit** and associate the policy with it, and then click **OK**. Then you would choose the Serial0/0 interface and associate the same policy with it.

EzVPN

If the interface is used in an Easy VPN connection, the name of the connection is shown here.

Note An interface cannot be used in both a virtual private network (VPN) connection and an Easy VPN connection.

Making Association Changes

When you change the association properties of an interface, the changes are reflected in the lower portion of the Edit Interface/Connection window. For example, if you associate an IPsec policy with the interface, the name of the IPsec policy appears in the lower portion of the window. If you delete an association, the value in the Item Value column changes to <None>.

NAT

If you intend to use this interface in a NAT configuration, you must designate it as either an inside or an outside interface. Choose the traffic direction to which NAT is to be applied. If the interface connects to a LAN that the router serves,

choose **Inside**. If it connects to the Internet or to your WAN, choose **Outside**. If you have chosen an interface that cannot be used in a NAT configuration, such as a logical interface, this field is disabled and contains the value Not Supported.

Edit Switch Port

This window lets you edit VLAN information for Ethernet switch ports.

Mode Group

Choose the type of VLAN information you want to be carried across this Ethernet switch port. Choosing **Access** causes the switch port to forward only data destined for the specific VLAN number. Choosing **Trunking** causes the switch port to forward data for all VLANs, including the VLAN data itself. Choose **Trunking** only for "trunking" VLAN ports that connect to other networking devices, such as another switch, that will connect to devices in multiple VLANs.

VLAN

To assign the switch port to a VLAN, enter the VLAN number to which this switch port should belong. If the switch port does not already have a VLAN associated with it, this field will show the default value VLAN 1. To create a new VLAN interface corresponding to a VLAN ID, enter that VLAN ID and check the **Make VLAN visible to interface list** check box.

Make VLAN visible to interface list Check Box

Check this check box to create a new VLAN with the VLAN ID specified in the VLAN field.

Stacking Partner

Choose a switch module as the stacking partner to use. When a device contains multiple switching modules, these must be stacked before other stacking partners.

Bridge Group Number

If you want this switch port to form part of a bridge to a wireless network, enter the number of an existing bridge group.

Speed

Choose the speed to match the network to which the switch port will be connected. Or choose **auto** to allow for the speed to be automatically set to the optimal value.

Duplex

Choose **full**, **half**, or **auto** to allow for the duplex to be automatically set to match the network to which the switch port will be connected.

If **Speed** is set to **auto**, then **Duplex** is disabled.

Power Inline

The **Power inline** drop-down list appears if the switch port supports an inline power supply. Choose one of the following values:

- **auto**—Automatically detect and power inline devices.
- **never** —Never apply inline power.

Application Service

This window allows you to associate Quality of Service (QoS) policies, application, and protocol monitoring with the chosen interface.

QoS

To associate a QoS policy with the interface in the inbound direction, choose a QoS policy from the **Inbound** drop-down menu.

To associate a QoS policy with the interface in the outbound direction, choose a QoS policy from the **Outbound** drop-down menu.

To enable the QoS feature on the DMVPN tunnel interface, use the QoS wizard. Go to **Configure > Router > QoS**. The Quality of Service page opens with the Create QoS Policy tab selected by default. Click the **Launch QoS Wizard** button to start the QoS wizard.

You can monitor QoS statistics for the interface. Go to **Monitor > Router > QoS Status**.

Netflow

To associate Netflow statistics monitoring with the interface in the inbound direction, check the **Inbound** check box.

To associate Netflow statistics monitoring with the interface in the outbound direction, check the **Outbound** check box.

Netflow statistics for the interface can be monitored by going to **Monitor > Router > Interface Status**. Netflow top talkers and top protocols can be monitored by going to **Monitor > Router > Traffic Status > Top N Traffic Flows**.

NBAR

To associate Network-based application recognition (NBAR) with the interface, check the **NBAR Protocol** check box.

NBAR statistics for the interface can be monitored by going to **Monitor > Router > Traffic Status > Application/Protocol Traffic**.

General

This window displays general security settings and allows you to enable or disable them by checking or unchecking the check box next to the name and description. If you have allowed the Security Audit feature to disable certain properties and want to reenable them, you can reenable them in this window. The properties listed in this window follow.

Description

In this field you can enter a short description of the interface configuration. This description is visible in the Edit Interfaces and Connections window. A description, such as “Accounting” or “Test Net 5” can help other Cisco CP users understand the purpose of the configuration.

IP Directed Broadcasts

An IP directed broadcast is a datagram that is sent to the broadcast address of a subnet to which the sending machine is not directly attached. The directed broadcast is routed through the network as a unicast packet until it arrives at the target subnet, where it is converted into a link-layer broadcast. Because of the nature of the IP addressing architecture, only the last router in the chain, the one that is connected directly to the target subnet, can conclusively identify a directed broadcast. Directed broadcasts are occasionally used for legitimate purposes, but such use is not common outside the financial services industry.

IP directed broadcasts are used in the common and popular “smurf” denial of service attack, and they can also be used in related attacks. In a “smurf” attack, the attacker sends ICMP echo requests from a falsified source address to a directed broadcast address, causing all the hosts on the target subnet to send replies to the falsified source. By sending a continuous stream of such requests, the attacker can create a much larger reply stream, which can completely inundate the host whose address is being falsified.

Disabling IP directed broadcasts drops directed broadcasts that would otherwise be “exploded” into link-layer broadcasts at that interface.

IP Proxy ARP

ARP is used by the network to convert IP addresses into MAC addresses. Normally ARP is confined to a single LAN, and a router can act as a proxy for ARP requests, making ARP queries available across multiple LAN segments. Because it breaks the LAN security barrier, proxy ARP should be used only between two LANs with an equal security level, and only when necessary.

IP Route Cache-Flow

This option enables the Cisco IOS Netflow feature. Using Netflow, you can determine packet distribution, protocol distribution, and current flows of data on the router. This information is useful for certain tasks, such as searching for the source of a spoofed IP address attack.

Note The IP Route Cache-Flow option enables Netflow on both inbound and outbound traffic. To enable Netflow on either inbound traffic *or* outbound traffic, use the Netflow options available on the Application Service tab.

IP Redirects

ICMP redirect messages instruct an end node to use a specific router as a part of its path to a particular destination. In a properly functioning IP network, a router sends redirects only to hosts on its own local subnets, no end node will ever send a redirect, and no redirect will ever traverse more than one network hop. However, an attacker may violate these rules. Disabling ICMP redirects has no negative impact on the network and can eliminate redirect attacks.

IP Mask-Reply

ICMP mask reply messages are sent when a network device must know the subnet mask for a particular subnetwork in the internetwork. ICMP mask reply messages are sent to the device requesting the information by devices that have the requested information. These messages can be used by an attacker to gain network mapping information.

IP Unreachables

ICMP host unreachable messages are sent if a router receives a nonbroadcast packet that uses an unknown protocol, or if the router receives a packet that it is unable to deliver to the ultimate destination because it knows of no route to the destination address. These messages can be used by an attacker to gain network mapping information.

Select Ethernet Configuration Type

This window is displayed when you click an interface in the Interfaces and Connections window and Cisco CP cannot determine whether the interface is configured as a LAN interface or as a WAN interface. When you configure an interface using Cisco CP, you designate it as an inside or outside interface, and Cisco CP adds a descriptive comment to the configuration file based on your designation. If you configure an interface using the CLI, the configuration will not include this descriptive comment, and Cisco CP will not have this information.

To Indicate that the Interface is a LAN Interface:

Click **LAN**, and then click **OK**. Cisco CP adds the comment line $ETH-LAN$ to the interface configuration, and the interface appears in the LAN wizard window with the designation Inside in the Interfaces and Connections window.

To Indicate that the Interface is a WAN Interface:

Click **WAN**, and then click **OK**. Cisco CP adds the comment line $ETH-WAN$ to the interface configuration, and the interface appears in the WAN wizard window with the designation Outside in the Interfaces and Connections window.

Connection: VLAN

This window lets you configure a VLAN interface.

VLAN ID

Enter the ID number of the new VLAN interface. If you are editing a VLAN interface, you cannot change the VLAN ID.

Native VLAN Check Box

Check if this VLAN is a nontrunking VLAN.

IP Address Fields

IP Address Type

Choose whether this VLAN interface will have a static IP address or no IP address. This field is visible when **VLAN only** is chosen in the Configure As field.

IP Address

Enter the IP address of the VLAN interface.

Subnet Mask

Enter the subnet mask of the VLAN interface, or indicate the number of subnet bits using the scrolling field.

DHCP Relay

Click DHCP Relay for more information.

Subinterfaces List

This window displays the subinterfaces configured for the interface that you chose, and enables you to add, edit, and remove configured subinterfaces. For each configured subinterface, the window displays the Subinterface ID, VLAN ID, IP address and mask, and a description, if one was entered. For example, if the router had the interface FastEthernet1, and the subinterfaces FastEthernet1.3 and FastEthernet1.5 are configured, this window might contain the following display

```
5       56      56.8.1.1/255.255.255.0
3       67      Bridge No. 77
```

In this example, FastEthernet1.5 is configured for routing, and FastEthernet1.3 is configured for IRB.

Note You must choose the physical interface on which the subinterfaces are configured to display this window. For the example described, you would have to choose FastEthernet1 to display this window. If you choose FastEthernet1.3 or FastEthernet1.5 and click edit, you display the edit dialog box with the information for that interface.

Add, Edit, and Delete Buttons

Use these buttons to configure, edit, and remove subinterfaces from the chosen physical interface.

Add or Edit BVI Interface

Add or edit a Bridge Group Virtual Interface (BVI) in this window. If your router has a Dot11Radio interface, a BVI is automatically created when you configure a new bridge group. This is done to support IRB bridging. You can change the IP address and subnet mask in this window.

IP Address/Subnet Mask

Enter the IP address and subnet mask that you want to give the BVI.

Add or Edit Loopback Interface

This window enables you to add a loopback interface to the chosen interface.

IP Address

Choose whether the loopback interface is to have no IP address or a static IP address.

Static IP Address

If you chose **Static IP address**, enter that IP address in this field.

Subnet Mask

Enter the subnet mask in this field, or choose the number of subnet bits from the field on the right. The subnet mask tells the router which bits of the IP address designate the network address and which bits designate the host address.

Connection: Virtual Template Interface

You can add or edit a VTI as part of an 802.1x or VPN configuration. When you are editing a VTI, the fields that you can edit appear in a Connection tab.

Interface Type

Choose either **default** or **tunnel**. If you choose tunnel, you must also select a tunnel mode.

IP Address

Choose **Unnumbered**. The VTI uses the IP address of the physical interface that is chosen in the Unnumbered to field.

Unnumbered to

This field appears when you choose **Unnumbered** in the IP Address field. Choose the interface whose IP address you want this VTI to use.

Tunnel Mode

Choose **IPSec-IPv4**.

Connection: Ethernet LAN

Use this window to configure the IP address and DHCP properties of an Ethernet interface that you want to use as a LAN interface.

IP Address

Enter the IP address for this interface. Obtain the IP address value from your service provider or network administrator. For more information, see IP Addresses and Subnet Masks.

Subnet Mask

Enter the subnet mask. Obtain this value from your network administrator. The subnet mask enables the router to determine how much of the IP address is used to define the network and subnet portion of the address.

DHCP Relay

Click to enable the router to act as a DHCP relay. A device acting as a DHCP relay forwards DHCP requests to a DHCP server. When a device needs to have an IP address dynamically assigned, it broadcasts a DHCP request. A DHCP server replies to this request with an IP address. You can have a maximum of one DHCP relay or one DHCP server per subnetwork.

Note If the router was configured to be a DHCP relay with more than one remote DHCP server IP address, this button is disabled.

IP Address of Remote DHCP Server

If you clicked **DHCP Relay**, enter the IP address of the DHCP server that will provide addresses to devices on the LAN.

Connection: Ethernet WAN

This window lets you add an Ethernet WAN connection.

Enable PPPoE Encapsulation

Click this option if the connection must use Point-to-Point Protocol over Ethernet (PPPoE) encapsulation. Your service provider can tell you whether the connection uses PPPoE. When you configure a PPPoE connection, a dialer interface is automatically created.

IP Address

Choose one of the following IP address types, and enter the information in the fields displayed. If the Ethernet connection is not using PPPoE, you will see only the Static IP address and Dynamic options.

Static IP Address

If you choose **Static IP Address**, enter the IP address and subnet mask or the network bits in the fields provided. For more information, see IP Addresses and Subnet Masks.

Dynamic (DHCP Client)

If you choose **Dynamic**, the router will lease an IP address from a remote DHCP server. Enter the name of the DHCP server from which addresses will be leased.

IP Unnumbered

Choose **IP Unnumbered** if you want the interface to share an IP address that is already assigned to another interface, choose the interface whose IP address this interface is to share.

Easy IP (IP Negotiated)

Choose Easy IP (IP Negotiated) if the router will obtain an IP address through Point-to-Point Protocol/IP Control Protocol (PPP/IPCP) address negotiation.

Authentication

Click to enter CHAP/PAP authentication password information.

Dynamic DNS

Enable dynamic DNS if you want to update your DNS servers automatically whenever the WAN interface IP address changes.

Note This feature appears only if supported by the Cisco IOS release on your router.

To choose a dynamic DNS method to use, do one of the following:

- Enter the name of an existing dynamic DNS method.

Enter the name in the **Dynamic DNS Method** field exactly as it appears in the list in **Configure > Router > DNS > Dynamic DNS Methods**.

- Choose an existing dynamic DNS method from a list.

  Click the drop-down menu and choose an existing method. A window with a list of existing dynamic DNS methods opens. This menu choice is available only if there are existing dynamic DNS methods.

- Create a new dynamic DNS method.

  Click the drop-down menu and choose to create a new dynamic DNS method.

To clear an associated dynamic DNS method from the interface, choose **None** from the drop-down menu.

Connection: Ethernet Properties

This window enables you to configure properties for an Ethernet WAN link.

Enable PPPoE Encapsulation

Click **Enable PPPoE encapsulation** if your service provider requires that you use it. PPPoE specifies Point-to-Point Protocol over Ethernet encapsulation.

IP Address

Static IP Address

Available with PPPoE encapsulation and with no encapsulation. If you choose **Static IP Address**, enter the IP address and subnet mask or the network bits in the fields provided. For more information, see IP Addresses and Subnet Masks.

Dynamic (DHCP Client)

Available with PPPoE encapsulation and with no encapsulation. If you choose **Dynamic**, the router will lease an IP address from a remote DHCP server. Enter the name of the DHCP server that will assign addresses.

IP Unnumbered

Available with PPPoE encapsulation. Choose **IP Unnumbered** if you want the interface to share an IP address that has already been assigned to another interface. Then choose the interface whose IP address this interface is to share.

Easy IP (IP Negotiated)

Available with PPPoE encapsulation. Choose **Easy IP (IP Negotiated)** if the router will obtain an IP address using PPP/IPCP address negotiation.

Authentication

Click to enter CHAP/PAP authentication password information.

Dynamic DNS

Enable dynamic DNS if you want to update your DNS servers automatically whenever the WAN interface IP address changes.

Note This feature appears only if supported by the Cisco IOS release on your router.

To choose a dynamic DNS method to use, do one of the following:

- Enter the name of an existing dynamic DNS method.

  Enter the name in the **Dynamic DNS Method** field exactly as it appears in the list in **Configure > Router > DNS > Dynamic DNS Methods**.

- Choose an existing dynamic DNS method from a list.

  Click the drop-down menu and choose an existing method. A window with a list of existing dynamic DNS methods opens. This menu choice is available only if there are existing dynamic DNS methods.

- Create a new dynamic DNS method.

  Click the drop-down menu and choose to create a new dynamic DNS method.

To clear an associated dynamic DNS method from the interface, choose **None** from the drop-down menu.

Connection: Ethernet with No Encapsulation

Use this window to configure an Ethernet connection with no encapsulation.

IP Address

Choose how the router will obtain an IP address for this link.

- Static IP address—If you choose **Static IP Address**, enter the IP address and subnet mask or network bits in the fields provided. For more information, see IP Addresses and Subnet Masks.
- Dynamic IP address—If you choose **Dynamic**, the router will lease an IP address from a remote DHCP server. Enter the name or IP address of the DHCP server.

Hostname

If your service provider inserts a hostname for the router into the DHCP response that contains the dynamic IP address, you can enter that name in this field for informational purposes.

Dynamic DNS

Enable dynamic DNS if you want to update your DNS servers automatically whenever the WAN interface IP address changes.

Note This feature appears only if supported by the Cisco IOS release on your router.

To choose a dynamic DNS method to use, do one of the following:

- Enter the name of an existing dynamic DNS method.

  Enter the name in the **Dynamic DNS Method** field exactly as it appears in the list in **Configure > Router > DNS > Dynamic DNS Methods**.
- Choose an existing dynamic DNS method from a list.

  Click the drop-down menu and choose an existing method. A window with a list of existing dynamic DNS methods opens. This menu choice is available only if there are existing dynamic DNS methods.
- Create a new dynamic DNS method.

Click the drop-down menu and choose to create a new dynamic DNS method.

To clear an associated dynamic DNS method from the interface, choose **None** from the drop-down menu.

Connection: ADSL

This window enables you to specify or edit properties of a PPPoE link supported by an ADSL connection.

Encapsulation

Choose the type of encapsulation that will be used for this link.

- PPPoE specifies Point-to-Point Protocol over Ethernet encapsulation.
- PPPoA specifies Point-to-Point Protocol over ATM encapsulation.
- RFC 1483 Routing (AAL5 SNAP) specifies that each PVC can carry multiple protocols.
- RFC 1483 Routing (AAL5 MUX) specifies that each PVC can carry only one type of protocol.

If you are editing a connection, the encapsulation is shown, but not editable. If you need to change the encapsulation type, delete the connection and re-create it using the encapsulation type you need.

For more information on these encapsulation types, click Encapsulation Autodetect.

Virtual Path Identifier

The virtual path identifier (VPI) is used in ATM switching and routing to identify the path used for a number of connections. Enter the VPI value given to you by your service provider.

If you are editing an existing connection, this field is disabled. If you need to change this value, delete the connection and re-create it using the value you need.

Virtual Circuit Identifier

The virtual circuit identifier (VCI) is used in ATM switching and routing to identify a particular connection within a path that your connection may share with other connections. Enter the VCI value given to you by your service provider.

If you are editing an existing connection, this field is disabled. If you need to change this value, delete the connection and re-create it using the value you need.

IP Address

Choose how the router will obtain an IP address for this link.

- Static IP address—If you choose **Static IP Address**, enter the IP address and subnet mask, or network bits in the fields provided. For more information, see IP Addresses and Subnet Masks.
- Dynamic IP address—If you choose **Dynamic**, the router will lease an IP address from a remote DHCP server. Enter the name or IP address of the DHCP server.
- Unnumbered IP address—Choose **IP Unnumbered** if you want the interface to share an IP address that has already been assigned to another interface. Choose the interface whose IP address this interface is to share.
- IP Negotiated—This interface will obtain an IP address using PPP/IP Control Protocol (IPCP) address negotiation.

Hostname

If your service provider has provided a hostname for DHCP option 12, enter it here.

Operating Mode

Choose one of the following values:

- **auto**—Configure the Asymmetric Digital Subscriber Line (ADSL) after autonegotiating with the digital subscriber access line multiplexer (DSLAM) located at the central office.
- a**nsi-dmt**—Configure the ADSL line to train in the ANSI T1.413 Issue 2 mode.
- **itu-dmt**—Configure the ADSL line to train in the ITU G.992.1 mode.

- **adls2**—Configure the ADSL line to train in the ITU G.992.3 mode. This mode is available for the HWIC-ADSL-B/ST, HWIC-ADSLI-B/ST, HWIC-1ADSL, and HWIC-1ADSLI ADSL network modules.
- **adsl2+**—Configure the ADSL line to train in the ITU G.992.4 mode. This mode is available for the HWIC-ADSL-B/ST, HWIC-ADSLI-B/ST, HWIC-1ADSL, and HWIC-1ADSLI ADSL network modules.
- **splitterless**—Configure the ADSL line to train in the G.Lite mode. This mode is available for older ADSL network modules such as the WIC-1ADSL.

Authentication

Click if you need to enter CHAP or PAP authentication information.

Dynamic DNS

Enable dynamic DNS if you want to update your DNS servers automatically whenever the WAN interface IP address changes.

Note This feature appears only if supported by the Cisco IOS release on your router.

To choose a dynamic DNS method to use, do one of the following:

- Enter the name of an existing dynamic DNS method.

  Enter the name in the **Dynamic DNS Method** field exactly as it appears in the list in **Configure > Router > DNS > Dynamic DNS Methods**.
- Choose an existing dynamic DNS method from a list.

  Click the drop-down menu and choose an existing method. A window with a list of existing dynamic DNS methods opens. This menu choice is available only if there are existing dynamic DNS methods.
- Create a new dynamic DNS method.

  Click the drop-down menu and choose to create a new dynamic DNS method.

To clear an associated dynamic DNS method from the interface, choose **None** from the drop-down menu.

Enable Multilink PPP

Check this check box if you want to use Multilink Point-to-Point Protocol (MLP) with this interface. MLP can improve the performance of a network with multiple WAN connections by using load balancing functionality, packet fragmentation, bandwidth-on-demand, and other features.

Connection: ADSL over ISDN

Add or edit an ADSL over ISDN connection in this window.

Encapsulation

Choose the type of encapsulation to use for this link.

- **PPPoE—**Specifies Point-to-Point Protocol over Ethernet encapsulation.
- **RFC 1483 Routing** (**AAL5 SNAP**)—Specifies that each PVC can carry multiple protocols.
- **RFC 1483 Routing** (**AAL5 MUX**)—Specifies that each PVC can carry only one type of protocol.

If you are editing a connection, the encapsulation is shown, but not editable. If you need to change the encapsulation type, delete the connection and re-create it using the encapsulation type you need.

Virtual Path Identifier

The virtual path identifier (VPI) is used in ATM switching and routing to identify the path used for a number of connections. Obtain this value from your service provider.

If you are editing an existing connection, this field is disabled. If you need to change this value, delete the connection and re-create it using the value you need.

Virtual Circuit Identifier

The virtual circuit identifier (VCI) is used in ATM switching and routing to identify a particular connection within a path that your connection may share with other connections. Obtain this value from your service provider.

If you are editing an existing connection, this field is disabled. If you need to change this value, delete the connection and re-create it using the value you need.

IP Address

Choose how the router will obtain an IP address for this link.

- Static IP address—If you choose **Static IP Address**, enter the IP address and subnet mask, or network bits in the fields provided. For more information, see IP Addresses and Subnet Masks.
- Dynamic IP address—If you choose **Dynamic**, the router will lease an IP address from a remote DHCP server. Then enter the name or IP address of the DHCP server.
- Unnumbered IP address—Choose **IP Unnumbered** for the interface to share an IP address that has already been assigned to another interface. Then choose the interface whose IP address this interface is to share.
- IP Negotiated—This interface will obtain an IP address using PPP/IP Control Protocol (IPCP) address negotiation.

Operating Mode

Choose the mode that the ADSL line should use when training.

Note If the Cisco IOS release you are running on the router does not support all five operating modes, you will see options only for the operating modes supported by your Cisco IOS release.

- **annexb**—Standard Annex-B mode of ITU-T G.992.1.
- **annexb-ur2**—ITU-T G.992.1 Annex-B mode.
- **auto**—Configure the ADSL line after autonegotiating with the digital subscriber access line multiplexer (DSLAM) located at the central office.

- **etsi**—European Telecommunications Standards Institute mode.
- **multimode**—Mode chosen by the firmware for the best operating condition on DSL. The final mode can be either ETSI mode or standard Annex-B mode depending on the current DSLAM setting.

Authentication

Click if you need to enter CHAP or PAP authentication information.

Dynamic DNS

Enable dynamic DNS if you want to update your DNS servers automatically whenever the WAN interface IP address changes.

Note This feature appears only if supported by the Cisco IOS release on your router.

To choose a dynamic DNS method to use, do one of the following:

- Enter the name of an existing dynamic DNS method.

  Enter the name in the **Dynamic DNS Method** field exactly as it appears in the list in **Configure > Router > DNS > Dynamic DNS Methods**.

- Choose an existing dynamic DNS method from a list.

  Click the drop-down menu and choose an existing method. A window with a list of existing dynamic DNS methods opens. This menu choice is available only if there are existing dynamic DNS methods.

- Create a new dynamic DNS method.

  Click the drop-down menu and choose to create a new dynamic DNS method.

To clear an associated dynamic DNS method from the interface, choose **None** from the drop-down menu.

Enable Multilink PPP

Check this check box if you want to use MLP with this interface. MLP can improve the performance of a network with multiple WAN connections by using load balancing functionality, packet fragmentation, bandwidth-on-demand, and other features.

Connection: G.SHDSL

This window enables you to create or edit a G.SHDSL connection.

Note If the connection that you are configuring uses a DSL controller, the Equipment Type and Operating Mode fields do not appear in the dialog.

Encapsulation

Choose the type of encapsulation that will be used for this link.

- **PPPoE**—Specifies Point-to-Point Protocol over Ethernet encapsulation.
- **PPPoA—**Specifies Point-to-Point Protocol over ATM encapsulation.
- **RFC 1483 Routing** (**AAL5 SNAP**)—Specifies that each PVC can carry multiple protocols.
- **RFC 1483 Routing** (**AAL5 MUX**)—Specifies that each PVC can carry only one type of protocol.

If you are editing a connection, the encapsulation is shown, but not editable. If you need to change the encapsulation type, delete the connection and re-create it using the encapsulation type you need.

For more information on these encapsulation types, click Encapsulation Autodetect.

Virtual Path Identifier

The virtual path identifier (VPI) is used in ATM switching and routing to identify the path used for a number of connections. Obtain this value from your service provider.

If you are editing an existing connection, this field is disabled. If you need to change this value, delete the connection and re-create it using the value you need.

Virtual Circuit Identifier

The virtual circuit identifier (VCI) is used in ATM switching and routing to identify a particular connection within a path that your connection may share with other connections. Obtain this value from your service provider.

If you are editing an existing connection, this field is disabled. If you need to change this value, delete the connection and re-create it using the value you need.

IP Address

Choose how the router will obtain an IP address for this link. The fields that appear in this area change according to the encapsulation type chosen. Your service provider or network administrator must tell you the method the router should use to obtain an IP address.

Static IP address

If you choose **Static IP Address**, enter the address that the interface will use, and the subnet mask or the network bits. Obtain this information from your service provider or network administrator. For more information, see IP Addresses and Subnet Masks.

Dynamic IP address

If you choose Dynamic IP address, the interface will obtain an IP address from a DHCP server on the network. If the DHCP server uses DHCP option 12, it sends a hostname for the router along with the IP address the router is to use. Check with your service provider or network administrator to determine the hostname sent.

IP Unnumbered

Choose this option if you want the interface to share an IP address with an Ethernet interface on the router. If you choose this option, you must specify from the drop-down list the Ethernet interface whose address you want to use.

IP Address for Remote Connection in Central Office

Enter the IP address of the gateway system to which this link will connect. This IP address is supplied by the service provider or network administrator. The gateway is the system to which the router must connect to access the Internet or your WAN.

Equipment Type

Choose one of the values:

CPE

Customer premises equipment. If the encapsulation type is PPPoE, CPE is automatically chosen and the field is disabled.

CO

Central office.

Operating Mode

Choose one of the values:

Annex A (U.S.)

Configures the regional operating parameters for North America.

Annex B (Europe)

Configures the regional operating parameters for Europe.

Enable Multilink PPP

Check this check box if you want to use Multilink Point-to-Point Protocol (MLP) with this interface. MLP can improve the performance of a network with multiple WAN connections by using load balancing functionality, packet fragmentation, bandwidth-on-demand, and other features.

Authentication

Click if you need to enter CHAP or PAP authentication information.

Dynamic DNS

Enable dynamic DNS if you want to update your DNS servers automatically whenever the WAN interface IP address changes.

Note This feature appears only if supported by the Cisco IOS release on your router.

To choose a dynamic DNS method to use, do one of the following:

- Enter the name of an existing dynamic DNS method.

  Enter the name in the **Dynamic DNS Method** field exactly as it appears in the list in **Configure > Router > DNS > Dynamic DNS Methods**.

- Choose an existing dynamic DNS method from a list.

  Click the drop-down menu and choose an existing method. A window with a list of existing dynamic DNS methods opens. This menu choice is available only if there are existing dynamic DNS methods.

- Create a new dynamic DNS method.

  Click the drop-down menu and choose to create a new dynamic DNS method.

To clear an associated dynamic DNS method from the interface, choose **None** from the drop-down menu.

Connection: Cable Modem

Use this dialog to change the default IP address of the cable modem service module.

Field Description

Table 6-1 Cable Modem

Element	Description
Change the default service module IP address	
Check box	Check the **Change the default service module IP address** check box to change the default IP address of this service module.

Table 6-1 Cable Modem

Element	Description
IP Address	Enter the IP address in dotted decimal format. For example, 192.168.4.5
Subnet Mask	Enter the subnet mask in decimal format, or choose the number of bits to include in the subnet mask. An example of a subnet mask in decimal format is 255.255.255.0. That subnet mask value is equivalent to 24 bits. Use the up arrow and the down arrow to choose the number of bits. If you enter a decimal value, the bit value is automatically updated. If you enter a bit value, the decimal value is automatically updated.

Connection: Serial Interface, Frame Relay Encapsulation

Complete these fields if you are configuring a serial subinterface for Frame Relay encapsulation. If you are editing a connection or creating a connection in the Edit Interfaces and Connections window, the encapsulation is shown but is not editable. If you need to change the encapsulation type, delete the connection and re-create it using the encapsulation type you need.

Encapsulation

Frame Relay chosen.

IP Address

Choose either **Static IP address** or **IP unnumbered**.

IP Address

If you chose **Static IP address**, enter the IP address for this interface. Obtain this value from your network administrator or service provider. For more information, see IP Addresses and Subnet Masks.

Subnet Mask

If you chose **Static IP address**, enter the subnet mask. The subnet mask specifies the portion of the IP address that provides the network address. This value is synchronized with the subnet bits. Your network administrator or service provider provides the value of the subnet mask or the network bits.

Subnet Bits

Alternatively, enter the network bits to specify how much of the IP address provides the network address.

IP Unnumbered

If you chose IP unnumbered, the interface will share an IP address that has already been assigned to another interface. Choose the interface whose IP address this interface is to share.

DLCI

Enter the data link connection identifier (DLCI) in this field. This number must be unique among all DLCIs used on this interface. The DLCI provides a unique Frame Relay identifier for this connection.

If you are editing an existing connection, the DLCI field will be disabled. If you need to change the DLCI, delete the connection and create it again.

LMI Type

Ask your service provider which of the following Local Management Interface (LMI) types you should use. The LMI type specifies the protocol used to monitor the connection:

ANSI

Annex D defined by American National Standards Institute (ANSI) standard T1.617.

Cisco

LMI type defined jointly by Cisco and three other companies.

ITU-T Q.933

ITU-T Q.933 Annex A.

Autosense

Default. This setting allows the router to detect which LMI type is used by the switch and then use that type. If autosense fails, the router will use the Cisco LMI type.

Use IETF Frame Relay Encapsulation

Check this check box to use Internet Engineering Task Force (IETF) encapsulation. This option is used to connect with routers not from Cisco. Check this box if you are connecting to a router not from Cisco on this interface.

Clock Settings

In most cases, clock settings should not be changed from the default values. If you know that your requirements are different from the defaults, click and adjust the clock settings in the window displayed.

The Clock Settings button appears only if you are configuring a T1 or E1 serial connection.

Dynamic DNS

Enable dynamic DNS if you want to update your DNS servers automatically whenever the WAN interface IP address changes.

Note This feature appears only if supported by the Cisco IOS release on your router.

To choose a dynamic DNS method to use, do one of the following:

- Enter the name of an existing dynamic DNS method.

  Enter the name in the **Dynamic DNS Method** field exactly as it appears in the list in **Configure > Router > DNS> Dynamic DNS Methods**.

- Choose an existing dynamic DNS method from a list.

  Click the drop-down menu and choose an existing method. A window with a list of existing dynamic DNS methods opens. This menu choice is available only if there are existing dynamic DNS methods.

- Create a new dynamic DNS method.

  Click the drop-down menu and choose to create a new dynamic DNS method.

To clear an associated dynamic DNS method from the interface, choose **None** from the drop-down menu.

Connection: Serial Interface, PPP Encapsulation

Complete these fields if you are configuring a serial interface for Point-to-Point Protocol encapsulation. If you are editing a connection or creating a connection in the Edit Interfaces and Connections window, the encapsulation is shown but is not editable. If you need to change the encapsulation type, delete the connection and re-create it using the encapsulation type you need.

Encapsulation

PPP chosen.

IP Address

Choose **Static IP Address**, **IP Unnumbered**, or **IP Negotiated**. If you choose **IP Unnumbered**, choose the interface whose IP address this interface is to share. If you choose **IP Negotiated**, the router obtains an IP address from the service provider for this interface. If you choose **Specify an IP address**, complete the fields below.

IP Address

Enter the IP address for this point-to-point subinterface. Obtain this value from your network administrator or service provider. For more information, see IP Addresses and Subnet Masks.

Subnet Mask

Enter the subnet mask. The subnet mask specifies the portion of the IP address that provides the network address. This value is synchronized with the network bits. Obtain the value of the subnet mask or the network bits from your network administrator or service provider.

Subnet Bits

Alternatively, enter the network bits to specify how many bits in the IP address provide the network address.

Authentication

Click if you need to enter CHAP or PAP authentication information.

Clock Settings

In most cases, clock settings should not be changed from the default values. If you know that your requirements are different from the defaults, click and adjust the clock settings in the window displayed.

The Clock Settings button appears only if you are configuring a T1 or E1 serial connection.

Dynamic DNS

Enable dynamic DNS if you want to update your DNS servers automatically whenever the WAN interface IP address changes.

Note This feature appears only if supported by the Cisco IOS release on your router.

To choose a dynamic DNS method to use, do one of the following:

- Enter the name of an existing dynamic DNS method.

  Enter the name in the **Dynamic DNS Method** field exactly as it appears in the list in **Configure > Router > DNS > Dynamic DNS Methods**.

- Choose an existing dynamic DNS method from a list.

  Click the drop-down menu and choose an existing method. A window with a list of existing dynamic DNS methods opens. This menu choice is available only if there are existing dynamic DNS methods.

- Create a new dynamic DNS method.

  Click the drop-down menu and choose to create a new dynamic DNS method.

To clear an associated dynamic DNS method from the interface, choose **None** from the drop-down menu.

Connection: Serial Interface, HDLC Encapsulation

Fill out these fields if you are configuring a serial interface for HDLC encapsulation. If you are editing a connection or creating a connection in the Edit Interfaces and Connections window, the encapsulation is shown but is not editable. If you need to change the encapsulation type, delete the connection and re-create it using the encapsulation type you need.

Encapsulation

HDLC chosen.

IP Address

Choose either **Static IP address** or **IP Unnumbered**. If you choose **IP Unnumbered**, choose the interface whose IP address this interface is to share. If you choose **Static IP Address**, complete the fields below.

IP Address

Enter the IP address for this interface. Obtain this value from your network administrator or service provider. For more information, see IP Addresses and Subnet Masks.

Subnet Mask

Enter the subnet mask. The subnet mask specifies the portion of the IP address that provides the network address. This value is synchronized with the network bits. Obtain the value of the subnet mask or the network bits from your network administrator or service provider.

Subnet Bits

Alternatively, choose the number of bits that specify how much of the IP address provides the network address.

Clock Settings

In most cases, clock settings should not be changed from the default values. If you know that your requirements are different from the defaults, click and adjust the clock settings in the window displayed.

The Clock Settings button appears only if you are configuring a T1 or E1 serial connection.

Dynamic DNS

Enable dynamic DNS if you want to update your DNS servers automatically whenever the WAN interface IP address changes.

Note This feature appears only if supported by the Cisco IOS release on your router.

To choose a dynamic DNS method to use, do one of the following:

- Enter the name of an existing dynamic DNS method.

  Enter the name in the **Dynamic DNS Method** field exactly as it appears in the list in **Configure > Router > DNS > Dynamic DNS Methods**.

- Choose an existing dynamic DNS method from a list.

  Click the drop-down menu and choose an existing method. A window with a list of existing dynamic DNS methods opens. This menu choice is available only if there are existing dynamic DNS methods.

- Create a new dynamic DNS method.

  Click the drop-down menu and choose to create a new dynamic DNS method.

To clear an associated dynamic DNS method from the interface, choose **None** from the drop-down menu.

Add or Edit GRE Tunnel

You can add a GRE tunnel to an interface or edit an existing interface in this window. This window does not appear if the GRE tunnel is not configured using **gre ip** mode.

Tunnel Number

Enter a number for this tunnel.

Tunnel Source

Choose the interface that the tunnel will use. This interface must be reachable from the other end of the tunnel; therefore, it must have a public, routable IP address.

Tunnel Destination

The tunnel destination is the interface on the router at the other end of the tunnel. Choose whether you will specify an IP address or a hostname, and then enter that information. If you chose IP address, provide the IP address and subnet mask in dotted decimal format; for example, 192.168.20.1 and 255.255.255.0.

Make sure that this address or hostname is reachable using the **ping** command; otherwise, the tunnel will not be properly created.

Tunnel IP Address

Enter the IP address of the tunnel in dotted decimal format; for example, 192.168.20.1. For more information, see "IP Addresses and Subnet Masks" section on page 97-1.

GRE Keepalive Check Box

Check the GRE Keepalive Check Box for the router to send GRE keepalives. Specify the interval, in seconds, that keepalives will be sent, and the waiting period, in seconds, between retries.

Maximum Transmission Unit

Enter the maximum transmission unit (MTU) size. If you want the size adjusted to a lower value when the adjustment should avoid packet fragmentation, click **Adjust MTU to avoid fragmentation**.

Bandwidth

Click to specify the bandwidth for this tunnel in kilobytes.

Connection: ISDN BRI

Complete these fields if you are configuring an ISDN BRI connection. Because Cisco CP supports only PPP encapsulation over an ISDN BRI connection, the encapsulation shown is not editable.

Encapsulation

PPP chosen.

ISDN Switch Type

Choose the ISDN switch type. Contact your ISDN service provider for the switch type for your connection.

Cisco CP supports these BRI switch types:

- For North America:
  - basic-5ess—Lucent (AT&T) basic rate 5ESS switch
  - basic-dms100—Northern Telecom DMS-100 basic rate switch
  - basic-ni—National ISDN switches
- For Australia, Europe, and the United Kingdom:
  - basic-1tr6—German 1TR6 ISDN switch
  - basic-net3—NET3 ISDN BRI for Norway NET3, Australia NET3, and New Zealand NET3 switch types; ETSI-compliant switch types for Euro-ISDN E-DSS1 signaling system
  - vn3—French ISDN BRI switches
- For Japan:
  - ntt—Japanese NTT ISDN switches
- For Voice/PBX systems:
  - basic-qsig—PINX (PBX) switches with QSIG signaling per Q.931 ()

SPIDs

Click if you need to enter service profile ID (SPID) information.

Some service providers use SPIDs to define the services subscribed to by the ISDN device that is accessing the ISDN service provider. The service provider assigns the ISDN device one or more SPIDs when you first subscribe to the service. If you are using a service provider that requires SPIDs, your ISDN device cannot place or receive calls until it sends a valid, assigned SPID to the service provider when accessing the switch to initialize the connection.

Only the DMS-100 and NI switch types require SPIDs. The Lucent (AT&T) 5ESS switch type may support a SPID, but we recommend that you set up that ISDN service without SPIDs. In addition, SPIDs have significance at the local-access ISDN interface only. Remote routers never receive the SPID.

A SPID is usually a seven-digit telephone number with some optional numbers. However, service providers may use different numbering schemes. For the DMS-100 switch type, two SPIDs are assigned, one for each B channel.

Remote Phone Number

Enter the phone number of the destination of the ISDN connection.

Options

Click if you need to associate ACLs with a dialer list to identify interesting traffic, enter timer settings, or enable or disable multilink PPP.

Identifying interesting traffic will cause the router to dial out and create an active connection only when the router detects interesting traffic.

Timer settings will cause the router to automatically disconnect a call after the line is idle for the specified amount of time.

Multilink PPP can be configured to provide load balancing between ISDN B channels.

IP Address

Choose **Static IP address**, **IP Unnumbered**, or **IP Negotiated**. If you choose **Specify an IP address**, complete the fields below.

IP Address

Enter the IP address for this point-to-point subinterface. Obtain this value from your network administrator or service provider. For more information, see "IP Addresses and Subnet Masks" section on page 97-1.

Subnet Mask

Enter the subnet mask. The subnet mask specifies the portion of the IP address that provides the network address. This value is synchronized with the network bits. Obtain the value of the subnet mask or the network bits from your network administrator or service provider.

Subnet Bits

Alternatively, enter the network bits to specify how many bits in the IP address provide the network address.

Authentication

Click if you need to enter CHAP or PAP authentication information.

Dynamic DNS

Enable dynamic DNS if you want to update your DNS servers automatically whenever the WAN interface IP address changes.

Note This feature appears only if supported by the Cisco IOS release on your router.

To choose a dynamic DNS method to use, do one of the following:

- Enter the name of an existing dynamic DNS method.

  Enter the name in the **Dynamic DNS Method** field exactly as it appears in the list in **Configure > Router > DNS > Dynamic DNS Methods**.

- Choose an existing dynamic DNS method from a list.

  Click the drop-down menu and choose an existing method. A window with a list of existing dynamic DNS methods opens. This menu choice is available only if there are existing dynamic DNS methods.

- Create a new dynamic DNS method.

  Click the drop-down menu and choose to create a new dynamic DNS method.

To clear an associated dynamic DNS method from the interface, choose **None** from the drop-down menu.

Connection: Analog Modem

Complete these fields if you are configuring an analog modem connection. Because Cisco CP supports only PPP encapsulation over an analog modem connection, the encapsulation shown is not editable.

Encapsulation

PPP chosen.

Remote Phone Number

Enter the phone number of the destination of the analog modem connection.

Options

Click if you need to associate ACLs with a dialer list to identify interesting traffic or enter timer settings.

Identifying interesting traffic will cause the router to dial out and create an active connection only when the router detects interesting traffic.

Timer settings will cause the router to automatically disconnect a call after the line is idle for the specified amount of time.

Clear Line

Click to clear the line. You should clear the line after creating an async connection so that interesting traffic triggers the connection.

IP Address

Choose **Static IP address**, **IP Unnumbered**, or **IP Negotiated**. If you choose **Specify an IP address**, complete the fields below.

IP Address

Enter the IP address for this point-to-point subinterface. Obtain this value from your network administrator or service provider. For more information, see "IP Addresses and Subnet Masks" section on page 97-1.

Subnet Mask

Enter the subnet mask. The subnet mask specifies the portion of the IP address that provides the network address. This value is synchronized with the network bits. Obtain the value of the subnet mask or the network bits from your network administrator or service provider.

Subnet Bits

Alternatively, enter the network bits to specify how many bits in the IP address provide the network address.

Authentication

Click if you need to enter CHAP or PAP authentication information.

Dynamic DNS

Enable dynamic DNS if you want to update your DNS servers automatically whenever the WAN interface IP address changes.

Note This feature appears only if supported by the Cisco IOS release on your router.

To choose a dynamic DNS method to use, do one of the following:

- Enter the name of an existing dynamic DNS method.

  Enter the name in the **Dynamic DNS Method** field exactly as it appears in the list in **Configure > Router > DNS > Dynamic DNS Methods**.

- Choose an existing dynamic DNS method from a list.

  Click the drop-down menu and choose an existing method. A window with a list of existing dynamic DNS methods opens. This menu choice is available only if there are existing dynamic DNS methods.

- Create a new dynamic DNS method.

  Click the drop-down menu and choose to create a new dynamic DNS method.

To clear an associated dynamic DNS method from the interface, choose **None** from the drop-down menu.

Connection: (AUX Backup)

Complete these fields if you are configuring an asynchronous dial-up connection using the console port to double as an AUX port on a Cisco 831 or 837 router. Enter the information in this window, click **Backup Details** and enter dial-backup information, which is required for this type of connection. Note that because Cisco CP supports only PPP encapsulation over an analog modem connection, the encapsulation shown is not editable.

The option to configure the AUX port as a dial-up connection is available only for the Cisco 831 and 837 routers. This option will not be available for those routers if any of the following conditions occur:

- Router is not using a Zutswang Cisco IOS release
- Primary WAN interface is not configured
- Asynchronous interface is already configured
- Asynchronous interface is not configurable by Cisco CP because of the presence of unsupported Cisco IOS commands in the existing configuration

Encapsulation

PPP chosen.

Remote Phone Number

Enter the phone number of the destination of the analog modem connection.

Options

Click if you need to associate ACLs with a dialer list to identify interesting traffic or enter timer settings.

Identifying interesting traffic will cause the router to dial out and create an active connection only when the router detects interesting traffic.

Timer settings will cause the router to automatically disconnect a call after the line is idle for the specified amount of time.

Clear Line

Click to clear the line. You should clear the line after creating an async connection so that interesting traffic triggers the connection.

IP Address

Choose **Static IP address**, **IP Unnumbered**, or **IP Negotiated**. If you choose **Specify an IP address**, complete the fields below.

IP Address

Enter the IP address for this point-to-point subinterface. Obtain this value from your network administrator or service provider. For more information, see "IP Addresses and Subnet Masks" section on page 97-1.

Subnet Mask

Enter the subnet mask. The subnet mask specifies the portion of the IP address that provides the network address. This value is synchronized with the network bits. Obtain the value of the subnet mask or the network bits from your network administrator or service provider.

Subnet Bits

Alternatively, enter the network bits to specify how many bits in the IP address provide the network address.

Backup Details

Click to display the Backup Configuration window, which lets you configure dial-backup information for this connection. This information is mandatory for this type of connection, and an error will be displayed if you try to complete the connection configuration without entering dial-backup configuration information.

Authentication

Click if you need to enter CHAP or PAP authentication information.

Dynamic DNS

Enable dynamic DNS if you want to update your DNS servers automatically whenever the WAN interface IP address changes.

Note This feature appears only if supported by the Cisco IOS release on your router.

To choose a dynamic DNS method to use, do one of the following:

- Enter the name of an existing dynamic DNS method.

  Enter the name in the **Dynamic DNS Method** field exactly as it appears in the list in **Configure > Router > DNS > Dynamic DNS Methods**.

- Choose an existing dynamic DNS method from a list.

  Click the drop-down menu and choose an existing method. A window with a list of existing dynamic DNS methods opens. This menu choice is available only if there are existing dynamic DNS methods.

- Create a new dynamic DNS method.

  Click the drop-down menu and choose to create a new dynamic DNS method.

To clear an associated dynamic DNS method from the interface, choose **None** from the drop-down menu.

Authentication

This page is displayed if you enabled PPP for a serial connection or PPPoE encapsulation for an ATM or Ethernet connection, or you are configuring an ISDN BRI or analog modem connection. Your service provider or network administrator may use a Challenge Handshake Authentication Protocol (CHAP) password or a Password Authentication Protocol (PAP) password to secure the connection between the devices. This password secures both incoming and outgoing access.

CHAP/PAP

Check the box for the type of authentication used by your service provider. If you do not know which type your service provider uses, you can check both boxes. The router will attempt both types of authentication, and one attempt will succeed.

CHAP authentication is more secure than PAP authentication.

Login Name

The login name is given to you by your service provider and is used as the username for CHAP/PAP authentication.

Password

Enter the password exactly as given to you by your service provider. Passwords are case sensitive. For example, the password *test* is not the same as *TEST*.

Reenter Password

Reenter the same password that you entered in the previous box.

SPID Details

Some service providers use service profile ID numbers (SPIDs) to define the services subscribed to by the ISDN device that is accessing the ISDN service provider. The service provider assigns the ISDN device one or more SPIDs when you first subscribe to the service. If you are using a service provider that requires SPIDs, your ISDN device cannot place or receive calls until it sends a valid, assigned SPID to the service provider when accessing the switch to initialize the connection.

Only the DMS-100 and NI switch types require SPIDs. The AT&T 5ESS switch type may support a SPID, and we recommend that you set up that ISDN service without SPIDs. In addition, SPIDs have significance at the local-access ISDN interface only. Remote routers never receive the SPID.

A SPID is usually a seven-digit telephone number with some optional numbers. However, service providers may use different numbering schemes. For the DMS-100 switch type, two SPIDs are assigned, one for each B channel.

SPID1

Enter the SPID to the first BRI B channel provided to you by your ISP.

SPID2

Enter the SPID to the second BRI B channel provided to you by your ISP.

Dialer Options

Both ISDN BRI and analog modem interfaces can be configured for dial-on-demand routing (DDR), which causes the connection to dial out and become active only under specified circumstances, thus saving connection time and cost. This window lets you configure options specifying when ISDN BRI or analog modem connections should be initiated and ended.

Dialer List Association

The dialer list lets you associate the ISDN BRI or analog modem connection with an ACL to identify interesting traffic. Identifying interesting traffic will cause the interface to dial out and establish a connection only when the router detects data traffic that matches the ACL.

Allow all IP traffic

Choose this option to cause the interface to dial out and establish a connection whenever there is any IP traffic being sent over the interface.

Filter traffic based on selected ACL

Choose this option to associate an ACL, which must be created using the rules interface, with the interface. Only traffic that matches the traffic identified in the ACL will cause the interface to dial out and establish a connection.

You can enter the ACL number you want to associate with the dialer interface to identify interesting traffic, or you can click the button next to the field to browse the list of ACLs or create a new ACL and choose it.

Timer Settings

Timer settings let you configure the maximum amount of time that a connection with no traffic stays active. By configuring timer settings, you can have connections that shut down automatically, saving you connection time and cost.

Idle timeout

Enter the number of seconds that are allowed to pass before an idle connection (one that has no traffic passing over it) is terminated.

Fast idle timeout

The fast idle timeout is used when one connection is active while a competing connection is waiting to be made. The fast idle timeout sets the maximum number of seconds with no interesting traffic before the active connection is terminated and the competing connection is made.

This occurs when the interface has an active connection to a next hop IP address and the interface receives interesting data with a different next hop IP destination. Because the dialer connection is point-to-point, the competing packet cannot be delivered until the current connection is ended. This timer sets the amount of time that must pass while the first connection is idle before that connection will be terminated and the competing connection made.

Enable Multilink PPP

Multilink PPP lets you load-balance data over multiple ISDN BRI B channels and asynchronous interfaces. With multilink PPP, when an ISDN connection is initially made, only one B channel is used for the connection. If the traffic load on the connection exceeds the specified threshold (entered as a percentage of total bandwidth), then a connection with a second B channel is made, and the data traffic is shared over both connections. This has the advantage of reducing connection time and cost when data traffic is low, and letting you use your full ISDN BRI bandwidth when it is needed.

Check this check box to enable multilink PPP. Uncheck it if you do not want to enable multilink PPP.

Load Threshold

Use this field to configure the percentage of bandwidth that must be used on a single ISDN BRI channel before another ISDN BRI channel connection will be made to load-balance traffic. Enter a number between 1 and 255, where 255 equals 100 percent of bandwidth on the first connection being utilized.

Data Direction

Cisco CP supports Multilink PPP only for outbound network traffic.

Backup Configuration

ISDN BRI and analog modem interfaces can be configured to work as backup interfaces to other, primary interfaces. In that case, an ISDN or analog modem connection will be made only if the primary interface goes down for some reason. If the primary interface and connection go down, the ISDN or analog modem interface will immediately dial out and try to establish a connection so that network services are not lost.

Enable Backup

Check if you want this ISDN BRI or analog modem interface to act as a backup connection. Uncheck this check box if you do not want the ISDN BRI or analog modem interface to be a backup interface.

Primary Interface

Choose the interface on the router that will maintain the primary connection. The ISDN BRI or analog modem connection will only be made if the connection on the chosen interface goes down.

Tracking Details

Use this section to identify a specific host to which connectivity must be maintained. The router will track connectivity to that host, and if the router discovers that connectivity to the host specified was lost by the primary interface, this will initiate a backup connection over the ISDN BRI or analog modem interface.

Hostname or IP Address to be Tracked

Enter the hostname or IP address of the destination host to which connectivity will be tracked. Specify an infrequently contacted destination as the site to be tracked.

Track Object Number

This is a read-only field that displays an internal object number generated and used by Cisco CP for tracking the connectivity to the remote host.

Next Hop Forwarding

These fields are optional. You can enter the IP address to which the primary and backup interfaces will connect when they are active. This is known as the next hop IP address. If you do not enter next hop IP addresses, Cisco CP will configure static routes using the interface name. Note that when you back up a multipoint WAN connection, such as an Ethernet connection, you must enter next hop IP addresses for routing to occur properly, but when backing up a point-to-point connection, this information is not necessary.

Primary Next Hop IP Address

Enter the next hop IP address of the primary interface.

Backup Next Hop IP Address

Enter the next hop IP address of the ISDN BRI or analog modem backup interface.

Delete Connection

You can delete a WAN connection that appears in the Edit Interface/Connections window. This window appears when you are deleting an interface configuration, and when the connection you want to delete contains associations such as access rules that have been applied to this interface. This window gives you the opportunity to save the associations for use with another connection.

When you delete a connection, the Create New Connection list is refreshed if the deletion makes a connection type available that was not available before the deletion.

You can automatically delete all associations that the connection has, or delete the associations later.

To view the associations that the connection has:

Click **View Details**.

To delete the connection and all associations:

Click **Automatically delete all associations**, and then click **OK** to cause Cisco CP to delete the connection and all of the associations.

To manually delete the associations:

To manually delete the associations, click **View Details** to see a list of the associations that this connection has. Make note of the associations, choose **I will delete the associations later**, and then click **OK**. You can manually delete the associations using the instructions in the following list.

The possible associations and the instructions for deleting them are:

- Default Static Route—The interface is configured as the forwarding interface for a default static route. To delete the static route with which this interface is associated, click **Configure**, then click **Routing**. Click the static route in the Static Routing table, and click **Delete**.
- Port Address Translation—PAT is configured, using the interface on which this connection was created. To delete the PAT association, click **Configure**, then click **NAT**. Click the rule associated with this connection, and click **Delete**.
- NAT—The interface is designated as either a NAT inside or NAT outside interface. To delete the NAT association, click **Configure**, then click **Interfaces and Connections**. Click the connection in the interface list, and then click **Edit**. Click the **NAT** tab, then choose **None** from the NAT drop-down menu.
- ACL—An ACL is applied to the interface on which the connection was created. To delete the ACL, click **Configure**, then click **Interfaces and Connections**. Click the connection in the Interface List, then click **Edit**. Click the **Association tab**, then in the Access Rule group, click the **...** button, which is next to both the Inbound and Outbound fields, and click **None**.
- Inspect—An inspection rule is applied to the interface on which the connection was created. To delete the inspection rule, click **Configure**, then click **Interfaces and Connections**. Click the connection in the Interface List, then click **Edit**. Click the **Association** tab, in the Inspection Rule group, for both the Inbound and Outbound fields, choose **None**.
- Crypto—A crypto map is applied to the interface on which the connection was created. To delete the crypto map, click **Configure**, then click **Interfaces and Connections**. Click the connection in the Interface List, and then click **Edit**. Click the **Association tab**, in the VPN group, in the IPSec Policy field, click **None**.

- EZVPN—An Easy VPN is applied to the interface on which the connection was created. To delete the Easy VPN, click **Configure**, then click **Interfaces and Connections**. Click the connection in the Interface List, and then click **Edit**. Click the **Association tab**, in the VPN group, in the Easy VPN field, click **None**.
- VPDN—VPDN commands that are required for a PPPoE configuration are present in the router configuration. If there are any other PPPoE connections configured on the router, do not delete the VPDN commands.
- **ip tcp adjust mss**—This command is applied to a LAN interface to adjust the TCP maximum size. If there are any other PPPoE connections configured on the router, do not delete this command.
- Backup connection—When a backup connection is configured for the primary interface.To delete the backup association, click **Configure**, then click **Interfaces and Connections**. Click the Backup interface in the Interface List, then click **Edit**. Click the **Backup** tab and uncheck the **Enable Backup** check box.
- PAT on Backup connection—PAT is configured on the backup interface. To delete the PAT association, click **Configure**, then click **NAT**. Click the rule associated with this connection, and then click **Delete**.
- Floating Default Route on Backup connection—The Backup interface is configured with a floating default static route. To delete the floating static route, click **Configure**, then click **Routing**. Click the floating static route in the Static Routing table, and click **Delete**.

Connectivity Testing and Troubleshooting

This window allows you to test a configured connection by pinging a remote host. If the ping fails, Cisco CP reports the probable cause and suggests actions you can take to correct the problem.

Which connection types can be tested?

Cisco CP can troubleshoot ADSL, G.SHDSL V1, and G.SHDSL V2 connections, using PPPoE, AAL5SNAP, or AAL5MUX encapsulation.

Cisco CP can troubleshoot Ethernet connections with PPPoE encapsulation.

Cisco CP cannot troubleshoot unencapsulated Ethernet connections, Serial and T1 or E1 connections, Analog connections, and ISDN connections. Cisco CP provides basic ping testing for these connection types.

What is Basic Ping Testing?

When Cisco CP performs basic ping testing, it does the following:

1. Checks the interface status to see if it is up or down.
2. Checks DNS Settings, whether they are Cisco CP default options or user-specified hostnames.
3. Checks for DHCP and IPCP configurations on the interface.
4. Exits interface test.
5. Pings the destination.

Cisco CP reports the results of each of these checks in the Activity/Status columns. If the ping succeeds, then the connection will be reported as successful. Otherwise the connection is reported down, and the test that failed is noted.

How does Cisco CP Troubleshoot?

When Cisco CP troubleshoots a connection, it performs a more extensive check than the basic ping test. If the router fails a test, Cisco CP performs additional checks so it can provide you with the possible reasons for failure. For example, if Layer 2 status is down, Cisco CP attempts to determine the reasons, reports them, and recommends actions you can take to rectify the problem. Cisco CP performs the following tasks:

1. Checks interface status. If the Layer 2 protocol is up, Cisco CP goes to Step 2.

   If Layer 2 protocol status is down, Cisco CP checks ATM PVC status for XDSL connections, or PPPoE status for encapsulated Ethernet connections.

   - If the ATM PVC test fails, Cisco CP displays possible reasons for the failure and actions you can take to correct the problem.
   - If the PPPoE connection is down, there is a cabling problem, and Cisco CP displays appropriate reasons and actions.

   After performing these checks, the test is terminated and Cisco CP reports the results and suggests actions.

2. Checks DNS Settings, whether they are Cisco CP default options or user-specified hostnames.
3. Checks DHCP or IPCP configuration and status. If the router has an IP address through either DHCP or IPCP, Cisco CP goes to Step 4.

   If the router is configured for DHCP or IPCP but has not received an IP address through either of these methods, Cisco CP performs the checks in Step 1. The test terminates and Cisco CP reports the results and suggests actions.
4. Pings the destination. If the ping succeeds, Cisco CP reports success.

   If the ping fails on an xDSL connection with PPPoE encapsulation, Cisco CP checks:

   - ATM PVC status
   - PPPoE tunnel status
   - PPP authentication status

After performing these checks, Cisco CP reports the reason that the ping failed.

If the ping fails on an Ethernet with PPPoE encapsulation connection, Cisco CP checks:

- PPPoE tunnel status
- PPP authentication status

After performing these checks, Cisco CP reports the reason that the ping failed.

If the ping fails on an xDSL connection with AAL5SNAP or AAL5MUX encapsulation, Cisco CP checks the ATM PVC status and reports the reason the ping failed.

IP Address/Hostname

Specify the server name to ping to test WAN interface.

Automatically determined by Cisco CP

Cisco CP pings its default host to test WAN interface. Cisco CP detects the statically configured DNS servers on the router, and dynamically imported DNS servers. Cisco CP pings these servers, and if successful pings exit through the interface under test, Cisco CP reports success. If no pings succeeds, or successful pings are not found to exit the interface being tested, Cisco CP reports failure.

User Specified

Specify the IP address of the hostname of your choice for testing the WAN interface.

Summary

Click this button if you want to view the summarized troubleshooting information.

Details

Click this button if you want to view the detailed troubleshooting information.

Activity

This column displays the troubleshooting activities.

Status

Displays the status of each troubleshooting activity by the following icons and text alerts:


The connection is up.


The connection is down.


Test is successful.


Test failed.

Reason

This box provides the possible reasons for the WAN interface connection failure.

Recommended action(s)

This box provides a possible action or solution to rectify the problem.

What Do You Want to Do?

To:	Do this:
Troubleshoot the WAN interface connection.	Click the **Start** button. When a test is running, the Start button label changes to Stop. You have the option to abort the troubleshooting while the test is in progress.
Save the test report.	Click the **Save Report** button to save the test report in HTML format. This button will be active only when test is in progress or when the testing is complete.

CHAPTER 7

Edit Controller/Connection

The Edit Controller/Connection tab appears when there are DSL or VDSL controllers installed on the router. It enables you to configure DSL controllers, G.SHDSL controllers, and VDSL controllers. We recommend that you perform the initial controller configuration using the wizards available from the Create Connection tab.

This chapter contains the following sections:

- Configuring a Cisco WIC-1SHDSL-V2 Controller, page 7-1
- Configuring a Cisco Multi-mode VDSL Router, page 7-7
- Configuring a Cisco HWIC-SHDSL Controller, page 7-12

Configuring a Cisco WIC-1SHDSL-V2 Controller

To configure a Cisco WIC-1SHDSL-V2 controller, complete the following steps:

Step 1 Click **Configure > Interface Management > Interface and Connections**.

Step 2 Click **Edit Controllers/Connection**.

Step 3 In the Controllers pane, click the Plus (+) icon next to the DSL Controller branch to display the available DSL controllers.

Step 4 In the right pane, configure the interfaces associated with the controller. You can add, edit, delete, enable, or disable an interface. See the section DSL Controller Screen Reference, page 7-2 for more information.

Step 5 To test a configuration change that you have made, choose the interface you have made changes to, and click **Test Connection**.

DSL Controller Screen Reference

The following sections describes the screens used to configure a Cisco WIC-1SHDSL-V2 controller:

- DSL Edit Controllers/Connection Tab, page 7-12
- Configure DSL Controller, page 7-2
- Add a G.SHDSL Connection, page 7-4

Configure DSL Controller

Cisco CP supports the configuration of the Cisco WIC-1SHDSL-V2. This WIC supports TI, E1, or a G.SHDSL connection over an ATM interface. However, Cisco CP supports only a G.SHDSL connection using the ATM interface.

The Configure DSL Controller window lets you set the controller mode on the WIC to ATM, enabling a G.SHDSL connection, and lets you create or edit DSL controller information for the G.SHDSL connection.

How to get to this screen

Click **Configure > Interface Management > Interface and Connections > Edit Controllers /Connection > DSL Controller > DSL *N/N/N***.

Field Reference

Table 7-1 describes the fields to configure the DSL Controller.

Table 7-1 Configure DSL Controller Fields

Element	Description
Controller Mode	Cisco CP supports only ATM mode, which provides for a G.SHDSL connection, on this controller. This field is automatically set to ATM mode when the OK button is clicked.
Equipment Type	If the connection terminates at the central office, choose **CO**. If the connection terminates at customer premises equipment, choose **CPE**.
Operating Mode	Choose whether the DSL connection should use Annex A signaling (for DSL connections in the United States) or Annex B signaling (for DSL connections in Europe).
Line Mode	Choose whether this is a 2-wire or 4-wire G.SHDSL connection.
Line Number	Choose the interface number on which the connection will be made.
Line Rate	Choose the DSL line rate for the G.SHDSL port. If you choose a 2-wire connection, you can choose either **auto**, which configures the interface to automatically negotiate the line rate between the G.SHDSL port and the DSLAM, or the actual DSL line rate. The supported line rates are 200, 264, 392, 520, 776, 1032, 1160, 1544, 2056, and 2312. If you have chosen a 4-wire connection, you must choose a fixed line rate. The supported line rates for a 4-wire connection are 384, 512, 640, 768, 896, 1024, 1152, 1280, 1408, 1664, 1792, 1920, 2048, 2176, 2304, 2432, 2688, 2816, 2944, 3072, 3200, 3328, 3456, 3584, 3712, 3840, 3968, 4096, 4224, 4352, 4480, and 4608. **Note** If different DSL line rates are configured at opposite ends of the DSL uplink, the actual DSL line rate is always the lower rate.

Table 7-1 Configure DSL Controller Fields (continued)

Element	Description
Enable Sound-to-Noise Ratio Margin	The sound-to-noise ratio margin provides a threshold for the DSL modem to determine whether it should reduce or increase its power output depending on the amount of noise on the connection. If you have set the line rate to "auto", you can enable this feature to maximize the quality of the DSL connection. You cannot use this feature if your line rate is fixed. To enable the sound-to-noise ratio margin, check this check box and choose the ratio margins in the Current and Snext fields. To disable this feature, uncheck this check box.
Current	Choose the sound-to-noise ratio margin in the form of decibels (dB) on the current connection. The lower the ratio chosen here, the more noise will be tolerated on the connection. A lower dB setting will cause the DSL modem to allow more noise on the line, potentially resulting in a connection of lower quality but higher throughput. A higher dB setting causes the modem to restrict noise, potentially resulting in a connection of higher quality but lower throughput.
Snext	Choose the Self near-end crosstalk (Snext) sound-to-noise ratio margin in the form of decibels.
DSL Connections	This area displays all of the G.SHDSL connections currently configured on this controller. To configure a new G.SHDSL connection, click **Add**. This displays the Add a G.SHDSL Connection page, letting you configure the new connection. To edit an existing G.SHDSL connection, choose the connection in this field and click **Edit**. This also will display the Add a G.SHDSL Connection page, letting you edit the connection configuration. To delete a connection, choose the connection in this field, and click **Delete**.

Add a G.SHDSL Connection

This dialog enables you to create or edit a G.SHDSL connection.

How to get to this screen

Click **Configure > Interface Management > Interface and Connections > Edit Controllers/Connection > DSL Controller > DSL *N/N/N***.

Field Reference

Table 7-2 Add a G.SHDSL Connection

Element	Description
Encapsulation	Select the type of encapsulation to use for this link. • PPPoE—specifies Point-to-Point Protocol over Ethernet encapsulation. • PPPoA—specifies Point-to-Point Protocol over ATM encapsulation. • RFC 1483 Routing (AAL5 SNAP)—specifies that each PVC can carry multiple protocols. • RFC 1483 Routing (AAL5 MUX)—specifies that each PVC carry only one type of protocol. If you are editing a connection, the encapsulation is shown, but not editable. To change the encapsulation type, delete the connection and recreate it using the encapsulation type you need.
Virtual Path Identifier	The virtual path identifier (VPI) is used in ATM switching and routing to identify the path used for a number of connections. Obtain this value from your service provider. If you are editing an existing connection, this field is disabled. To change this value, delete the connection and recreate it using the value you need.
Virtual Circuit Identifier	The virtual circuit identifier (VCI) is used in ATM switching and routing to identify a particular connection within a path that it may share with other connections. Obtain this value from your service provider. If you are editing an existing connection, this field is disabled. To change this value, delete the connection and recreate it using the value you need.
IP Address	Select how the router obtains an IP address for this link. The fields that appear in this area change according to the encapsulation type chosen. Your service provider or network administrator must tell you the method the router should use to obtain an IP address.

Table 7-2 Add a G.SHDSL Connection (continued)

Element	Description
Static IP address	If you select Static IP address, enter the address that the interface will use, and the subnet mask, or the network bits. Obtain this information from your service provider or network administrator. For more information, see the "IP Addresses and Subnet Masks" section on page 97-1.
Dynamic IP address	If you select Dynamic IP address, the interface will obtain an IP address from a DHCP server on the network. If the DHCP server uses DHCP option 12, it sends a host name for the router along with the IP address it is to use. Check with your service provider or network administrator to determine the host name sent.
IP Unnumbered	Select this option to have the interface share an IP address with an Ethernet interface on the router. If you select this option, you must specify from the drop-down list, the address of the Ethernet interface to use.
Description	Enter a description of this connection that makes it easy to recognize and manage.
Enable Multilink PPP	Check this check box to use Multilink Point-to-Point Protocol (MLP) with this interface. MLP can improve the performance of a network with multiple WAN connections by using load balancing functionality, packet fragmentation, bandwidth-on-demand, and other features.
Authentication	Click to enter CHAP or PAP authentication information.
Dynamic DNS	Enable dynamic DNS to automatically update your DNS servers whenever the WAN interface's IP address changes. **Note** This feature appears only if supported by the Cisco IOS image.
Use one of the methods described in the following rows to enable Dynamic DNS. The method is listed in the left column, and the process is described in the right column.	
Enter the name of an existing dynamic DNS method.	Enter the name in the Dynamic DNS Method field exactly as it appears in the list on the **Configure > Router > DNS > Dynamic DNS Methods** screen.

Table 7-2 Add a G.SHDSL Connection (continued)

Element	Description
Choose an existing dynamic DNS method from a list.	Click the drop-down menu and choose an existing method. A window with a list of existing dynamic DNS methods opens. This menu choice is available only if there are existing dynamic DNS methods.
Create a new dynamic DNS method.	Click the drop-down menu and choose to create a new dynamic DNS method.
To clear an associated dynamic DNS method from the interface, choose **None** from the drop-down menu.	

Configuring a Cisco Multi-mode VDSL Router

To configure a Cisco Multi-mode VDSL router, complete the following steps:

Step 1 Click **Configure > Interface Management > Interface and Connections**.

Step 2 Click **Edit Controllers/Connection**.

Step 3 In the Controllers pane, click the Plus (+) icon next to the VDSL Controller branch to display the available VDSL controllers.

Step 4 In the right pane, configure the interfaces associated with the controller. You can add, edit, delete, enable, or disable an interface. See Cisco Multi-mode VDSL Router Reference for more information.

Step 5 To test a configuration change that you have made, choose the interface whose properties you have changed, and click **Test Connection**.

Cisco Multi-mode VDSL Router Reference

The following sections describe the Cisco CP screens used to configure a Cisco Multi-mode VDSL router:

- DSL Edit Controllers/Connection Tab, page 7-12
- Configure VDSL Controller dialog box, page 7-8
- Connection: Ethernet LAN, page 6-21
- Add a VDSL Connection dialog box, page 7-8

Configure VDSL Controller dialog box

Use this dialog box to configure the Cisco Multi-mode VDSL router.

How to get to this screen

Click **Configure > Interface Management > Interface and Connections > Edit Controllers /Connection** > **VDSL Controller > VDSL *N/N/N* > Edit**.

Field Reference

Table 7-3 Configure VDSL Controller dialog box fields

Element	Description
Operating Mode drop-down list	Choose ADSL1, ADSL2, ADSL2+, ETS1, or VDSL2 from the list. The default selection is Auto.
Use lower tone of 29 to 48 for Upstream Traffic checkbox	Select the checkbox to lower the upstream rate. The bandwidth and traffic are adjusted in the DSL line from your customer premises-equipment (CPE) to the Internet Service Provider (ISP).

Add a VDSL Connection dialog box

Use this dialog box to create or edit a VDSL connection.

How to get to this screen

Click **Configure > Interface Management > Interface and Connections > Edit Controllers /Connection > Add a VDSL Connection**.

Field Reference

Table 7-4 Add a VDSL Connection dialog box fields

Element	Description
Encapsulation	Select the type of encapsulation that will be used for this link. • PPPoE—specifies Point-to-Point Protocol over Ethernet encapsulation. • PPPoA—specifies Point-to-Point Protocol over ATM encapsulation. • RFC 1483 Routing (AAL5 SNAP)—specifies that each PVC can carry multiple protocols. • RFC 1483 Routing (AAL5 MUX)—specifies that each PVC carry only one type of protocol. If you are editing a connection, the encapsulation is shown, but not editable. If you need to change the encapsulation type, delete the connection, and recreate it, using the encapsulation type you need.
Virtual Path Identifier	The virtual path identifier (VPI) is used in ATM switching and routing to identify the path used for a number of connections. Obtain this value from your service provider. If you are editing an existing connection, this field is disabled. If you need to change this value, delete the connection and recreate it using the value you need.
Virtual Circuit Identifier	The virtual circuit identifier (VCI) is used in ATM switching and routing to identify a particular connection within a path that it may share with other connections. Obtain this value from your service provider. If you are editing an existing connection, this field is disabled. If you need to change this value, delete the connection and recreate it using the value you need.
IP Address	Select how the router will obtain an IP address for this link. The fields that appear in this area change according to the encapsulation type chosen. Your service provider or network administrator must tell you the method the router should use to obtain an IP address.

Table 7-4 Add a VDSL Connection dialog box fields (continued)

Element	Description
Static IP address	If you select Static IP address, enter the address that the interface will use, and the subnet mask, or the network bits. Obtain this information from your service provider or network administrator. For more information, refer to IP Addresses and Subnet Masks.
Dynamic IP address	If you select Dynamic IP address, the interface will obtain an IP address from a DHCP server on the network. If the DHCP server uses DHCP option 12, it sends a host name for the router along with the IP address it is to use. Check with your service provider or network administrator to determine the host name sent.
IP Unnumbered	Select this option if you want the interface to share an IP address with an Ethernet interface on the router. If you select this option, you must specify from the drop-down list the Ethernet interface whose address you want to use.
Description	Enter a description of this connection that makes it easy to recognize and manage.
Enable Multilink PPP	Check this check box if you want to use Multilink Point-to-Point Protocol (MLP) with this interface. MLP can improve the performance of a network with multiple WAN connections by using load balancing functionality, packet fragmentation, bandwidth-on-demand, and other features.
Authentication	Click if you need to enter CHAP or PAP authentication information.
Dynamic DNS	Enable dynamic DNS if you want to automatically update your DNS servers whenever the WAN interface's IP address changes. **Note** This feature appears only if supported by the Cisco IOS image. Use one of the methods described in the following rows to enable Dynamic DNS. The method is listed in the left column, and the process is described in the right column.
Enter the name of an existing dynamic DNS method.	Enter the name in the Dynamic DNS Method field exactly as it appears in the list in **Configure > Router > DNS > Dynamic DNS Methods** screen.

Table 7-4 Add a VDSL Connection dialog box fields (continued)

Element	Description
Choose an existing dynamic DNS method from a list.	Click the drop-down menu and choose to use an existing method. A window with a list of existing dynamic DNS methods will open. This menu choice is available only if there are existing dynamic DNS methods.
Create a new dynamic DNS method.	Click the drop-down menu and choose to create a new dynamic DNS method.
To clear an associated dynamic DNS method from the interface, choose **None** from the drop-down menu.	

Configuring a Cisco HWIC-SHDSL Controller

The following procedure describes how to configure a Cisco HWIC-1SHDSL, Cisco HWIC-2SHDSL, and a Cisco HWIC-4SHDSL controller.

Step 1 Click **Configure > Interface Management > Interface and Connections**.

Step 2 Click **Edit Controllers/Connection**.

Step 3 In the Controllers pane, click the Plus (+) icon next to the SHDSL Controller branch to display the available SHDSL controllers.

Step 4 In the right pane, configure the interfaces associated with the controller. You can add, edit, delete, enable, or disable an interface. See the section Cisco HWIC SHDSL Screen Reference, page 7-12 for more information.

Step 5 To test a configuration change that you have made, choose the interface you have made changes to, and click **Test Connection**.

Cisco HWIC SHDSL Screen Reference

The Cisco CP **Edit Controllers /Connection** screen is described in the following sections:

- DSL Edit Controllers/Connection Tab, page 7-12
- Add DSL Group for a 2SHDSL Controller, page 7-15
- Edit DSL Group for a 2SHDSL Controller, page 7-15
- Add DSL Group for a 4SHDSL Controller, page 7-16
- Edit DSL Group for a 4SHDSL Controller, page 7-17

DSL Edit Controllers/Connection Tab

This tab appears in the 8xx VDSL platform routers and also when you have any of the following DSL controllers installed:

- WIC-1SHDSL-V2
- HWIC-2SHDSL

- HWIC-4SHDSL
- HWIC-1VDSL (Triple sec)

How to get to this screen

Click **Configure > Interface Management > Interface and Connections > Edit Controllers/Connection > SHDSL or VDSL Controller > SHDSL or VDSL *N/N/N***.

Field Reference

Table 7-5 Edit Controllers/Connection Fields

Element	Description
Controller List Pane	The left pane lists the router DSL, SHDSL, and VDSL controllers. To display information about a DSL, SHDSL, or VDSL controller, click the Plus (+) sign to the left of the branch, and then select a controller. The Group List and Interface list areas are updated with the information about that controller.
Group List Area	The Group List Area displays the DSL groups configured for the selected controller, and includes the name, IP address, controller type, slot, status, and available description. **Note** The Group List appears if you are displaying an HWIC-SHDSL controller.
Add	To create a new DSL group, click **Add**, and enter the required information in the displayed dialog. If groups 0 and 1 are already configured, the Add button is disabled.
Delete	To delete a DSL group, select the group and click **Delete**. Then, click **OK** to confirm the deletion.
Edit	To edit the properties of a DSL group, select the group and click **Edit**. Then, edit the group properties in the displayed dialog.

Table 7-5 Edit Controllers/Connection Fields (continued)

Element	Description
Interface List	The interface list displays the configured ATM interfaces and subinterfaces. It includes the interface name, IP address, interface type, the slot number, and the status of the interface. To determine which DSL group an interface or subinterface is associated with, look for the interface name in the Interface column of the Group List. **Note** When a DSL group is deleted, the ATM interfaces and subinterfaces associated with the DSL group are also deleted.
Add	To configure a new ATM interface for the selected controller, click **Add**, and set interface properties in the displayed dialog.
Edit	To edit an ATM interface, choose the interface and click **Edit**. Change interface properties in the displayed dialog.
Delete	To delete an ATM interface, choose the interface, and click **Delete**. Click **OK** to confirm the deletion.
Enable / Disable	To enable a disabled interface, choose the interface, and click **Enable**. The interface is enabled when the commands are delivered to the router, and the icon changes to green. To disable an enabled interface, choose the interface, and click **Disable**. The interface is disabled when the commands are delivered to the router, and the icon changes to red.
Test Connection	To test the connection of an ATM interface, choose the interface and click **Test Connection**. The results of the test are displayed in a status window.

Add DSL Group for a 2SHDSL Controller

This dialog allows you to add a DSL group to a 2SHDSL controller. After a DSL group has been added, you can make additional settings by editing the DSL group.

How to get to this dialog

Click **Configure > Interface Management > Interface and Connections > Edit Controllers/Connection > SHDSL Controller > SHDSL *N/N/N* > Add**.

Field Reference

Table 7-6 Add DSL Group for 2SHDSL Controller

Element	Description
Group Number	Choose 0 or 1. If a group number is already in use, it will not be available in the list.
DSL Pairs	Check the pairs to use for this group. Pairs that are already in use are disabled.

Edit DSL Group for a 2SHDSL Controller

This dialog allows you to edit a DSL group on a 2SHDSL controller.

How to get to this dialog

Click **Configure > Interface Management > Interface and Connections > Edit Controllers/Connection > SHDSL Controller > SHDSL *N/N/N* > Edit**.

Field Reference

Table 7-7 Edit DSL Group for 2SHDSL Controller

Element	Description
Operating Mode	Choose one the following: • Annex A—Regional operating parameters for North America. This is Annex A of the G.991.2 standard. • Annex B—Regional operating parameters for Europe. This is Annex B of the G.991.2 standard. • Annex A-B—Annex A/B of the G.991.2 standard. • Annex F-G—(available for only M-pair) Annex F/G of the G.991.2 standard. • Annex F—(available for only M-pair) Annex F of the G.991.2 standard. • Annex G—(available for only M-pair) Annex G of the G.991.2 standard.
Line Rate	Choose the DSL line rate for the G.SHDSL port. If you choose a 2-wire connection (the default), you can choose either **auto**, which configures the interface to automatically negotiate the line rate between the G.SHDSL port and the DSLAM, or the actual DSL line rate. If you choose a 4-wire connection, you must choose a fixed line rate. A 4-wire connection is a DSL group with two pairs. The line rates that you can set depend on the operating mode chosen. Line rates increase in 64-byte increments. • Annex A, Annex B, and Annex A-B—384 through 4608 • Annex F, Annex F-G—4608 through 7680. **Note** If different DSL line rates are configured at opposite ends of the DSL uplink, the actual DSL line rate is always the lower rate.

Add DSL Group for a 4SHDSL Controller

This dialog allows you to add a DSL group to a 4SHDSL controller.

How to get to this dialog

Click **Configure > Interface Management > Interface and Connections > Edit Controllers/Connection > SHDSL Controller > SHDSL *N/N/N* > Add**.

Field Reference

Table 7-8 Add DSL Group for 4SHDSL Controller Fields

Element	Description
Group Number	Choose 0 or 1. If a group number is already in use, it will not be available in the list.
DSL Pairs	Check the pairs that you want to use for this group. You can check any combination of pairs. Pairs that are already in use are disabled.
Group Type	Choose the type of group that you want to create. • IMA—Inverse multiplexing over ATM. IMA allows you to bundle communications lines to obtain speeds in excess of 3 Mbps. IMA provides a protocol that handles link failure and recovery, and also the addition and deletion of links. IMA bundling creates an ATM-IMA interface. • M-Pair—Multi-pair bundling allows you to group pairs to create an ATM interface without IMA features.

Edit DSL Group for a 4SHDSL Controller

This dialog allows you to edit a DSL group on a 4SHDSL controller.

How to get to this dialog

Click **Configure > Interface Management > Interface and Connections > Edit Controllers/Connection > SHDSL Controller > SHDSL *N/N/N* > Edit**.

Field Reference

Table 7-9 Edit DSL Group for 4SHDSL Controller

Element	Description
Operating Mode	Choose one the following: • Annex A—Regional operating parameters for North America. This is Annex A of the G.991.2 standard. • Annex B—Regional operating parameters for Europe. This is Annex B of the G.991.2 standard. • Annex A-B—Annex A/B of the G.991.2 standard. • Annex F-G—(available for only M-pair) Annex F/G of the G.991.2 standard. • Annex F—(available for only M-pair) Annex F of the G.991.2 standard. • Annex G—(available for only M-pair) Annex G of the G.991.2 standard.
Coding	Choose one of the following: • 16-TCPAM—4-bit Trellis Coded Pulse Amplitude Modulation. • 32-TCPAM—5-bit Trellis Coded Pulse Amplitude Modulation.
Line Rate	Choose the DSL line rate for the G.SHDSL port. If you choose a 2-wire connection (the default), you can choose either **auto**, which configures the interface to automatically negotiate the line rate between the G.SHDSL port and the DSLAM, or the actual DSL line rate. If you choose a 4-wire connection, you must choose a fixed line rate. A 4-wire connection is a DSL group with two pairs. The line rates that you can set depend on the operating mode you choose. Line rates increase in 64-byte increments. • Annex A, Annex B, and Annex A-B—384 through 4608 • Annex F, Annex F-G—4608 through 7680. **Note** If different DSL line rates are configured at opposite ends of the DSL uplink, the actual DSL line rate is always the lower rate.
IMA Group	Make minimum links settings and clock mode settings as described in the following rows.
Minimum Links	Enter the minimum number of links that must be active in order for the IMA group to be active.

Table 7-9 Edit DSL Group for 4SHDSL Controller (continued)

Element	Description
Clock Mode	Choose one of the following: • CTC—Common • ITC—Independent
IMA Link	To add a link to the DSL group, check the box next to the link number. To remove a link from the DSL group, uncheck the box next to the link number. Links that are not available to this DSL group are disabled.
Shut Down IMA Links	To disable an active link for this DSL group, check the box next to the link number. To enable a link that has been disabled, uncheck the box next to the link number.

CHAPTER 8

Wireless Support

For information about how to use Cisco Configuration Professional (Cisco CP) to configure the Wireless Support feature, see the screencast at: http://www.cisco.com/en/US/docs/net_mgmt/cisco_configuration_professional/scrcst/ccpsc.html.

Note You must have internet access to view the screencast.

CHAPTER 9

Cellular WAN Interface

For information about how to use Cisco Configuration Professional (Cisco CP) to configure cellular WAN interfaces, see the screencast at: http://www.cisco.com/en/US/docs/net_mgmt/cisco_configuration_professional/scrcst/ccpsc.html.

Note You must have internet access to view the screencast.

CHAPTER 10

Module Configuration

- For information about how to use Cisco Configuration Professional (Cisco CP) to configure modules, see the screencast at:

  http://www.cisco.com/en/US/docs/net_mgmt/cisco_configuration_professional/scrcst/ccpsc.html.

- For information about how to use Cisco Configuration Professional (Cisco CP) to configure the SRE-V module, see the screencast at:

  http://www.cisco.com/en/US/docs/net_mgmt/cisco_configuration_professional/scrcst/ccpsc.html.

Note You must have internet access to view the screencast.

You need to configure sip-ua CLIs for SRSV-CUE by running the following commands:

```
Router(config)#sip-ua
Router(config-sip-ua)# sip-ua mwi-server ipv4:<ip of SRSV-CUE module>
expires 3600 port 5060 transport udp
```

You also need to create dial peers from **Configure > Unified Communications > Dial Plans > VoIP** for the triggers to work when fallback is active.

CHAPTER 11

EnergyWise

For information about how to use Cisco Configuration Professional (Cisco CP) to configure the EnergyWise feature, see the screencast at: http://www.cisco.com/en/US/docs/net_mgmt/cisco_configuration_professional/scrcst/ccpsc.html.

Note You must have internet access to view the screencast.

CHAPTER 12

Trunks

The trunk configuration screens allow you to view and edit trunk voice configurations for each port on the device.

This chapter contains the following sections:

- Configure an Analog Trunk
- Configure a Digital Trunk
- Configuring PSTN Trunk Groups
- Configuring SIP Trunks

Configuring Trunks

A trunk (tie-line) is a permanent point-to-point communication line between two voice ports. Trunk lines are the phone lines coming into the PBX from the telephone provider. This differentiates these incoming lines from extension lines that leave the PBX and usually lead to individual phone sets. Trunking saves cost, because there are usually fewer trunk lines than extension lines, since it is unusual in most offices to have all extension lines in use for external calls at once.

FXS and DID Modes

Foreign Exchange Station (FXS) is a two-wire telephone communication mode. An FXS interface connects directly to a standard telephone and supplies ring, voltage, and dial tone. Cisco's FXS interface is an RJ-11 connector that allows connections to basic telephone service equipment, keysets, and PBXs.

Direct Inward Dialing (DID) is a service offered by telephone companies that enables callers to dial directly an extension on a PBX or packet voice system without the assistance of an operator or automated call attendant. This service makes use of DID trunks, which forward only the last three to five digits of a phone number to the PBX, router, or gateway. For example, a company has phone extensions 555-1000 to 555-1999. A caller dials 555-1234 and the local central office (CO) forwards 234 to the PBX or packet voice system. The PBX or packet voice system then rings extension 234. This entire process is transparent to the caller.

FXO Modes

FXO is a two-wire telephone communication mode. An FXO interface connects to the public switched telephone network (PSTN) central office and is the interface offered on a standard telephone. Cisco FXO interface is an RJ-11 connector that allows an analog connection at the PSTN central office or to a station interface on a PBX.

Trunks Reference

The following topics describe the windows used to configure trunk ports:

- Configure an Analog Trunk
- Edit an Analog Trunk
- Analog Trunks: General Settings Tab
- Analog Trunks: Advanced Signal Settings Tab
- Analog Trunks: Advanced Audio Settings Tab
- Analog Trunks: Advanced Timer Settings Tab
- Configure a Digital Trunk
- Edit a Digital Trunk
- Digital Trunks: T1/E1 Settings
- Digital Trunks: PRI or BRI Settings Tab
- Digital Trunks: PRI or BRI Audio Tab

Configure an Analog Trunk

You can view and edit an analog trunk voice configuration for each port on the device.

How to get to this screen

Click **Configure > Interface Management > Analog Trunks**.

Click **Configure > Unified Communications > Trunks > Analog Trunks**.

Related Links

- Configuring Trunks
- Edit an Analog Trunk
- Analog Trunks: General Settings Tab
- Analog Trunks: Advanced Signal Settings Tab
- Analog Trunks: Advanced Audio Settings Tab
- Analog Trunks: Advanced Timer Settings Tab

Field Reference

Table 12-1 Trunks

Element	Description
Trunk Type	Connection type.
Hardware	Device providing the trunk connection.
Location	Location of the voice port.
Description	A string that identifies a trunk.
Destination Number	The Destination Number is populated for FXO cards. It is blank for FXS or DID cards.

Edit an Analog Trunk

The screen is subdivided by tabs. The active content in the tabs varies depending on which port you are configuring.

If an analog phone is configured to a FXS port, the FXS port cannot be configured as a trunk by using Cisco Configuration Professional and it is not listed in the Trunks window. To use Cisco Configuration Professional to configure an FXS port as a trunk, delete any analog phone configuration. The FXS port is released to be configured as a trunk.

You cannot reset an analog voice port to the factory default configuration by using Cisco Configuration Professional. You must reset the configuration to factory defaults manually.

Related Links

- Configure an Analog Trunk
- Configuring Trunks
- Configure an Analog Trunk
- Analog Trunks: General Settings Tab
- Analog Trunks: Advanced Signal Settings Tab
- Analog Trunks: Advanced Audio Settings Tab
- Analog Trunks: Advanced Timer Settings Tab

Analog Trunks: General Settings Tab

In the General Settings tab, enter settings for trunk shown in Table 12-2.

How to get to this screen

Click **Configure > Interface Management > Analog Trunks >** (select a) **Trunk Type > Edit > General Settings** tab.

Click **Configure > Unified Communications > Trunks > Analog Trunks >** (select a) **Trunk Type > Edit > General Settings** tab.

Field Reference

Table 12-2 General Settings Tab

Element	Description
Card Type	If you are editing a FXS-DID port, choose the **FXS** or **DID** radio button. If the trunk type is changed from DID to FXS, inputs for the Battery Reversal and Caller ID options are disabled until the change is applied to the device by clicking **Apply**.
Description	Enter the identifying information for the port.
Shutdown Voice Port?	To shut down the voice port, click the **Yes** radio button. To bring up the voice port, click the **No** radio button.
Station Number (FXS and FXO ports)	Enter the station number associated with the voice port. This information is sent when a user places a call.
Destination Number (FXO ports)	Enter a default destination number for incoming telephone calls.
Station ID (FXS ports)	Enter the calling station ID. This information is sent when a user places a call.
Send Caller ID (FXS ports)	To send caller ID information when a user places a call, click the **Yes** radio button. To prevent caller ID information from being sent, click the **No** radio button.
Receive Caller ID (FXO ports)	To receive caller ID information, click the **On** radio button. To block the caller ID information, click the **Off** radio button.

Analog Trunks: Advanced Signal Settings Tab

On the Advanced Signal Settings tab, enter settings for FXS or DID signals shown in Table 12-3.

How to get to this screen

Click **Configure > Interface Management > Analog Trunks** > (select a) **Trunk Type > Edit > Advanced Signal Settings** tab.

Click **Configure > Unified Communications > Trunks > Analog Trunks** > (select a) **Trunk Type > Edit > Advanced Signal Settings** tab.

Field Reference

Table 12-3 Advanced Signal Settings Tab

Element	Description
Port Signaling	Select the port signaling. For PRI, select **loopStart** or **groundStart** from the list. For BRI, select **wink-start**, **immediate**, or **delay-dial**
Supervisory Disconnect (FXO port)	Select the signal from the drop-down list. Signaling protocols such as loop-start do not provide means for quickly detecting when the call initiation is terminated prior to call connection. Supervisory disconnect quickly makes this determination and frees valuable resources for other calls.
Dual Tone Detection (FXO port)	Click the **Disable** radio button to configure the FXO voice port to detect voice, fax, and modem traffic when calls are answered. Click the **Enable** radio button to configure the FXO voice port so calls are not recorded as connected until answer supervision is triggered.
Battery Reversal	To disable battery reversal, click the **Disable** radio button. To enable battery reversal, click the **Enable** radio button. FXS ports normally reverse battery upon call connection. If an FXS port is connected to an FXO port that does not support battery reversal detection, disable battery-reversal on the FXS port to prevent unexpected behavior.

Analog Trunks: Advanced Audio Settings Tab

In the Advanced Audio Settings tab, enter settings for audio shown in Table 12-4.

How to get to this screen

Click **Configure > Interface Management > Analog Trunks** > (select a) **Trunk Type > Edit > Advanced Audio Settings** tab.

Click **Configure > Unified Communications > Trunks > Analog Trunks** > (select a) **Trunk Type > Edit > Advanced Audio Settings** tab.

Field Reference

Table 12-4 Advanced Audio Settings Tab

Element	Description
Echo Cancel	To enable the Cisco-proprietary G.165 echo canceller (EC), click the **On** radio button. To disable the Cisco-proprietary G.165 echo canceller (EC), click the **Disable** radio button. Disabling echo cancellation might cause the remote side of a connection to hear an echo. Because echo cancellation is an invasive process that can minimally degrade voice quality, this command should be disabled if it is not needed.
Echo Trail	Choose the echo trail wait time from the list. Echo cancellers are, by design, limited by the total amount of time they will wait for the reflected speech to be received. This amount of time is called an echo trail. The echo trail default is 64 milliseconds. VoIP also has configurable echo trails of 8, 16, 24, and 32 milliseconds.
Impedance	Choose the impedance from the list. 600 ohm impedance is normally used for FXS applications. Complex line impedance is normally used for FXO applications that connect to a PSTN. Usually, either position will provide acceptable performance.
Increase Receive Volume	To change the receive volume, select the volume from the drop-down list.
Decrease Volume Transmit	To change the transmit volume, select the volume from the drop-down list.
Nonlinear Processing	To disable nonlinear processing, click the **Disable** check box. When enabled, it shuts off any signal if no near-end speech is detected.

Analog Trunks: Advanced Timer Settings Tab

The Advanced Timer Settings Tab displays if you are configuring a FXO or FXS port. Enter settings for timers shown in Table 12-5.

How to get to this screen

Click **Configure > Interface Management > Analog Trunks** > (select a) **Trunk Type > Edit > Advanced Timer Settings** tab.

Click **Configure > Unified Communications > Trunks > Analog Trunks** > (select a) **Trunk Type > Edit > Advanced Timer Settings** tab.

Field Reference

Table 12-5 Advanced Timer Settings Tab

Element	Description
Timeouts Initial	Enter the number of seconds the system waits for the caller to input the first digit of the dialed digits.
Interdigit	Enter the length of time allotted for a user to dial a telephone number.
Ringing	Enter the length of time for which a caller can continue ringing a telephone when there is no answer.
Wait to release ports	Enter the time a voice port can be held in a failure state.
Call disconnect	Enter the delay time for releasing the calling voice port after a disconnect tone is received from the called voice port.

Configure a Digital Trunk

You can view and edit a digital trunk voice configuration for each port on the device.

Cisco routing devices support ISDN PRI and ISDN BRI. Both media types use bearer (B) channels and data (D) channels.

Basic Rate Interface (BRI) provides two 64 kbps B channels, and one 16 kbps D channel that carries signaling traffic. The D channel is used by the telephone network to carry instructions about how to handle each of the B channels. ISDN BRI (also referred to as 2B + D) provides a maximum transmission speed of 128 kbps.

Primary Rate Interface (PRI) consists of a single 64 kbps D channel plus 23 (T1) or 30 (E1) B channels.

Only ISDN-PRI Voice mode is supported; Data mode or Voice and Data mode are not supported:

- If the controller is configured as **ISDN-PRI**, the mode is set to ISDN-PRI and cannot be modified. If the controller is configured to support other voice modes, the modes are displayed in a summary table.
- If you have configured the controller timeslots as **ds0-group**, **channel-group**, or **tdm-group**, Cisco Configuration Professional displays the Mode as CAS and you cannot edit the configuration.
- If the controller is configured with **pri-group** with **ds0-group**, **channel-group**, or **tdm-group**, you cannot edit the configuration.

If the device is already configured, Cisco Configuration Professional reads and displays the configuration. If the controller has just the default configuration, Cisco Configuration Professional does not display the configuration. You must configure the **pri-timegroup** to configure the port by using Cisco Configuration Professional.

If T1/E1 card is configured as Media Gateway Control Protocol (MGCP) OOB (out-of-band), Cisco Configuration Professional does not allow you to edit configuration on that port.

How to get to this screen

Click **Configure > Interface Management > Digital Trunks.**

Click **Configure > Unified Communications > Trunks > Digital Trunks**.

Related Links

- Edit a Digital Trunk
- Digital Trunks: T1/E1 Settings
- Digital Trunks: PRI or BRI Settings Tab
- Digital Trunks: PRI or BRI Audio Tab

Field Reference

Table 12-6 Trunks

Element	Description
Trunk Type	Connection type.
Description	Description of the voice port.
Location	Location of the interface.
Associated Timeslots	Time slot range. 1 through 30 for E1. 1 through 24 for T1.
Mode Type	Connection mode of the interface. (Only ISDN-PRI is supported.)

Edit a Digital Trunk

The screen is subdivided by tabs. The active content in the tabs varies depending on which port you are configuring.

The first time a BRI port is configured as a trunk by using the **Digital Trunks** > **Edit** dialog, the global and interface parameters are applied to the device. For T1/E1 ports, the switch type is configured only in global mode.

If network clock type is not supported for switch type selected on the BRI trunk edit dialog and the PRI trunk edit dialog, Cisco Configuration Professional automatically changes the value of the network clock. For example, if you selected NTT for the switch type, only **user** mode is supported. If you change the value to **network** mode, Cisco Configuration Professional automatically changes it back to **user** mode and displays the warning message, “Network mode is not supported.”

Related Links

- Configuring Trunks
- Configure a Digital Trunk
- Digital Trunks: T1/E1 Settings
- Digital Trunks: PRI or BRI Settings Tab
- Digital Trunks: PRI or BRI Audio Tab

Digital Trunks: T1/E1 Settings

The Digital T1/E1 Packet Voice Trunk Network Module provides the gateway to the PSTN allowing users to gain access to the public telephone network to and from traditional PBX, phone, fax, key communication systems, as well as IP telephony.

Enter settings for T1 or E1 trunk shown in Table 12-7.

How to get to this screen

Click **Configure > Interface Management > Digital Trunks** > (select a) **Trunk Type > Edit**.

Click **Configure > Unified Communications > Trunks > Digital Trunks >** (select a) **Trunk Type > Edit**.

Field Reference

Table 12-7 T1/E1

Element	Description
Type	Gateway type.
Description	Description of the gateway. You can have a maximum of 80 characters.
Telephone Mode Settings	
Mode	Not a user configurable parameter. Only ISDN-PRI is supported.

Table 12-7 T1/E1

Element	Description
ISDN Switch Type	Choose the ISDN Switch Type from the drop-down list. The options are: • primary-4ess—Lucent 4ESS switch type for the U.S. • primary-5ess—Lucent 5ESS switch type for the U.S. • primary-dms100—Northern Telecom DMS-100 switch type for the U.S. • primary-dpnss—DPNSS switch type for Europe. • primary-net5—NET5 switch type for UK, Europe, Asia and Australia. • primary-ni—National ISDN Switch type for the U.S. • primary-ntt—NTT switch type for Japan. • primary-qsig—QSIG switch type. • primary-ts014—TS014 switch type for Australia (obsolete).
Timeslots From	Enter a pair of numbers that indicate a range of timeslots. For T1, allowable values are from 1 to 24. For E1, allowable values are from 1 to 30.
Network Clock Priority	Clock source priority, which can range from 1 to 8. **Note** The lower the number, the higher the priority.
Link Settings	
Clock Source	Select the source of the timers. The network clock source can be internal or derived from an external (line) source—for example, PSTN, PBX, or ATM network.

Table 12-7 T1/E1

Element	Description
Framing	Select the framing. Digital T1 packet voice trunk network modules support two types of framing for T1 CAS: ESF (Extended SuperFrame) or SF (SuperFrame), also called D4 framing. Digital E1 packet voice trunk network modules support two types of framing: crc4 (frame alignment signal) or no-crc4. The framing type of the router and switch (CO or PBX) must match.
Linecode	Select the line code. The line encoding of the router and switch (CO or PBX) must match.

Digital Trunks: PRI or BRI Settings Tab

On the Advanced PRI Settings tab or the BRI Settings tab, enter settings for PRI signals shown in Table 12-8.

How to get to this screen

- Click **Configure** > **Interface Management** > **Digital Trunks** > (select a) **Trunk Type** > **Edit** > **PRI Settings** tab.
- Click **Configure** > **Interface Management** > **Digital Trunks** > (select a) **Trunk Type** > **Edit** > **BRI Settings** tab.
- Click **Configure** > **Unified Communications** > **Trunks** > **Digital Trunks** > (select a) **Trunk Type** > **Edit** > **PRI Settings** tab.
- Click **Configure** > **Unified Communications** > **Trunks** > **Digital Trunks** > (select a) **Trunk Type** > **Edit** > **BRI Settings** tab.

Field Reference

Table 12-8 PRI or BRI Settings Tab

Element	Description
Clock Type	Select the clock type. Use the clock slave for out-of-band clocking.
ISDN Overlap Receiving	When enabled, the router waits for all the digits to be received before the call is routed.

Table 12-8 PRI or BRI Settings Tab (continued)

Element	Description
T302 Timeout	Enter the number of milliseconds that the T302 timer should wait before expiring. Valid values for the milliseconds argument range from 500 to 20000. The default value is 10000 (10 seconds).
Companding Type	Select the companding standard used to convert between analog and digital signals in PCM systems.

Digital Trunks: PRI or BRI Audio Tab

In the Advanced PRI Audio tab or the Advanced PRI Audio tab, enter settings for audio shown in Table 12-9.

How to get to this screen

- Click **Configure** > **Interface Management** > **Digital Trunks** > (select a) **Trunk Type** > **Edit** > **PRI Audio** tab.
- Click **Configure** > **Interface Management** > **Digital Trunks** > (select a) **Trunk Type** > **Edit** > **BRI Audio** tab.
- Click **Configure** > **Unified Communications** > **Trunks** > **Digital Trunks** > (select a) **Trunk Type** > **Edit** > **PRI Audio** tab.
- Click **Configure** > **Unified Communications** > **Trunks** > **Digital Trunks** > (select a) **Trunk Type** > **Edit** > **BRI Audio** tab.

Field Reference

Table 12-9 PRI or BRI Audio Tab

Element	Description
Echo Cancel	To enable the Cisco-proprietary G.165 echo canceller (EC), click the **On** radio button. To disable the Cisco-proprietary G.165 echo canceller (EC), click the **Disable** radio button. Disabling echo cancellation might cause the remote side of a connection to hear an echo. Because echo cancellation is an invasive process that can minimally degrade voice quality, this command should be disabled if it is not needed.

Table 12-9 PRI or BRI Audio Tab (continued)

Element	Description
Echo Trail	Choose the echo trail wait time from the list. Echo cancellers are, by design, limited by the total amount of time they will wait for the reflected speech to be received. This amount of time is called an echo trail. The echo trail is normally 64 milliseconds. VoIP also has configurable echo trails of 8, 16, 24, and 32 milliseconds.
Increase Receive Volume	To change the receive volume, select the volume from the drop-down list.
Decrease Volume Transmit	To change the transmit volume, select the volume from the drop-down list.
Nonlinear Processing	To disable nonlinear processing, click the **Disable** check box. When enabled, it shuts off any signal if no near-end speech is detected.

Configuring PSTN Trunk Groups

For information about how to use Cisco Configuration Professional (Cisco CP) to configure the Trunk Groups feature, see the screencast at: http://www.cisco.com/en/US/docs/net_mgmt/cisco_configuration_professional/scrcst/ccpsc.html.

Note You must have internet access to view the screencast.

Configuring SIP Trunks

For information about how to use Cisco Configuration Professional (Cisco CP) to configure the SIP feature, see the screencast at: http://www.cisco.com/en/US/docs/net_mgmt/cisco_configuration_professional/scrcst/ccpsc.html.

Note You must have internet access to view the screencast.

PART 3

Configuring Router Features

This section provides information such as how to create a new connection, how to configure LAN, WAN, and Network Address Translation on the router.

CHAPTER 13

Routing

The Routing window displays the configured static routes and Routing Internet Protocol, (RIP), Open Shortest Path First (OSPF), and Extended Interior Gateway Routing Protocol (EIGRP) configured routes. From this window, you can review the routes, add new routes, edit existing routes, and delete routes.

Note Static and dynamic routes configured for GRE over IPSec tunnels will appear in this window. If you delete a routing entry that is used for GRE over IPSec tunneling in this window, that route will no longer be available to the tunnel.

Static Routing

Destination Network

This is the network that the static route provides a path to.

Forwarding

This is the interface or IP address through which packets must be sent to reach the destination network.

Optional

This area shows whether a distance metric has been entered, and whether or not the route has been designated as a permanent route.

What Do You Want To Do?

If you want to:	Do this:
Add a static route.	Click **Add**, and create the static route in the Add a Static Route window.
Edit a static route.	Select the static route, and click **Edit**. Edit the route information in the IP Static Route window. When a route has been configured that Cisco CP does not support, the Edit button is disabled.
Delete a static route.	Select the static route, and click **Delete**. Then, confirm the deletion in the warning window.
Delete all static routes.	Click **Delete All**. Then, confirm the deletion in the warning window.

Note

- If Cisco CP detects a previously configured static route entry that has the next hop interface configured as the "Null" interface, then the static route entry will be read-only.
- If Cisco CP detects a previously configured static route entry with "tag" or "name" options, that entry will be read-only.
- If you are configuring a Cisco 7000 router, and the interface used for a next hop is unsupported, that route will be marked as read only.
- Read-only entries cannot be edited or deleted using Cisco CP.

Dynamic Routing

This portion of the window allows you to configure RIP, OSPF, and EIGRP dynamic routes.

Item Name

If no dynamic routes have been configured, this column contains the text RIP, OSPF, and EIGRP. When one or more routes have been configured, this column contains the parameter names for the type of routing configured.

Routing Protocol	Configuration Parameters
RIP	RIP Version, Network, Passive Interface
OSPF	Process ID
EIGRP	Autonomous System Number

Item Value

This column contains the text "Enabled," and configuration values when a routing type has been configured. It contains the text "Disabled" when a routing protocol has not been configured.

What Do You Want To Do?

If you want to:	Do this:
Configure an RIP route.	Select the RIP tab and click **Edit**. Then, configure the route in the RIP Dynamic Route window.
Configure an OSPF route.	Select the OSPF tab and click **Edit**. Then, configure the route in the displayed window.
Configure an EIGRP route.	Select the EIGRP tab and click **Edit**. Then, configure the route in the displayed window.

Add or Edit IP Static Route

Use this window to add or edit a static route.

Destination Network

Enter the destination network address information in these fields.

Prefix

Enter the IP address of the destination network. For more information, refer to Available Interface Configurations.

Prefix Mask

Enter the destination address subnet mask.

Make this the default route

Check this box to make this the default route for this router. A default route forwards all the unknown outbound packets through this route.

Forwarding

Specify how to forward data to the destination network.

Interface

Click **Interface** if you want to select the interface of the router that forwards the packet to the remote network.

IP Address

Click **IP Address** if you want to enter the IP Address of the next hop router that receives and forwards the packet to the remote network.

Optional

You can optionally provide a distance metric for this route, and designate it as a permanent route.

Distance Metric for this route

Enter the metric value that has to be entered in the routing table. Valid values are 1 through 255.

Permanent Route

Check this box to make this static route entry a permanent route. Permanent routes are not deleted even if the interface is shut down or the router is unable to communicate with the next router.

Add or Edit an RIP Route

Use this window to add or edit a Routing Internet Protocol (RIP) route.

RIP Version

The values are RIP version 1, RIP version 2, and Default. Select the version supported by the Cisco IOS image that the router is running. When you select version 1, the router sends version 1 RIP packets and can receive version 1 packets. When you select version 2, the router sends version 2 RIP packets and can receive version 2 packets. When you select Default, the router sends version 1 packets, and can receive both version 1 and version 2 RIP packets.

IP Network List

Enter the networks on which you want to enable RIP. Click **Add** to add a network. Click **Delete** to delete a network from the list.

Available Interface List

The available interfaces are shown in this list.

Make Interface Passive

Check the box next to the interface if you do not want it to send updates to its neighbor. The interface will still receive routing updates, however.

Add or Edit an OSPF Route

Use this window to add or edit an Open Shortest Path First (OSPF) route.

OSPF Process ID

This field is editable when OSPF is first enabled; it is disabled once OSPF routing has been enabled. The process ID identifies the router's OSPF routing process to other routers.

IP Network List

Enter the networks that you want to create routes to. Click **Add** to add a network. Click **Delete** to delete a network from the list.

Network

The address of the destination network for this route. For more information, refer to Available Interface Configurations.

Mask

The subnet mask used on that network.

Area

The OSPF area number for that network. Each router in a particular OSPF area maintains a topological database for that area.

Note If Cisco CP detects previously configured OSPF routing that includes "area" commands, then the IP Network List table will be read-only and cannot be edited.

Available Interface List

The available interfaces are shown in this list.

Make Interface Passive

Check the box next to the interface if you do not want it to send updates to its neighbor. The interface will still receive routing updates, however.

Add

Click **Add** to provide an IP address, network mask, and area number in the IP address window.

Edit

Click **Edit** to edit the IP address, network mask, or area number in the IP address window.

Add or Edit EIGRP Route

Use this window to add or delete an Extended IGRP (EIGRP) route.

Autonomous System Number

The autonomous system number is used to identify the router's EIGRP routing process to other routers.

IP Network List

Enter the networks that you want to create routes to. Click **Add** to add a network. Click **Delete** to delete a network from the list.

Available Interface List

The available interfaces are shown in this list.

Make Interface Passive

Check the box next to the interface if you do not want it to send updates to its neighbor. The interface will neither send nor receive routing updates.

Caution When you make an interface passive, EIGRP suppresses the exchange of hello packets between routers, resulting in the loss of their neighbor relationship. This not only stops routing updates from being advertised, but also suppresses incoming routing updates.

Add

Click **Add** to add a destination network IP address to the Network list.

Delete

Select an IP address, and click **Delete to remove an IP address** from the Network list.

CHAPTER 14

Authentication, Authorization, and Accounting

Cisco IOS Authentication, Authorization, and Accounting (AAA) is an architectural framework for configuring a set of three independent security functions in a consistent manner. AAA provides a modular way of performing authentication, authorization, and accounting services.

Cisco IOS AAA provides the following benefits:

- Increased flexibility and control
- Scalability
- Standardized authentication methods. Cisco CP enables you to configure the Remote Authentication Dialin User Service (RADIUS), and the Terminal Access Controller Access Control System Plus (TACACS+) authentication methods.

This chapter contains the following section:

- Configuring AAA
- AAA Screen Reference

Configuring AAA

To configure AAA, complete the following steps:

Step 1 In the Cisco CP navigation pane, click **Configure > Router > AAA > Overview**.

Step 2 In the AAA screen, click **Enable AAA**. This enables AAA on the router.

Step 3 Click **+** (the plus sign) next to the AAA folder to display other AAA branches.

Step 4 Click the branch for the type of configuration you need to perform.

Step 5 In the displayed AAA screen, click **Add** to create a configuration, or select an existing entry in the screen, and click **Edit** to change configuration settings.

Step 6 Make configuration settings in the displayed dialogs, and click **OK** to send the configuration to the router.

AAA Screen Reference

The topics in this section describe the AAA configuration screens:

- AAA Overview Screen
- AAA Servers and Server Groups
- AAA Servers
- Add or Edit a TACACS+ Server
- Add or Edit a RADIUS Server
- AAA Server Groups
- Add or Edit AAA Server Group
- Authentication, Authorization, and Accounting Policies
- Authentication and Authorization
- Authentication NAC
- Authentication 802.1x
- Add or Edit a Method List for Authentication or Authorization

AAA Overview Screen

This screen is located at the top level of the AAA tree. It provides a summary view of the AAA configuration on the router. To view more detailed information or to edit the AAA configuration, click the appropriate node on the AAA tree.

Field Reference

Table 14-1 AAA Main Screen Fields

Element	Description
Enable AAA Disable AAA	If AAA is enabled, the button name is Disable AAA. If AAA is disabled, the button name is Enable AAA. AAA is enabled by default. If you click **Disable AAA**, Cisco CP displays a message telling you that it will make configuration changes to ensure that the router can be accessed. Disabling AAA will prevent you from configuring your router as an Easy VPN server, and will prevent you from associating user accounts with command line interface (CLI) views.
AAA Servers and Groups	This read-only field displays a count of the AAA servers and server groups. The router relays authentication, authorization, and accounting requests to AAA servers. AAA servers are organized into groups to provide the router with alternate servers to contact if the first server contacted is not available.
Authentication Policies	This read-only field lists configured authentication policies. Authentication policies define how users are identified. To edit authentication policies, click the **Login** sub-node under **Authentication Policies** in the AAA tree.
Authorization Policies	This read-only field lists configured authorization policies. Authorization policies define the methods that are used to permit or deny a user login. To edit authorization policies, click **Authorization Policies** in the AAA tree. To edit authorization policies (Exec Authorization and Network Authorization), click the **Exec** and **Network** sub-nodes respectively under the **Authorization Policies** node in the AAA tree.

AAA Servers and Server Groups

This window provides a description of AAA servers and AAA server groups.

To display the AAA Servers window, click the **AAA Servers** branch.

To display the AAA Server Groups window, click the **AAA Server Groups** branch.

AAA Servers

This window lets you view a snapshot of the information about the AAA servers that the router is configured to use. The IP address, server type, and other parameters are displayed for each server.

Field Reference

Table 14-2 AAA Servers Fields

Element	Description
Global Settings	Click **Global Settings** to make global settings for TACACS+ and RADIUS servers. In the Edit Global Settings window, you can specify how long to attempt contact with an AAA server before going on to the next server, the key to use when contacting TACACS+ or RADIUS servers, and the interface on which TACACS+ or RADIUS packets will be received. These settings will apply to all servers for which server-specific settings have not been made.
Add	Click **Add** to add a TACACS+ or a RADIUS server to the list.
Edit	Click **Edit** to edit the information for the selected AAA server.
Delete	Click **Delete** to delete the information for the selected AAA server.
Server IP	The IP address of the AAA server.
Parameters	This column lists the timeout, key, and other parameters for each server.

Add or Edit a TACACS+ Server

Add or edit information for a TACACS+ server in this window.

Field Reference

Table 14-3 Add or Edit a TACACS+ Server Fields

Element	Description
Server IP or Host	Enter the IP address or the host name of the server. If the router has not been configured to use a Domain Name Service (DNS) server, enter an IP address.
Single Connection to Server	Check this box if you want the router to maintain a single open connection to the TACACS+ server, rather than opening and closing a TCP connection each time it communicates with the server. A single open connection is more efficient because it allows the TACACS+ server to handle a higher number of TACACS+ operations. **Note** This option is supported only if the TACACS+ server is running CiscoSecure version 1.0.1 or later.
Server-Specific Setup (Optional)	Use this area if you want to override AAA server global settings, and specify a server-specific timeout value and encryption key. You can make the following settings: • Timeout (seconds)—Enter the number of seconds that the router should attempt to contact this server before going on to the next server in the group list. If you do not enter a value, the router will use the value configured in the AAA Servers Global Settings window. • Configure Key—Optional. Check **Configure Key** and enter the key to use to encrypt traffic between the router and this server. If you do not enter a value, the router will use the value configured in the AAA Servers Global Settings window. • New Key/Confirm Key—Enter the key and reenter it for confirmation.

Add or Edit a RADIUS Server

Add or edit information for a RADIUS server in this window.

Field Reference

Table 14-4 Add or Edit a RADIUS Server Fields

Element	Description
Server IP or Host	Enter the IP address or the host name of the server. If the router has not been configured to use a Domain Name Service (DNS) server, enter an IP address.
Authorization Port	Specify the server port to use for authorization requests. The default is 1645.
Accounting Port	Specify the server port to use for accounting requests. The default is 1646.
Timeout in seconds	Optional. Enter the number of seconds that the router should attempt to contact this server before going on to the next server in the group list. If you do not enter a value, the router will use the value configured in the AAA Servers Global Settings window.
Configure Key	Optional. Enter the key to use to encrypt traffic between the router and this server. If you do not enter a value, the router will use the value configured in the AAA Servers Global Settings window. • New Key and Confirm Key—Enter the key and reenter it for confirmation.

Edit Global Settings

You can specify communication settings that will apply to all communications between the router and AAA servers in this window. Any communications settings made for a specific router will override settings made in this window.

Field Reference

Table 14-5 Global Settings Fields

Element	Description
TACACS+ Server RADIUS Server	Click the appropriate button to specify the server type for which you are setting global parameters. If you select TACACS+ Server, the parameters will apply to all communication with TACACS+ servers that do not have server specific parameters set. If you select RADIUS Server, the parameters will apply to all communication with RADIUS servers that do not have server specific parameters set.
Timeout (seconds)	Enter the number of seconds to wait for a response from the RADIUS or TACACS+ server
Key	Enter the encryption key for all communication between the router and the TACACS+ or RADIUS servers.
Select the source interface	Check this box if you want to specify a single interface on which the router is to receive TACACS+ or RADIUS packets. Interface—Select the router interface on which the router is to receive TACACS+ or RADIUS packets.If the **Select the source interface** box is not checked, this field will be disabled.

AAA Server Groups

This window displays the AAA server groups configured on this router. If no AAA servers have been configured, this window is empty.

Field Reference

Table 14-6 AAA Server Groups Fields

Element	Description
Add	Click the **Add** button to create a RADIUS server group. After you create this group, the name and group members are displayed in this window.
Edit	Click **Edit** to modify the information for the highlighted server group.

Table 14-6 AAA Server Groups Fields

Element	Description
Delete	Click **Delete** to remove the highlighted server group.
Group Name	The name of the server group. Server group names allow you to use a single name to reference multiple servers.
Type	The type of servers in the selected group, either TACACS+, or RADIUS.
Group Members	The IP addresses or host names of the AAA servers in this group.

Add or Edit AAA Server Group

Create or modify an AAA server group in this window.

Field Reference

Table 14-7 Add or Edit AAA Server Group Fields

Element	Description
Group Name	Enter a name for the group.
Server Type	Select the Server type, either RADIUS, or TACACS+. **Note** This field may be protected and set to a specific type, depending on the configuration that you are performing.
Select the servers that need to be placed in this AAA server group	This area lists the IP addresses of all the AAA servers configured on the router of the type chosen, along with the Authorization and Accounting ports used. Check the **Select** box next to the servers that you want to add.

Authentication, Authorization, and Accounting Policies

The Authentication Policies, Authorization Policies, and Accounting Policies windows summarize the authentication policy information on the router.

Field Reference

Table 14-8 Authentication, Authorization, Accounting Policy Fields

Element	Description
Authentication Type/Authorization Type/Accounting Type	The type of authentication policy.
Number of Policies	The number of policies of this type.
Usage	The usage description for these policies.

Authentication and Authorization

The Login and the Exec and Network authorization windows display the method lists used to authenticate logins, NAC requests and authorize Exec command level and network requests. You can review and manage these method lists from these windows.

Field Reference

Table 14-9 Authentication and Authorization Fields

Element	Description
Add Edit Delete	Use these buttons to create, edit, and remove method lists.
List Name	The method list name. A method list is a sequential list describing the authentication methods to be queried in order to authenticate a user.

Table 14-9 Authentication and Authorization Fields

Element	Description
Method 1	The method that the router will attempt first. If one of the servers in this method authenticates the user (sends a PASS response), authentication is successful. If a server returns a FAIL response, authentication fails. If no servers in the first method respond, then the router uses the next method in the list. Methods can be ordered when you create or edit a method list.
Method 2 Method 3 Method 4	The methods, in order, that the router will use if the servers referenced in method 1 do not respond. If there are fewer than four methods, the positions for which no list has been configured are kept empty.

Authentication NAC

The Authentication NAC window displays the EAPoUDP method lists configured on the router.You can specify additional method lists in this window if you want the router to attempt the methods that you enter before resorting to the default method list.

Field Reference

Table 14-10 NAC Authentication Fields

Element	Description
Add Edit Delete	Use these buttons to create, edit, and remove method lists.
List Name	The method list name. A method list is a sequential list describing the authentication methods to be queried in order to authenticate a user. If the NAC wizard was used to create a NAC configuration, the list name “default” is displayed in this column.

Table 14-10 NAC Authentication Fields

Element	Description
Method 1	The method that the router will attempt first. If the NAC wizard was used to create a NAC configuration, the method name "group SDM_NAC_Group" is displayed in this column. If one of the servers in this method authenticates the user (sends a PASS response), authentication is successful. If a server returns a FAIL response, authentication fails. If no servers in the first method respond, then the router uses the next method in the list. Methods can be ordered when you create or edit a method list.
Method 2 Method 3 Method 4	The methods, in order, that the router will use if the servers referenced in method 1 do not respond. If there are fewer than four methods, the positions for which no list has been configured are kept empty.

Authentication 802.1x

The Authentication 802.1x window displays the method lists configured for 802.1x authentication.

Note You cannot specify additional method lists for 802.1x configuration.

Field Reference

Table 14-11 802.1x Authentication Fields

Element	Description
Add Edit Delete	Use these buttons to create, edit, and remove method lists.
List Name	The method list name. A method list is a sequential list describing the authentication methods to be queried in order to authenticate a user. If the LAN wizard has been used to create an 802.1x configuration, the list name "default" is displayed in this column.
Method 1	The method that the router will attempt first. If one of the servers in this method authenticates the user (sends a PASS response), authentication is successful. If a server returns a FAIL response, authentication fails. If no servers in the first method respond, then the router uses the next method in the list. Methods can be ordered when you create or edit a method list. If the LAN wizard has been used to create an 802.1x configuration, the Method name "group SDM_802.1x" is displayed in this column.
Method 2 Method 3 Method 4	The methods that the router will use if the servers referenced in method 1 do not respond. If there are fewer than four methods, the positions for which no list has been configured are kept empty.

Add or Edit a Method List for Authentication or Authorization

A method list is a sequential list describing the authentication methods to be queried in order to authenticate a user. Method lists enable you to designate one or more security protocols to be used for authentication, thus ensuring a backup system for authentication in case the initial method fails.

Cisco IOS software uses the first listed method to authenticate users. If that method fails to respond, the Cisco IOS software selects the next authentication method listed in the method list. This process continues until there is successful communication with a listed authentication method, or all methods defined in the method list are exhausted.

It is important to note that the Cisco IOS software attempts authentication with the next listed authentication method only when there is no response from the previous method. If authentication fails at any point in this cycle—meaning that the security server or local username database responds by denying the user access—the authentication process stops and no other authentication methods are attempted.

Field Reference

Table 14-12 Add a Method List for Authentication or Authorization Fields

Element	Description
Name Specify	Choose the name **Default** in the Name list, or choose **User Defined**, and enter a method list name in the Specify field.
Methods	A method is a configured server group. Up to four methods can be specified and placed in the list in the order you want the router to use them. The router will attempt the first method in the list. If the authentication request receives a PASS or a FAIL response, the router does not query further. If the router does not receive a response by using the first method, it uses the next method in the list, and continues to the end of the list until it receives a PASS or a FAIL response.
Add	Click **Add** to add a method to the list. If there are no configured server groups to add, you can configure a server group in the window displayed.
Delete	Click this button to delete a method from the list.

Table 14-12 Add a Method List for Authentication or Authorization Fields

Element	Description
Move Up Move Down	The router attempts the methods in the order they are listed in this window. Click **Move Up** to move a method up the list. Click **Move Down** to move a method further down the list. The method "none" will always be last in the list. No other method in the list can be moved below it. This is an IOS restriction. IOS will not accept any method name after the method name "none" has been added to a Method List.
Enable Password Aging	Check **Enable Password Aging** to have the Easy VPN Server notify the user when their password has expired and prompt them to enter a new password.

Authorization Web Authentication

The Authorization Web Authentication window displays the method lists configured for WebAuth authorization.

How to get to this page

Click **Configure > Router > AAA > Authorization Policies > Web Auth**

Related Topics

- Add or Edit a Method List for Authentication or Authorization, page 14-12

Field Reference

Table 14-13 WebAuth Authorization Fields

Element	Description
Add Edit Delete	Use these buttons to create, edit, and remove method lists.
List Name	The method list name. A method list is a sequential list describing the authorization methods to be queried in order to authorize a user.

Table 14-13 WebAuth Authorization Fields

Element	Description
Method 1	The method that the router will attempt first. If one of the servers in this method authorizes the user (sends a PASS response), authorization is successful. If a server returns a FAIL response, authorization fails. If no servers in the first method respond, then the router uses the next method in the list. Methods can be ordered when you create or edit a method list.
Method 2 Method 3 Method 4	The methods that the router will use if the servers referenced in method 1 do not respond. If there are fewer than four methods, the positions for which no list has been configured are kept empty.

Accounting 802.1x

The Accounting 802.1x window displays the method lists configured for 802.1x accounting.

Note You cannot specify additional method lists for 802.1x configuration.

How to get to this page

Click **Configure > Router > AAA > Accounting Policies > 802.1x**

Related Topics

- Authentication, Authorization, and Accounting Policies, page 14-8
- Accounting Web Authentication, page 14-16

Field Reference

Table 14-14 802.1x Accounting Fields

Element	Description
Add Edit Delete	Use these buttons to create, edit, and remove method lists.
List Name	The method list name. A method list is a sequential list describing the accounting methods to be queried in order to authenticate a user. If the LAN wizard has been used to create an 802.1x configuration, the list name "default" is displayed in this column.
Method 1	The method that the router will attempt first. If one of the servers in this method authenticates the user (sends a PASS response), authentication is successful. If a server returns a FAIL response, authentication fails. If no servers in the first method respond, then the router uses the next method in the list. Methods can be ordered when you create or edit a method list. If the LAN wizard has been used to create an 802.1x configuration, the Method name "group SDM_802.1x" is displayed in this column.
Method 2 Method 3 Method 4	The methods that the router will use if the servers referenced in method 1 do not respond. If there are fewer than four methods, the positions for which no list has been configured are kept empty.

Accounting Web Authentication

The Accounting Web Authentication window displays the method lists configured for WebAuth accounting.

How to get to this page

Click **Configure > Router > AAA > Accounting Policies > Web Auth**

Related Topics

- Accounting 802.1x, page 14-15
- Authentication, Authorization, and Accounting Policies, page 14-8

Field Reference

Table 14-15 WebAuth Accounting Fields

Element	Description
Add Edit Delete	Use these buttons to create, edit, and remove method lists.
List Name	The method list name. A method list is a sequential list describing the accounting methods to be queried in order to account a user.
Method 1	The method that the router will attempt first. If one of the servers in this method accounts the user (sends a PASS response), accounting is successful. If a server returns a FAIL response, accounting fails. If no servers in the first method respond, then the router uses the next method in the list. Methods can be ordered when you create or edit a method list.
Method 2 Method 3 Method 4	The methods that the router will use if the servers referenced in method 1 do not respond. If there are fewer than four methods, the positions for which no list has been configured are kept empty.

CHAPTER 15

ACL

Rules define how the router will respond to a particular kind of traffic. Using Cisco CP, you can create access rules that cause the router to block certain types of traffic while permitting other types, NAT rules that define the traffic that is to receive address translation, and IPSec rules that specify which traffic is to be encrypted. Cisco CP also provides default rules that are used in guided configurations, and that you can examine and use when you create your own access rules. It also allows you to view rules that were not created using Cisco CP, called external rules, and rules with syntax that Cisco CP does not support, called unsupported rules.

Use the Rules screen to view a summary of the rules in the router's configuration and to navigate to other windows to create, edit, or delete rules.

Category

A type of rule. One of the following:

ACL Editor	Rules that govern the traffic that can enter and leave the network. These rules are used by router interfaces, and by VTY lines that let users log on to the router.
NAT Rules	Rules that determine how private IP addresses are translated into valid Internet IP addresses.
IPSec Rules	Rules that determine which traffic will be encrypted on secure connections.

NAC Rules	Rules that specify the IP addresses to be admitted to the network, or blocked from the network.
Firewall Rules	Rules that can specify source and destination addresses, type of traffic, and whether the traffic should be permitted or denied.
QoS Rules	Rules that specify traffic that should belong to the QoS Class that the rule is associated with.
Unsupported Rules	Rules that have not been created using Cisco CP, and that Cisco CP does not support. These rules are read only, and cannot be modified using Cisco CP.
Externally Defined Rules	Rules that have not been created using Cisco CP, but that Cisco CP does support. These rules may not be associated with any interface.

No. of Rules

The number of rules of this type.

Description

A description of the rule if one has been entered.

To configure rules:

Click the category of rule in the rule tree to display the window for that type of rule. Create and edit rules from that window.

The help topic for these windows contains general procedures that you may find helpful. Useful Procedures for Access Rules and Firewalls contains step by step procedures for other tasks.

Useful Procedures for Access Rules and Firewalls

This section contains procedures that you may find useful.

- How Do I View Activity on My Firewall?
- How Do I Configure a Firewall on an Unsupported Interface?
- How Do I Configure a Firewall After I Have Configured a VPN?
- How Do I Permit Specific Traffic Through a DMZ Interface?
- How Do I Modify an Existing Firewall to Permit Traffic from a New Network or Host?
- How Do I Configure NAT Passthrough for a Firewall?
- How Do I Permit Traffic Through a Firewall to My Easy VPN Concentrator?
- How Do I Associate a Rule with an Interface?
- How Do I Disassociate an Access Rule from an Interface
- How Do I Delete a Rule That Is Associated with an Interface?
- How Do I Create an Access Rule for a Java List?

Rules Windows

These windows let you examine, create, edit, and delete rules.

- ACL Editor window—ACL editor most commonly defines the traffic that you want to permit or deny entry to your LAN or exit from your LAN, but they can be used for other purposes as well.
- NAT Rules window—NAT rules are used to specify a set of addresses to translate.
- IPSec Rules window—IPSec rules are extended rules used in IPSec policies to specify which traffic will be encrypted for VPN connections.
- NAC Rules window—Rules that specify the IP addresses to be admitted to the network, or blocked from the network.
- Firewall Rules window—Rules that can specify source and destination addresses, type of traffic, and whether the traffic should be permitted or denied.

- QoS Rules window—Rules that specify traffic that should belong to the QoS Class that the rule is associated with.
- Unsupported Rules window—Unsupported rules contain syntax or keywords that Cisco CP does not support. Unsupported rules may affect the way the router operates, but are marked as read-only by Cisco CP.
- Externally Defined Rules window—Externally defined rules are those that Cisco CP was not used to create.
- NAC Rules window. NAC rules are used in the NAC exception policy to specify hosts that are to be exempted from the NAC validation process. They are also used to define the hosts or networks for admission control.

The upper portion of the screen lists the access rules that have been configured on this router. The lower portion of the window lists the rule entries associated with the selected rule. A rule entry consists of criteria that incoming or outgoing traffic is compared against, and the action to take on traffic matching the criteria. If traffic does not match the criteria of any of the entries in this box, it is dropped.

First column

This column may contain icons that indicate the status of a rule.

 If the rule is read only, the read-only icon will appear in this column.

Name/Number

The name or the number of the access rule.

The numbers 1 through 99 are used to identify standard access lists. The numbers 100 through 199 are used to identify extended access lists. Names, which can contain alphabetic characters, allow you to extend the range of standard access lists beyond 99, and extended access lists beyond 199.

Used By

The name of the interface or VTY numbers to which this rule has been applied.

Type

The type of rule, either standard or extended.

Standard rules compare a packet's source IP address against its IP address criteria to determine a match. The rule's IP address criteria can be a single IP address, or portions of an IP address, defined by a wildcard mask.

Extended rules can examine a greater variety of packet fields to determine a match. Extended rules can examine both the packet's source and destination IP addresses, the protocol type, the source and destination ports, and other packet fields.

Access rules can be either standard rules or extended rules. IPSec rules have to extended rules because they must be able to specify a service type. Externally defined and unsupported rules may be either standard or extended.

Description

A description of the rule, if one has been entered.

First Column (Rule Entry Area)

 Permit traffic.

 Deny traffic.

Action

The action to take when a packet matching the criteria in this entry arrives on the interface. Either Permit or Deny:

- Permit—Allow traffic matching the criteria in this row.
- Deny—Do not allow traffic matching the criteria in this row.

Click Meanings of the Permit and Deny Keywords to learn more about the action of permit and the action of deny in the context of a specific type of rule.

Source

The source IP address criteria that the traffic must match. This column may contain:

- An IP address and wildcard mask. The IP address specifies a network, and the wildcard mask specifies how much of the rule's IP address the IP address in the packet must match.

- The keyword **any.** Any indicates that the source IP address can be any IP address
- A host name.

Destination

For extended rules, the destination IP address criteria that the traffic must match. The address may be for a network, or a specific host. This column may contain:

- An IP address and wildcard mask. The IP address specifies a network, and the wildcard mask specifies how much of the rule's IP address the IP address in the packet must match.
- The keyword **any.** Any indicates that the source IP address can be any IP address
- A host name.

Service

For extended rules, the service specifies the type of traffic that packets matching the rule must contain. This is shown by displaying the service, such as echo-reply, followed by the protocol, such as ICMP. A rule permitting or denying multiple services between the same end points must contain an entry for each service.

Attributes

This field can contain other information about this entry, such as whether logging has been enabled.

Description

A short description of the entry.

What do you want to do?

If you want to:	Do this:
Add a rule.	Click the **Add** button and create the rule in the windows displayed.
Edit a rule, or edit a rule entry.	Select the access rule and click **Edit**. Then edit the rule in the Edit rule window displayed.
Associate a rule with an interface.	See How Do I Associate a Rule with an Interface?
Delete a rule that has not been associated with an interface.	Select the Access rule, and click **Delete**.
Delete a rule that has been associated with an interface	Cisco CP does not permit you to delete a rule that has been associated with an interface. In order to delete the rule, you must first disassociate it from the interface. See How Do I Delete a Rule That Is Associated with an Interface?
What I want to do is not described here.	The following link contains procedures that you may want to consult: Useful Procedures for Access Rules and Firewalls.

Add or Edit a Rule

This window lets you add or edit a rule you have selected in the Rules window. You can rename or renumber the rule, add, change, reorder, or delete rule entries, and add or change the description of the rule.

Name/Number

Add or edit the name or number of the rule.

Standard rules must be numbered in the range 1–99, or 1300–1999.

Extended rules must be numbered in the range 100–199 or 2000–2699.

Names, which can contain alphabetic characters, allow you to associate a meaningful label to the access rule.

Type

Select the type of rule you are adding. Standard rules let you have the router examine the source host or network in the packet. Extended rules let you have the router examine the source host or network, the destination host or network, and the type of traffic that the packet contains.

Description

You can provide a description of the rule in this field. The description must be less than 100 characters long.

Rule Entry List

This list shows the entries that make up the rule. You can add, edit, and delete entries. You can also reorder them to change the order in which they are evaluated.

Observe the following guidelines when creating rule entries:

- There must be at least one permit statement in the list; otherwise, all traffic will be denied.
- A permit all or deny all entry in the list must be the last entry.
- Standard entries and extended entries cannot be mixed in the same rule.
- No duplicate entries can exist in the same rule.

Clone

Click this button to use the selected entry as a template for a new entry. This feature can save you time, and help reduce errors. For example, if you want to create a number of extended rule entries with the same source and destination, but different protocols or ports, you could create the first one using the Add button. After creating the first entry, you could copy it using **Clone**, and change the protocol field or port field to create a new entry.

Interface Association

Click the **Associate** button to apply the rule to an interface.

Note The Associate button is enabled only if you are adding a rule from the Access Rules window.

What do you want to do?

If you want to:	Do this:
Add or edit a rule entry.	Click **Add,** and create the entry in the window displayed. Or click **Edit**, and change the entry in the window displayed.
Add a rule entry using an existing entry as a template.	Select the entry you want to use as a template, and click **Clone**. Then create the entry in the dialog box displayed. The dialog box displays the contents of the entry you selected so that you can edit it to create a new entry.
Reorder rule entries to make sure that the router evaluates particular entries.	Select the rule entry, and click the **Move Up** or the **Move Down** button to move the entry where you want it.
Associate a rule with an interface.	Click **Associate** and select the interface and direction in the Associate with an Interface window. If the **Associate** button is not enabled, you can associate the rule with an interface by double-clicking the interface in the Interfaces and Connections window and using the Associate tab.
Delete a rule entry.	Select the rule entry, and click **Delete**. Then confirm deletion in the Warning window displayed.
Learn more about rules.	Explore the resources on Cisco.com. The document *Configuring IP Access Lists* at following link contains information about IP access lists: http://www.cisco.com/en/US/products/sw/secursw/ps1018/products_tech_note09186a00800a5b9a.shtml
What I want to do is not described here.	The following link contains procedures that you may want to consult: Useful Procedures for Access Rules and Firewalls

Associate with an Interface

You can use this window to associate a rule you have created from the Access Rules window with an interface and to specify whether it applies to outbound traffic or inbound traffic.

Select an Interface

Select the interface to which you want this rule to apply.

Specify a Direction

If you want the router to check packets inbound to the interface, click **Inbound**. The router checks for a match with the rule before routing it; the router accepts or drops the packet based on whether the rule states permit or deny. If you want the router to forward the packet to the outbound interface before comparing it to the entries in the access rule, click **Outbound**.

If Another Rule is Already Associated with the Interface

If an information box appears that tells that another Access Rule is associated with the interface and direction you specified, you can either cancel the operation, or you can continue, by appending the rule entries to the rule that is already applied to the interface, or by disassociating the rule with the interface and associating the new rule.

What do you want to do?

If you want to:	Do this:
Cancel the operation and preserve the association between the interface and the existing rule.	Click **No**. The association between the existing rule and the interface is preserved, and the rule that you created in the Add a Rule window is saved. You can examine the existing rule and the new rule and decide whether you want to replace the existing rule or to merge the entries of the new rule with the existing rule.

If you want to:	Do this:
Continue, and merge the entries of the rule you created with the entries of the existing rule.	Click **Yes**. Then, when the window appears that asks whether you want to merge or replace the existing rule, click **Merge**. The entries you created for the new rule are appended after the last entry of the existing rule. **Note** If the rule you want to merge is not compatible with the existing rule, you will be allowed only to replace the existing rule.
Continue, and replace the rule existing rule with the rule you created.	Click **Yes**. Then, when the window appears that asks you if you want to merge or replace the existing rule, click **Replace**. The rule you are replacing is not erased. It is just disassociated with the interface and direction.

Add a Standard Rule Entry

A standard rule entry allows you to permit or deny traffic that came from a specified source. The source can be a network or a host within a specific network. You can create a single rule entry in this window, but you can return to this window to create additional entries for a rule if you need to.

Note Any traffic that does not match the criteria in one of the rule entries you create is implicitly denied. To ensure that traffic you do not intend to deny is permitted, you must append explicit permit entries to the that rule you are configuring.

Action

Select the action you want the router to take when a packet matches the criteria in the rule entry. The choices are **Permit** and **Deny**. What Permit and Deny do depends on the type of rule in which they are used. In Cisco CP, standard rule entries can be used in access rules, NAT rules, and in access lists associated with

route maps. Click Meanings of the Permit and Deny Keywords to learn more about the action of Permit and the action of Deny in the context of a specific type of rule.

Source Host/Network

The source IP address criteria that the traffic must match. The fields in this area of the window change, based on the value of the Type field.

Type

Select one of the following:

- A Network. Select if you want the action to apply to all the IP addresses in a network.
- A Host Name or IP Address. Select if you want the action to apply to a specific host or IP address.
- Any IP address. Select if you want the action to apply to any IP address.

IP Address

If you selected **A Network or if you selected A Host Name or IP address**, enter the IP address in this field. If the address you enter is a network address, enter a wildcard mask to specify the parts of the network address that must be matched.

Mask

If you selected **A Network or if you selected A Host Name or IP address**, either select the wildcard mask from this list, or enter a custom wildcard mask. A binary 0 in a wildcard mask means that the corresponding bit in a packet's IP address must match exactly. A binary 1 in a wildcard mask means that the corresponding bit in the packet's IP address need not match.

Hostname/IP

If you selected **A Host Name or IP address** in the Type field, enter the name or the IP address of the host. If you enter a hostname, the router must be configured to use a DNS server.

Description

You can enter a short description of the entry in this field. The description must be fewer than 100 characters long.

Log Matches Against This Entry

If you have specified syslog in System Properties, you can check this box; matches will be recorded in the system log.

Add an Extended Rule Entry

An extended rule entry allows you to permit or deny traffic based on its source and destination and on the protocol and service specified in the packet.

Note Any traffic that does not match the criteria in one of the rule entries you create is implicitly denied. To ensure that traffic you do not intend to deny is permitted, you must append explicit permit entries to the rule that you are configuring.

Action

Select the action you want the router to take when a packet matches the criteria in the rule entry. The choices are **Permit** and **Deny**. If you are creating an entry for an IPSec rule, the choices are **protect the traffic** and **don't protect the traffic**.

What Permit and Deny do depends on the type of rule in which they are used. In Cisco CP, extended rule entries can be used in access rules, NAT rules, IPSec rules, and access lists associated with route maps. Click Meanings of the Permit and Deny Keywords to learn more about the action of Permit and the action of Deny in the context of a specific type of rule.

Source Host/Network

The source IP address criteria that the traffic must match. The fields in this area of the window change, based on the value of the Type field.

Type

Select one of the following:

- A specific IP address. This can be a network address, or the address of a specific host.
- A host name.

- Any IP address.
- Network object group.

IP Address

If you selected **A specific IP address**, enter the **IP address** in this field. If the address you enter is a network address, enter a wildcard mask to specify the parts of the network address that must be matched.

Mask

If you selected **A specific IP address**, either select the wildcard mask from this list, or enter a custom wildcard mask. A binary 0 in a wildcard mask means that the corresponding bit in the packet's IP address must match exactly. A binary 1 in a wildcard mask means that the corresponding bit in the packet's IP address need not match.

Hostname

If you selected **A host name** in the Type field, enter the name of the host.

Network Object Group

If you selected **Network Object Group** in the Type field, click the **...** (more) button—located next to the Network Object Group field—to open the Select Network Object Groups Dialog Box. Select the network object group from the Available Groups pane, and then click **OK**. For details, see Select Network Object Groups Dialog Box, page 16-37.

Destination Host/Network

The source IP address criteria that the traffic must match. The fields in this area of the window change, based on the value of the Type field.

Type

Select one of the following:

- A specific IP address. This can be a network address or the address of a specific host.
- A host name.
- Any IP address.
- Network object group.

Mask

If you selected **A specific IP address**, either select the wildcard mask from this list or enter a custom wildcard mask. A binary 0 in a wildcard mask means that the corresponding bit in the packet's IP address must match exactly. A binary 1 in a wildcard mask means that the corresponding bit in the packet's IP address need not match.

Hostname

If you selected **A host name** in the Type field, enter the name of the host.

Network Object Group

If you selected **Network Object Group** in the Type field, click the **...** (more) button—located next to the Network Object Group field—to open the Select Network Object Groups Dialog Box. Select the network object group from the Available Groups pane, and then click **OK**. For details, see Select Network Object Groups Dialog Box, page 16-37.

Description

You can enter a short description of the entry in this field. The description must be fewer than 100 characters long.

Protocol and Service

Select the protocol and service, if applicable, that you want the entry to apply to. The information that you provide differs from protocol to protocol. Click the protocol to see what information you need to provide.

Source Port

Available when either TCP or UDP is selected. Setting this field will cause the router to filter on the source port in a packet. It is rarely necessary to set a source port value for a TCP connection. If you are not sure you need to use this field, leave it set to **= any**.

Destination Port

Available when either TCP or UDP is selected. Setting this field will cause the router to filter on the destination port in a packet.

If you select this protocol:	You can specify the following in the Source Port and Destination Port fields:
TCP and UDP	Specify the source and destination port by name or number. If you do not remember the name or number, click the **...** button and select the value you want from the Service window. This field accepts protocol numbers from 0 through 65535. • =. The rule entry applies to the value that you enter in the field to the right. • !=. The rule entry applies to any value except the one that you enter in the field to the right. • <. The rule entry applies to all port numbers lower than the number you enter. • >. The rule entry applies to all port numbers higher than the number you enter. • range. The entry applies to the range of port numbers that you specify in the fields to the right.
ICMP	Specify **any** ICMP type, or specify a type by name or number. If you do not remember the name or number, click the **...** button, and select the value you want. This field accepts protocol numbers from 0 through 255.
IP	Specify **any** IP protocol, or specify a protocol by name or number. If you do not remember the name or number, click the **...** button, and select the value you want. This field accepts protocol numbers from 0 through 255.
Service Object Group(s)	Specify the Service Object Group by name. Click the **...** (more) button—located next to the Service Object Group field—to open the Select Service Object Groups Dialog Box. Select the service object group from the Available Groups pane, and then click **OK**. For details, see Select Service Object Groups Dialog Box, page 16-38.

See Services and Ports to see a table containing port names and numbers available in Cisco CP.

Log Matches Against This Entry

If you have configured logging for firewall messages, you can check this box and matches will be recorded in the log file sent to the syslog server. For more information refer to this link: Firewall Log.

Select a Rule

Use this window to select a rule to use.

Rule Category

Select the rule category that you want to select from. The rules in the category you select will appear in the box below the list. If no rules appear in the box, no rules of that category have been defined.

Name/Number

The name or number of the rule.

Used By

How the rule is being used. For example, if the rule has been associated with an interface, the name of the interface. If the rule is being used in an IPSec policy, the name of the policy. Or, if the rule has been used by NAT, this column contains the value NAT.

Description

A description of the rule.

Preview

This area of the screen displays the entries of the selected rule.

Action

Either **Permit** or **Deny**. See Meanings of the Permit and Deny Keywords to learn more about the action of Permit and the action of Deny in the context of a specific type of rule.

Source

The source IP address criteria that the traffic must match. This column may contain the following:

- An IP address and wildcard mask. The IP address specifies a network, and the wildcard mask specifies how much of the rule's IP address the IP address in the packet must match.

- The keyword **any.** Any indicates that the source IP address can be any IP address
- A host name.

Destination

For extended rules, the destination IP address criteria that the traffic must match. The address may be for a network, or a specific host. This column may contain the following:

- An IP address and wildcard mask. The IP address specifies a network, and the wildcard mask specifies how much of the rule's IP address the IP address in the packet must match.
- The keyword **any.** Any indicates that the source IP address can be any IP address
- A host name.

Service

For extended rules, the service specifies the type of traffic that packets matching the rule must contain. This is shown by displaying the service, such as echo-reply, followed by the protocol, such as ICMP. A rule permitting or denying multiple services between the same endpoints must contain an entry for each service.

CHAPTER 16

ACL Object Groups

Object group-based access control lists (ACLs) simplify static and dynamic ACL deployments for large user-access environments on Cisco IOS routers. The following sections provide more information:

- Understanding ACL Object Groups, page 16-1
- ACL Object Groups Basic Workflow, page 16-2
- Understanding Network Object Groups, page 16-3
- Understanding Service Object Groups, page 16-6
- Creating ACLs with Object Groups, page 16-10
- ACL Object Groups Reference, page 16-11

Understanding ACL Object Groups

ACLs provide basic security to the network by permitting or blocking certain types of traffic. ACLs use IP addresses, protocols, and ports to filter network traffic. In some networks, the number of ACLs can become quite large and difficult to manage. The ACL Object Groups feature simplifies this problem. By using the ACL Object Groups feature, the administrator can group users, devices, or protocols into object groups and create access control entries (ACEs). Each ACE can then permit or deny a group of users access to a group of servers or services.

The ACL Object Groups feature is supported on routers running Cisco IOS Release 12.4(20)T and later.

Benefits of Using ACL Object Groups

- Increases performance when network traffic is heavy.
- Reduces storage in NVRAM compared to conventional ACLs.
- Separates ownership of the components of an ACE. For example, you can create an ACE where each department within an organization can control its group membership. You can also create an ACE to permit or deny the departments to contact each other.
- Allows you to create an object group that contains other object groups. For example, you can create an ENG-ALL address group, which contains the ENG-EAST and ENG-WEST address groups.

ACL Object Groups Basic Workflow

1. Create ACL object groups.

   You can create two types of ACL object groups: network object groups and service object groups.

   - Network Object Groups—Can contain hostnames, host IP addresses, subnet masks, range of IP addresses, and other existing network object groups.
   - Service Object Groups—Can contain top-level protocols, such as TCP, UDP, and TCP-UDP; ICMP types; source and destination protocol ports; and other existing service object groups.

2. Create a rule (ACE), which can permit or deny traffic on specified ACL object groups.

   After you create the ACL object groups, use the Extended Rule Entry dialog box to create rules to permit or deny traffic on the specified ACL object groups. See Add an Extended Rule Entry, page 15-13, for details.

Understanding Network Object Groups

The ACL Object Groups feature allows you to create network object groups. Network object groups can contain hostnames, host IP addresses, subnet masks, range of IP addresses, and other existing network object groups.

Each group can contain multiple network types (group members). For example, you can create Group A, which contains multiple hostnames or IP addresses, multiple networks, multiple ranges of IP addresses, and multiple existing network object groups.

You cannot create circular object groups. For example, if you create two object groups, Group A and Group B, you cannot do the following:

- Associate Group A with Group A.
- Associate Group A with Group B and then try to associate Group B with Group A.

There is no limit to the number of group members that you can add to a group.

You can use the Network Object Group summary page to add, edit, or delete network object groups. See Working with Network Object Groups, page 16-3.

Working with Network Object Groups

This section contains the following topics:

- Creating Network Object Groups, page 16-3
- Editing Network Object Groups, page 16-4
- Deleting Network Object Groups, page 16-5

Creating Network Object Groups

Before You Begin

From the Select Community Member drop-down list, choose the router on which you want to create the network object group.

Note Make sure that the router is discovered and that it supports ACL object groups.

Procedure

Use this procedure to create a network object group.

Step 1 Choose **Configure > Router > ACL > Object Groups > Network Object Groups** to open the Network Object Groups summary page. See Network Object Groups Summary Page, page 16-12.

Step 2 Click **Create** to open the Create Network Object Group dialog box.

Step 3 Enter the group name and description, specify the parameters in the Network Object Group Members area, and then click the **Add >** button. The parameters that you entered on the left pane are added to the right pane.

For information about the parameters, see Create Network Object Group Dialog Box, page 16-13.

Step 4 Click **OK** to send the configured group information to the router.

Related Topics

- Understanding ACL Object Groups, page 16-1
- Understanding Network Object Groups, page 16-3
- Working with Network Object Groups, page 16-3

Editing Network Object Groups

Before You Begin

From the Select Community Member drop-down list, choose the router on which you want to change the network object group parameters.

Note Make sure that the router is discovered and that it supports ACL object groups.

Procedure

Use this procedure to change the parameters of a selected network object group.

Note The Group Name cannot be changed.

Step 1 Choose **Configure > Router > ACL > Object Groups > Network Object Groups** to open the Network Object Groups summary page. See Network Object Groups Summary Page, page 16-12.

Step 2 Select the group row to edit, and then click **Edit** to open the Edit Network Object Group dialog box.

Step 3 Change the parameters that you want to modify in the Network Object Group Members area, and then click the **Add >** button. The parameters that you entered on the left pane are added to the right pane.

For information about the parameters, see Edit Network Object Groups Dialog Box, page 16-15.

Step 4 Click **OK** to send the modified group configuration to the router.

Related Topics

- Understanding ACL Object Groups, page 16-1
- Understanding Network Object Groups, page 16-3
- Working with Network Object Groups, page 16-3

Deleting Network Object Groups

Before You Begin

From the Select Community Member drop-down list, choose the router from which you want to delete a network object group.

Note Make sure that the router is discovered and that it supports ACL object groups.

Procedure

Use this procedure to delete a selected network object group.

Note You cannot delete a network object group that is being used by an ACL. Also, you cannot delete a network object group that is being used by another network object group. If you try to delete it, a warning message is displayed.

Step 1 Choose **Configure > Router > ACL > Object Groups > Network Object Groups** to open the Network Object Groups summary page. See Network Object Groups Summary Page, page 16-12.

Step 2 Select the group row that you want to delete, and then click **Delete**. A Confirmation dialog box appears.

Step 3 Click **Yes** to delete the object group.

Related Topics

- Understanding ACL Object Groups, page 16-1
- Understanding Network Object Groups, page 16-3
- Working with Network Object Groups, page 16-3

Understanding Service Object Groups

The ACL Object Groups feature allows you to create service object groups. Service object groups can contain top level protocols, such as TCP, UDP, and TCP-UDP; ICMP types; source and destination protocol ports; and other existing service object groups.

Each group can contain multiple group members (service types). For example, you can create Group A, which contains multiple TCP, UDP, and TCP-UDP protocols, multiple ICMP types, multiple source and destination protocol ports, and multiple existing service object groups.

You cannot create circular object groups. For example, if you create two object groups, Group A and Group B, you cannot do the following:

- Associate Group A with Group A.
- Associate Group A with Group B and then try to associate Group B with Group A.

There is no limit to the number of group members you can add to a group.

You can use the Service Object Groups summary page to add, edit, or delete service object groups. See Working with Service Object Groups, page 16-7.

Working with Service Object Groups

This section contains the following topics:

- Creating Service Object Groups, page 16-7
- Editing Service Object Groups, page 16-8
- Deleting Service Object Groups, page 16-9

Creating Service Object Groups

Before You Begin

From the Select Community Member drop-down list, choose the router on which you want to create the service object group.

Note Make sure that the router is discovered and that it supports ACL object groups.

Procedure

Use this procedure to create a service object group.

Step 1 Choose **Configure > Router > ACL > Object Groups > Service Object Groups** to open the Service Object Group summary page. See Service Object Groups Summary Page, page 16-17.

Step 2 Click **Create** to open the Create Service Object Group dialog box.

Step 3 Enter the group name and description, specify the parameters in the Service Object Group Members area, and then click the **Add >** button. The parameters that you entered on the left pane are added to the right pane.

For information about the parameters, see Create Network Object Group Dialog Box, page 16-13.

Step 4 Click **OK** to send the configured group information to the router.

Related Topics

- Understanding ACL Object Groups, page 16-1
- Understanding Service Object Groups, page 16-6
- Working with Service Object Groups, page 16-7

Editing Service Object Groups

Before You Begin

From the Select Community Member drop-down list, choose the router on which you want to change the service object group parameters.

Note Make sure that the router is discovered and that it supports ACL object groups.

Procedure

Use this procedure to change the parameters of a selected service object group.

Note The Group Name cannot be changed.

Step 1 Choose **Configure > Router > ACL> Object Groups > Service Object Groups** to open the Service Object Group summary page. See Service Object Groups Summary Page, page 16-17.

Step 2 Select the group row to edit, and then click **Edit** to open the Edit Service Object Group dialog box.

Step 3 Change the parameters that you want to modify in the Service Object Group Members area, and then click the **Add >** button. The parameters that you entered on the left pane are added to the right pane.

For information about the parameters, see Edit Service Object Groups Dialog Box, page 16-34.

Step 4 Click **OK** to send the modified group configuration to the router.

Related Topics

- Understanding ACL Object Groups, page 16-1
- Understanding Service Object Groups, page 16-6
- Working with Service Object Groups, page 16-7

Deleting Service Object Groups

Before You Begin

From the Select Community Member drop-down list, choose the router from which you want to delete a service object group.

Note Make sure that the router is discovered and that it supports ACL object groups.

Procedure

Use this procedure to delete a selected service object group.

Note You cannot delete a service object group that is being used by an ACL. Also, you cannot delete a service object group that is being used by another service object group. If you try to delete it, a warning message is displayed.

Step 1 Choose **Configure > Router > ACL > Object Groups > Service Object Groups** to open the Service Object Groups summary page. See Service Object Groups Summary Page, page 16-17.

Step 2 Select the group row that you want to delete, and then click **Delete**. A Confirmation dialog box appears.

Step 3 Click **Yes** to delete the object group.

Related Topics

- Understanding ACL Object Groups, page 16-1
- Understanding Service Object Groups, page 16-6
- Working with Service Object Groups, page 16-7

Creating ACLs with Object Groups

After you create network object groups and/or service object groups, you can create an ACL that can permit or deny traffic to these object groups.

Before You Begin

From the Select Community Member drop-down list, choose the router on which you want to create an ACL with the object groups.

Make sure that the router is discovered and that it supports ACL object groups.

Make sure that you have created ACL object groups.

Procedure

Use this procedure to create an ACL that can permit or deny traffic to the configured object groups.

Step 1 Choose **Configure > Router > ACL > ACL Editor** to open the Additional Task Rules dialog box. For information about access rules, see Chapter 15, "ACL."

Step 2 Click **Add** to open the Add a Rule dialog box.

Step 3 Add a name and description for the rule in the appropriate fields, and then click **Add** to open the Add an Extended Rule Entry dialog box.

Step 4 From the Action field, choose the action you want to configure. The options are: Permit or Deny.

Step 5 From the Source Host/Network pane, do the following:

a. Choose **Network Object Group** from the Type field.

b. Click the **...** (more) button—located beside the Network Object Group field—to open the Select Network Object Groups dialog box. See Select Network Object Groups Dialog Box, page 16-37.

c. From the Select Network Object Groups dialog box, select the network object group, and then click **OK**.

Step 6 From the Destination Host/Network pane, do the following:

a. Choose **Network Object Group** from the Type field.

b. Click the **...** (more) button—located beside the Network Object Group field—to open the Select Network Object Groups dialog box. See Select Network Object Groups Dialog Box, page 16-37.

c. From the Select Network Object Groups dialog box, select the network object group, and then click **OK**.

Step 7 From the Protocol and Service pane, do the following:

a. Click the **Service Object Group(s)** radio button.

b. Click the **...** (more) button—located beside the Service Object Group field—to open the Select Service Object Groups dialog box. See Select Service Object Groups Dialog Box, page 16-38.

c. From the Select Service Object Groups dialog box, select the service object group, and then click **OK**.

Step 8 Click **OK** in the Add an Extended Rule Entry dialog box.

Related Topics

- Understanding ACL Object Groups, page 16-1
- Add an Extended Rule Entry, page 15-13

ACL Object Groups Reference

This section describes the dialog boxes you can use when working with the ACL Object Groups feature and includes the following topics:

- Network Object Groups Summary Page, page 16-12
- Create and Edit Network Object Groups Dialog Box, page 16-13
- Edit Network Object Groups Dialog Box, page 16-15
- Service Object Groups Summary Page, page 16-17
- Create and Edit Service Object Groups Dialog Box, page 16-18
- Edit Service Object Groups Dialog Box, page 16-34
- Add an Extended Rule Entry Dialog Box, page 16-37
- Select Network Object Groups Dialog Box, page 16-37
- Select Service Object Groups Dialog Box, page 16-38

Network Object Groups Summary Page

Use the Network Object Groups summary page to view the network object groups that are configured on the router, to create new network object groups, to modify parameters on a selected network group, and to delete a selected network object group.

How to Get to This Dialog Box

Choose **Configure > Router > ACL > Object Groups > Network Object Groups**.

Related Topics

- Understanding ACL Object Groups, page 16-1
- Understanding Network Object Groups, page 16-3
- Working with Network Object Groups, page 16-3

Field Reference

Table 16-1 Network Object Groups Summary Page

Element	Description
Filter	Allows you to filter the display according to what you want to view.

Table 16-1 Network Object Groups Summary Page (continued)

Element	Description
Name	The names of the network object groups that are configured and that exist on the router.
Group Members	Consists of any or all of the following: IP address or hostnames, IP address and mask, range of IP address that are included in the group, and the names of existing network groups.
Description	(Optional) Words or phrases that describe the network object groups.
Create button	Click this button to open the Create Network Object Group dialog box, in which you can create a new network object group. See Create and Edit Network Object Groups Dialog Box, page 16-13.
Edit button	Click this button to modify the parameters that are configured on a selected network object group. When you click this button, the Edit Network Object Group dialog box appears, in which you can edit the parameters that are configured on the selected network object group. See Edit Network Object Groups Dialog Box, page 16-15.
Delete button	Click this button to delete a selected group member row.

Create and Edit Network Object Groups Dialog Box

See the following topics as appropriate:

- Create Network Object Group Dialog Box, page 16-13
- Edit Network Object Groups Dialog Box, page 16-15

Create Network Object Group Dialog Box

Use the Create Network Object Group dialog box to create network object groups.

How to Get to This Dialog Box

1. Choose **Configure > Router > ACL > Object Groups > Network Object Groups** to open the Network Object Groups summary page.
2. From the Network Object Groups summary page, click **Create**.

Related Topics

- Understanding ACL Object Groups, page 16-1
- Understanding Network Object Groups, page 16-3
- Creating Network Object Groups, page 16-3
- Creating ACLs with Object Groups, page 16-10

Field Reference

Table 16-2 Create Network Object Group Dialog Box

Element	Description
Group Name	The name of the object group.
Description	(Optional) The word or phrase that describes the object group.
Network Object Group Members	
Type of Member	Choose the type of member from the drop-down list. The options are: IP Address/Hostname, Network, Range of IP Addresses, and Existing Network Object Group.
Context-Sensitive Area—Left Pane	
Context-sensitive area	Based on the type of member you choose from the Type of Member drop-down list, this context-sensitive area changes: • If you choose IP Address/Hostname from the drop-down list, the context-sensitive area displays the IP Address/Hostname pane, in which you can enter the IP address or hostname. **Note** If you enter the hostname, make sure that the router is configured for DNS resolution. • If you choose Network from the drop-down list, the context-sensitive area displays the Network pane, in which you can enter the IP address and subnet mask. • If you choose Range of IP Addresses from the drop-down list, the context-sensitive area displays the Range of IP Addresses pane, in which you can enter the range of IP addresses in the From and To fields. • If you choose Existing Network Object Group from the drop-down list, the context-sensitive area displays a list of existing group members and their description. Choose the group that you want from the list.

Table 16-2 Create Network Object Group Dialog Box (continued)

Element	Description
Add > button	Click this button to add the parameters that you entered in the left pane (context-sensitive area) to the right pane (Group Members pane).
Group Members—Right pane	
Group Members	List of group members that you entered in the left pane (context-sensitive area).
Remove button	Click this button to delete a selected group member.
Remove All button	Click this button to delete the entire list of group members. **Note** A group must have at least one group member. When you click the Remove All button, make sure that you add at least one group member to the group, otherwise you will get an error message.
OK button	Click this button to send the configured network object group information to the router.
Cancel button	Click this button to remove the configuration values that you entered.

Edit Network Object Groups Dialog Box

Use the Edit Network Object Groups dialog box to change the network object group parameters of a selected group.

How to Get to This Dialog Box

1. Choose **Configure > Router > ACL > Object Groups > Network Object Groups** to open the Network Object Groups summary page.
2. From the Network Object Groups summary page, click **Edit**.

Related Topics

- Understanding ACL Object Groups, page 16-1
- Understanding Network Object Groups, page 16-3
- Editing Network Object Groups, page 16-4
- Creating ACLs with Object Groups, page 16-10

Field Reference

Table 16-3 Edit Network Object Groups Dialog Box

Element	Description
Group Name	The name of the network object group. **Note** The Group Name cannot be changed.
Description	(Optional) The word or phrase that describes the network object group, which you can edit.
Network Object Group Members	
Type of Member	Choose the type of member from the drop-down list. The options are: IP Address/Hostname, Network, Range of IP Addresses, and Existing Network Object Group.
Context-Sensitive Area—Left Pane	
Context-sensitive area	Based on the type of member you choose from the Type of Member drop-down list, this context-sensitive area changes: • If you choose IP Address/Hostname from the drop-down list, the context-sensitive area displays the IP Address/Hostname pane. This pane contains the IP Address/Hostname field, which you can edit. • If you choose Network from the drop-down list, the context-sensitive area displays the Network pane. This pane contains the IP Address and Mask fields, which you can edit. • If you choose Range of IP Addresses from the drop-down list, the context-sensitive area displays the Range of IP Addresses pane. This pane contains the From and To fields, which you can edit. • If you choose Existing Network Object Group from the drop-down list, the context-sensitive area displays a list of existing group members and their descriptions. Select the group that you want.
Add > button	Click this button to add the parameters that you entered in the left pane (context-sensitive area) to the right pane (Group Members pane).
Group Members—Right pane	
Group Members	List of group members that you entered in the left pane (context-sensitive area).
Remove button	Click this button to delete a selected group member.

Table 16-3 Edit Network Object Groups Dialog Box (continued)

Element	Description
Remove All button	Click this button to delete the entire list of group members. **Note** A group must have at least one group member. When you click the Remove All button, make sure that you add at least one group member to the group, otherwise you will get an error message.
OK button	Click this button to send the modified network object group information to the router.
Cancel button	Click this button to remove the configuration values that you edited and to return to the original values.

Service Object Groups Summary Page

Use the Service Object Groups summary page to create service object groups. Service object groups can contain TCP, UDP, TCP-UDP, ICMP, IP protocols, and other existing service object groups.

How to Get to This Dialog Box

Choose **Configure > Router > ACL > Object Groups > Service Object Groups**.

Related Topics

- Understanding ACL Object Groups, page 16-1
- Understanding Service Object Groups, page 16-6
- Working with Service Object Groups, page 16-7
- Creating ACLs with Object Groups, page 16-10

Field Reference

Table 16-4 Service Object Groups Summary Page

Element	Description
Filter	Allows you to filter the display according to what you want to view.
Name	The names of the service object groups that are configured and that exist in the system.

Table 16-4 Service Object Groups Summary Page (continued)

Element	Description
Group Members	Consists of any or all of the following group member services that are configured on a service object group: TCP Service, UDP Service, TCP-UDP Service, ICMP Service, IP Protocol Service, and Existing Service Object Groups.
Description	(Optional) The word or phrase that describes each of the service object groups.
Create button	Click this button to open the Create Service Object Group dialog box, in which you can create a new service object group. See Create Service Object Groups Dialog Box, page 16-18.
Edit button	Click this button to modify parameters that are configured on a selected service object group. When you click this button, the Edit Service Object Group dialog box appears, in which you can edit the parameters for the selected service object group. See Edit Service Object Groups Dialog Box, page 16-34.
Delete button	Click this button to delete a selected group member row.

Create and Edit Service Object Groups Dialog Box

See the following topics as appropriate:

- Create Service Object Groups Dialog Box, page 16-18
- Edit Service Object Groups Dialog Box, page 16-34

Create Service Object Groups Dialog Box

Use the Create Service Object Groups dialog box to create service object groups.

How to Get to This Dialog Box

1. Choose **Configure > Router > ACL > Object Groups > Service Object Groups** to open the Service Object Groups summary page.
2. From the Service Object Groups summary page, click **Create**.

Related Topics

- Understanding ACL Object Groups, page 16-1
- Understanding Service Object Groups, page 16-6
- Working with Service Object Groups, page 16-7
- Creating ACLs with Object Groups, page 16-10

Field Reference

Table 16-5 Create Service Object Groups Dialog Box

Element	Description
Group Name	The name of the service object group.
Description	(Optional) The word or phrase that describes the service object group.
Service Object Group Members Area	
Type of Member	Choose a service from the drop-down list. The options are: TCP Service, UDP Service, TCP-UDP Service, ICMP Service, IP Protocol Service, and Existing Service Object Groups.
Context-Sensitive Area—Left Pane	

Table 16-5 Create Service Object Groups Dialog Box (continued)

Element	Description
Context-sensitive area	Based on the type of service you choose from the Type of Member drop-down list, this context-sensitive area changes: • If you choose TCP Service from the drop-down list, the context-sensitive area displays the Service Port pane. For details, see Create Service Object Groups Dialog Box—TCP Service. • If you choose UDP Service from the drop-down list, the context-sensitive area displays the Service Port pane. For details, see Create Service Object Groups Dialog Box—UDP Service. • If you choose TCP-UDP Service from the drop-down list, the context-sensitive area displays the Service Port pane. For details, see Create Service Object Groups Dialog Box—TCP-UDP Service. • If you choose ICMP Service from the drop-down list, the context-sensitive area displays the ICMP Service pane. For details, see Create Service Object Groups Dialog Box—ICMP Service. • If you choose IP Protocol Service from the drop-down list, the context-sensitive area displays the IP Protocol Service pane. For details, see Create Service Object Groups Dialog Box—IP Protocol Service. • If you choose Existing Network Object Group from the drop-down list, the context-sensitive area displays a list of existing group members and their description. For details, see Create Service Object Groups Dialog Box—Existing Service Object Groups.
Add > button	Click this button to add the parameters that you entered in the left pane (context-sensitive area) to the right pane (Group Members pane).
Group Members—Right pane	
Group Members	List of group members that you entered in the left pane (context-sensitive area).
Remove button	Click this button to delete a selected service group member.
Remove All button	Click this button to delete the entire list of service group members. **Note** A group must have at least one group member. When you click the Remove All button, make sure that you add at least one group member to the group, otherwise you will get an error message.

Table 16-5 Create Service Object Groups Dialog Box (continued)

Element	Description
OK button	Click this button to send the configured service object group information to the router.
Cancel button	Click this button to remove the configuration values that you entered.

Create Service Object Groups Dialog Box—TCP Service

Use the Create Service Object Groups dialog box to create TCP service object groups.

How to Get to This Dialog Box

1. Choose **Configure > Router > ACL > Object Groups > Service Object Groups** to open the Service Object Groups summary page.
2. From the Service Object Groups summary page, click **Create**.

Related Topics

- Create and Edit Service Object Groups Dialog Box, page 16-18
- Understanding ACL Object Groups, page 16-1
- Understanding Service Object Groups, page 16-6
- Working with Service Object Groups, page 16-7
- Creating ACLs with Object Groups, page 16-10

Field Reference

Table 16-6 Create Service Object Groups Dialog Box—TCP Service

Element	Description
Group Name	The name of the service object group.
Description	(Optional) The word or phrase that describes the service object group.
Service Object Group Members Area	
Type of Member	Choose the TCP Service option from the drop-down list.
Service Port—Left Pane	

Table 16-6 Create Service Object Groups Dialog Box—TCP Service (continued)

Element	Description
Context-sensitive area	When you choose the TCP Service option, the context-sensitive area displays the Service Port pane, which contains the Source Port and the Destination Port areas: • Source Port—Contains the **Select Source Port** check box and a drop-down list. Click the check box, then choose an option from the drop-down list. The options are: Greater Than, Less Than, Equals, and Range. – Greater Than—If you choose the Greater Than option, you can either enter the source port number in the numeric field or select the port number by clicking the Up arrow or Down arrow. Valid port numbers are 1 to 65535. – Less Than—If you choose the Less Than option, you can either enter the source port number in the numeric field or select the port number by clicking the Up arrow or Down arrow. Valid port numbers are 1 to 65535. – Equals—If you choose the Equals option, do the following: Select a service from the drop-down list. The options including bgp, chargen, cmd, daytime, and discard are displayed. Enter the source port number in the numeric field or select the port number by clicking the Up arrow or Down arrow. Valid port numbers are 1 to 65535. – Range—If you choose the Range option, you can either enter the source port number range in the numeric field or select the port number range by clicking the Up arrow or Down arrow. Valid port ranges include numbers from 1 to 65535.

Table 16-6 Create Service Object Groups Dialog Box—TCP Service (continued)

Element	Description
Context-sensitive area (continued)	• Destination Port—Contains the **Select Destination Port** check box and a drop-down list. Click the check box, then choose an option from the drop-down list. The options are: Greater Than, Less Than, Equals, and Range. – Greater Than—If you choose the Greater Than option, you can either enter the destination port number in the numeric field or select the port number by clicking the Up arrow or Down arrow. Valid port numbers are 1 to 65535. – Less Than—If you choose the Less Than option, you can either enter the destination port number in the numeric field or select the port number by clicking the Up arrow or Down arrow. Valid port numbers are 1 to 65535. – Equals—If you choose the Equals option, do the following: Select a service from the drop-down list. The options including bgp, chargen, cmd, daytime, and discard are displayed. Enter the destination port number in the numeric field or select the port number by clicking the Up arrow or Down arrow. Valid port numbers are 1 to 65535. – Range—If you choose the Range option, you can either enter the destination port number range in the numeric field or select the port number range by clicking the Up arrow or Down arrow. Valid port ranges include numbers from 1 to 65535.
Add > button	Click this button to add the parameters that you entered in the Service Port pane to the Group Members pane.
Group Members—Right Pane	
Group Members	List of group members that you entered in the Service Port pane.
Remove button	Click this button to delete a selected service group member.
Remove All button	Click this button to delete the entire list of service group members. **Note** A group must have at least one group member. When you click the Remove All button, make sure that you add at least one group member to the group, otherwise you will get an error message.

Table 16-6 Create Service Object Groups Dialog Box—TCP Service (continued)

Element	Description
OK button	Click this button to send the configured service object group information to the router.
Cancel button	Click this button to remove the configuration values that you entered.

Create Service Object Groups Dialog Box—UDP Service

Use the Create Service Object Groups dialog box to create UDP service object groups.

How to Get to This Dialog Box

1. Choose **Configure > Router > ACL > Object Groups > Service Object Groups** to open the Service Object Groups summary page.
2. From the Service Object Groups summary page, click **Create**.

Related Topics

- Create and Edit Service Object Groups Dialog Box, page 16-18
- Understanding ACL Object Groups, page 16-1
- Understanding Service Object Groups, page 16-6
- Working with Service Object Groups, page 16-7
- Creating ACLs with Object Groups, page 16-10

Field Reference

Table 16-7 Create Service Object Groups Dialog Box—UDP Service

Element	Description
Group Name	The name of the service object group.
Description	(Optional) The word or phrase that describes the service object group.
Service Object Group Members Area	
Type of Member	Choose the UDP Service option from the drop-down list.
Service Port—Left Pane	
Context-sensitive area	When you choose the UDP Service option, the context-sensitive area displays the Service Port pane, which contains the Source Port and the Destination Port areas: • Source Port—Contains the **Select Source Port** check box and a drop-down list. Click the check box, then choose an option from the drop-down list. The options are: Greater Than, Less Than, Equals, and Range. – Greater Than—If you choose the Greater Than option, you can either enter the source port number in the numeric field or select the port number by clicking the Up arrow or Down arrow. Valid port numbers are 1 to 65535. – Less Than—If you choose the Less Than option, you can either enter the source port number in the numeric field or select the port number by clicking the Up arrow or Down arrow. Valid port numbers are 1 to 65535. – Equals—If you choose the Equals option, do the following: Select a service from the drop-down list. The options including biff, bootpc, bootps, discard, and dnsix are displayed. Enter the source port number in the numeric field or select the port number by clicking the Up arrow or Down arrow. Valid port numbers are 1 to 65535. – Range—If you choose the Range option, you can either enter the source port number range in the numeric field or select the port number range by clicking the Up arrow or Down arrow. Valid port ranges include numbers from 1 to 65535.

Table 16-7 Create Service Object Groups Dialog Box—UDP Service (continued)

Element	Description
Context-sensitive area (continued)	• Destination Port—Contains the **Select Destination Port** check box and a drop-down list. Click the check box, then choose an option from the drop-down list. The options are: Greater Than, Less Than, Equals, and Range. – Greater Than—If you choose the Greater Than option, you can either enter the destination port number in the numeric field or select the port number by clicking the Up arrow or Down arrow. Valid port numbers are 1 to 65535. – Less Than—If you choose the Less Than option, you can either enter the destination port number in the numeric field or select the port number by clicking the Up arrow or Down arrow. Valid port numbers are 1 to 65535. – Equals—If you choose the Equals option, do the following: Select a service from the drop-down list. The options including biff, bootpc, bootps, discard, and dnsix are displayed. Enter the destination port number in the numeric field or select the port number by clicking the Up arrow or Down arrow. Valid port numbers are 1 to 65535. – Range—If you choose the Range option, you can either enter the destination port number range in the numeric field or select the port number range by clicking the Up arrow or Down arrow. Valid port ranges include numbers from 1 to 65535.
Add > button	Click this button to add the parameters that you entered in the Service Port pane to the Group Members pane.
Group Members—Right Pane	
Group Members	List of group members that you entered in the Service Port pane.
Remove button	Click this button to delete a selected service group member.
Remove All button	Click this button to delete the entire list of service group members. **Note** A group must have at least one group member. When you click the Remove All button, make sure that you add at least one group member to the group, otherwise you will get an error message.

Table 16-7 Create Service Object Groups Dialog Box—UDP Service (continued)

Element	Description
OK button	Click this button to send the configured service object group information to the router.
Cancel button	Click this button to remove the configuration values that you entered.

Create Service Object Groups Dialog Box—TCP-UDP Service

Use the Create Service Object Groups dialog box to create TCP-UDP service object groups.

How to Get to This Dialog Box

1. Choose **Configure > Router > ACL > Object Groups > Service Object Groups** to open the Service Object Groups summary page.
2. From the Service Object Groups summary page, click **Create**.

Related Topics

- Create and Edit Service Object Groups Dialog Box, page 16-18
- Understanding ACL Object Groups, page 16-1
- Understanding Service Object Groups, page 16-6
- Working with Service Object Groups, page 16-7
- Creating ACLs with Object Groups, page 16-10

Field Reference

Table 16-8 Create Service Object Groups Dialog Box—TCP-UDP Service

Element	Description
Group Name	The name of the service object group.
Description	(Optional) The word or phrase that describes the service object group.
Service Object Group Members Area	
Type of Member	Choose the TCP-UDP Service option from the drop-down list.
Service Port—Left Pane	

Table 16-8 Create Service Object Groups Dialog Box—TCP-UDP Service (continued)

Element	Description
Context-sensitive area	When you choose the TCP-UDP Service option, the context-sensitive area displays the Service Port pane, which contains the Source Port and the Destination Port areas: • Source Port—Contains the **Select Source Port** check box and a drop-down list. Click the check box, and then choose an option from the drop-down list. The options are: Greater Than, Less Than, Equals, and Range. – Greater Than—If you choose the Greater Than option, you can either enter the source port number in the numeric field or select the port number by clicking the Up arrow or Down arrow. Valid port numbers are 1 to 65535. – Less Than—If you choose the Less Than option, you can either enter the source port number in the numeric field or select the port number by clicking the Up arrow or Down arrow. Valid port numbers are 1 to 65535. – Equals—If you choose the Equals option, do the following: Select a service from the drop-down list. The options including discard domain, echo, sunrpc, and syslog are displayed. Enter the source port number in the numeric field or select the port number by clicking the Up arrow or Down arrow. Valid port numbers are 1 to 65535. – Range—If you choose the Range option, you can either enter the source port number range in the numeric field or select the port number range by clicking the Up arrow or Down arrow. Valid port ranges include numbers from 1 to 65535.

Table 16-8 Create Service Object Groups Dialog Box—TCP-UDP Service (continued)

Element	Description
Context-sensitive area (continued)	• Destination Port—Contains the **Select Destination Port** check box and a drop-down list. Click the check box, and then choose an option from the drop-down list. The options are: Greater Than, Less Than, Equals, and Range. – Greater Than—If you choose the Greater Than option, you can either enter the destination port number in the numeric field or select the port number by clicking the Up arrow or Down arrow. Valid port numbers are 1 to 65535. – Less Than—If you choose the Less Than option, you can either enter the destination port number in the numeric field or select the port number by clicking the Up arrow or Down arrow. Valid port numbers are 1 to 65535. – Equals—If you choose the Equals option, do the following: Select a service from the drop-down list. The options including discard domain, echo, sunrpc, and syslog are displayed. Enter the destination port number in the numeric field or select the port number by clicking the Up arrow or Down arrow. Valid port numbers are 1 to 65535. – Range—If you choose the Range option, you can either enter the destination port number range in the numeric field or select the port number range by clicking the Up arrow or Down arrow. Valid port ranges include numbers from 1 to 65535.
Add > button	Click this button to add the parameters that you entered in the Service Port pane to the Group Members pane.
Group Members—Right Pane	
Group Members	List of group members that you entered in the Service Port pane.
Remove button	Click this button to delete a selected service group member.
Remove All button	Click this button to delete the entire list of service group members. **Note** A group must have at least one group member. When you click the Remove All button, make sure that you add at least one group member to the group, otherwise you will get an error message.

Table 16-8 Create Service Object Groups Dialog Box—TCP-UDP Service (continued)

Element	Description
OK button	Click this button to send the configured service object group information to the router.
Cancel button	Click this button to remove the configuration values that you entered.

Create Service Object Groups Dialog Box—ICMP Service

Use the Create Service Object Groups dialog box to create ICMP service object groups.

How to Get to This Dialog Box

1. Choose **Configure > Router > ACL > Object Groups > Service Object Groups** to open the Service Object Groups summary page.
2. From the Service Object Groups summary page, click **Create**.

Related Topics

- Create and Edit Service Object Groups Dialog Box, page 16-18
- Understanding ACL Object Groups, page 16-1
- Understanding Service Object Groups, page 16-6
- Working with Service Object Groups, page 16-7
- Creating ACLs with Object Groups, page 16-10

Field Reference

Table 16-9 Create Service Object Groups Dialog Box—ICMP Service

Element	Description
Group Name	The name of the service object group.
Description	(Optional) The word or phrase that describes the service object group.
Service Object Group Members Area	
Type of Member	Choose the ICMP Service option from the drop-down list.
ICMP Service—Right Pane	

Table 16-9 Create Service Object Groups Dialog Box—ICMP Service (continued)

Element	Description
Context-sensitive area	When you choose the ICMP Service option from the drop-down list, the context-sensitive area displays the ICMP Service pane. Do one of the following: • Enter a value in the ICMP Type field or select the value by clicking the up or down arrow. The valid ICMP range is 0 to 255. • Select an ICMP message type from the drop-down list. The options including alternate-address, conversion-error, echo, echo-reply, and information reply are listed.
Add > button	Click this button to add the parameters that you entered in the ICMP Service pane to the Group Members pane.
Group Members—Right Pane	
Group Members	List of group members that you entered in the ICMP Service pane.
Remove button	Click this button to delete a selected service group member.
Remove All button	Click this button to delete the entire list of service group members. **Note** A group must have at least one group member. When you click the Remove All button, make sure that you add at least one group member to the group, otherwise you will get an error message.
OK button	Click this button to send the configured service object group information to the router.
Cancel button	Click this button to remove the configuration values that you entered.

Create Service Object Groups Dialog Box—IP Protocol Service

Use the Create Service Object Groups dialog box to create IP protocol service object groups.

How to Get to This Dialog Box

1. Choose **Configure > Router > ACL > Object Groups > Service Object Groups** to open the Service Object Groups summary page.
2. From the Service Object Groups summary page, click **Create**.

Related Topics

- Create and Edit Service Object Groups Dialog Box, page 16-18
- Understanding ACL Object Groups, page 16-1
- Understanding Service Object Groups, page 16-6
- Working with Service Object Groups, page 16-7
- Creating ACLs with Object Groups, page 16-10

Field Reference

Table 16-10 Create Service Object Groups Dialog Box—IP Protocol Service

Element	Description
Group Name	The name of the service object group.
Description	(Optional) The word or phrase that describes the service object group.
Service Object Group Members Area	
Type of Member	Choose the IP Protocol Service option from the drop-down list.
IP Protocol Service—Left Pane	
Context-sensitive area	If you choose the IP Protocol Service option, the context-sensitive area displays the IP Protocol Service pane. Do one of the following: • Enter a value in the IP Protocol field, or select the value by clicking the Up arrow or Down Arrow. The valid IP protocol range is 0 to 255. • Select the IP Protocol from the drop-down list. The options including ahp, eigrp, esp, gre, and igmp are listed.
Add > button	Click this button to add the parameters that you entered in the IP Protocol Service pane to the Group Members pane.
Group Members—Right Pane	
Group Members	List of group members that you entered in the IP Protocol Service pane.
Remove button	Click this button to delete a selected service group member.
Remove All button	Click this button to delete the entire list of service group members. **Note** A group must have at least one group member. When you click the Remove All button, make sure that you add at least one group member to the group, otherwise you will get an error message.

Table 16-10 Create Service Object Groups Dialog Box—IP Protocol Service (continued)

Element	Description
OK button	Click this button to send the configured service object group information to the router.
Cancel button	Click this button to remove the configuration values that you entered.

Create Service Object Groups Dialog Box—Existing Service Object Groups

Use the Create Service Object Groups dialog box to create service object groups.

How to Get to This Dialog Box

1. Choose **Configure > Router > ACL > Object Groups > Service Object Groups** to open the Service Object Groups summary page.
2. From the Service Object Groups summary page, click **Create**.

Related Topics

- Create and Edit Service Object Groups Dialog Box, page 16-18
- Understanding ACL Object Groups, page 16-1
- Understanding Service Object Groups, page 16-6
- Working with Service Object Groups, page 16-7
- Creating ACLs with Object Groups, page 16-10

Field Reference

Table 16-11 Create Service Object Groups Dialog Box—Existing Service Object Groups

Element	Description
Group Name	The name of the service object group.
Description	(Optional) The word or phrase that describes the service object group.
Service Object Group Members Area	
Type of Member	Choose the Existing Service Object Groups option from the drop-down list.
Group Name and Description—Left Pane	
Filter	Allows you to filter the display according to what you want to view.

Table 16-11 Create Service Object Groups Dialog Box—Existing Service Object Groups

Element	Description
Context-sensitive area	When you choose the Existing Service Object Groups option, the context-sensitive area displays a list of existing group members and their description. Select the group member you want to add in the service object group, and then click the **ADD >** button.
Add > button	Click this button to add the group member that you selected in the left pane to the right pane (Group Members pane).
Group Members—Right Pane	
Group Members	List of group members that you entered in the left pane.
Remove button	Click this button to delete a selected service group member.
Remove All button	Click this button to delete the entire list of service group members. **Note** A group must have at least one group member. When you click the Remove All button, make sure that you add at least one group member to the group, otherwise you will get an error message.
OK button	Click this button to send the configured service object group information to the router.
Cancel button	Click this button to remove the configuration values that you entered.

Edit Service Object Groups Dialog Box

Use the Edit Service Object Groups dialog box to change the service object group parameters of a selected group.

How to Get to This Dialog Box

1. Choose **Configure > Router > ACL > Object Groups > Service Object Groups** to open the Service Object Groups summary page.
2. From the Service Object Groups summary page, click **Edit**.

Related Topics

- Understanding ACL Object Groups, page 16-1
- Understanding Service Object Groups, page 16-6

- Editing Service Object Groups, page 16-8
- Creating ACLs with Object Groups, page 16-10

Field Reference

Table 16-12 Edit Service Object Groups Dialog Box

Element	Description
Group Name	The name of the service object group. **Note** The Group Name cannot be changed.
Description	(Optional) The word or phrase that describes the service object group, which you can edit.
Service Object Group Members Area	
Type of Member	Choose a service from the drop-down list. The options are: TCP Service, UDP Service, TCP-UDP Service, ICMP Service, IP Protocol Service, and Existing Service Object Groups.
Context-Sensitive Area—Left Pane	

Table 16-12 Edit Service Object Groups Dialog Box (continued)

Element	Description
Context-sensitive area	Based on the type of service you choose from the Type of Member drop-down list, the context-sensitive area in which you configure the group parameters, changes: • If you choose TCP Service from the drop-down list, the context-sensitive area displays the Service Port pane, which you can edit. For details, see Create Service Object Groups Dialog Box—TCP Service. • If you choose UDP Service from the drop-down list, the context-sensitive area displays the Service Port pane, which you can edit. For details, see Create Service Object Groups Dialog Box—UDP Service. • If you choose TCP-UDP Service from the drop-down list, the context-sensitive area displays the Service Port pane, which you can edit. For details, see Create Service Object Groups Dialog Box—TCP-UDP Service. • If you choose ICMP Service from the drop-down list, the context-sensitive area displays the ICMP Service pane, which you can edit. For details, see Create Service Object Groups Dialog Box—ICMP Service. • If you choose IP Protocol Service from the drop-down list, the context-sensitive area displays the IP Protocol Service pane, which you can edit. For details, see Create Service Object Groups Dialog Box—IP Protocol Service. • If you choose Existing Service Object Group from the drop-down list, the context-sensitive area displays the existing groups and their description, which you can edit. For details, see Create Service Object Groups Dialog Box—Existing Service Object Groups.
Add > button	Click this button to add the parameters that you edited in the left pane to the right pane.
Group Members Pane—Right pane	
Group Members	List of group members that you edited in the left pane.
Remove button	Click this button to delete a selected service group member.

Table 16-12 Edit Service Object Groups Dialog Box (continued)

Element	Description
Remove All button	Click this button to delete the entire list of service group members. **Note** A group must have at least one group member. When you click the Remove All button, make sure that you add at least one group member to the group, otherwise you will get an error message.
OK button	Click this button to send the edited configuration values to the router.
Cancel button	Click this button to remove the configuration values that you edited and to return to the original values.

Add an Extended Rule Entry Dialog Box

Use the Add an Extended Rule Entry dialog box to create an ACL that can permit or deny traffic to configured object groups.

For details, see Add an Extended Rule Entry, page 15-13.

Related Topics

- Creating ACLs with Object Groups, page 16-10
- Select Network Object Groups Dialog Box, page 16-37
- Select Service Object Groups Dialog Box, page 16-38

Select Network Object Groups Dialog Box

Use the Select Network Object Groups dialog box to display the list of existing network object groups, from which you can select the group to add to the ACL.

How to Get to This Dialog Box

From the Add an Extended Rule Entry dialog box, click the **...** (more) button—located beside the Network Object Group field—to open the Select Network Object Groups dialog box.

Related Topics

- Creating ACLs with Object Groups, page 16-10
- Add an Extended Rule Entry, page 15-13
- Select Network Object Groups Dialog Box, page 16-37

Field Reference

Table 16-13 Select Network Object Groups Dialog Box

Element	Description
Available Groups Pane—Upper Pane	
Name	List of network object groups that are configured and that exist in the system.
Details Pane—Lower Pane	
Click a group name in the Available Groups pane to display its details in the Details pane.	
Name	The name of the network object group.
Group Members	Lists the group members of the selected network object group.
Description	(Optional) The word or phrase that describes the network object group.
OK button	Click this button to add the selected group name to the Add an Extended Entry dialog box.
Cancel button	Click this button to cancel the object group you selected.
Help button	Click this button to open the context-sensitive help for this dialog box.

Select Service Object Groups Dialog Box

Use the Select Service Object Groups dialog box to display the list of existing service object groups, from which you can select the group to add to the ACL.

How to Get to This Dialog Box

From the Add an Extended Rule Entry dialog box, click the **...** (more) button—located beside the Service Object Group field—to open the Select Service Object Groups dialog box.

Related Topics

- Creating ACLs with Object Groups, page 16-10
- Add an Extended Rule Entry, page 15-13

Field Reference

Table 16-14 Select Service Object Groups Dialog Box

Element	Description
Available Groups —Upper Pane	
Name	List of service object groups that are configured and that exist in the system.
Details Pane—Lower Pane	
Click a group name in the Available Groups pane to display its details in the Details pane.	
Name	The name of the service object group.
Group Members	Lists the group members of the selected service object group.
Description	(Optional) The word or phrase that describes the service object group.
OK button	Click this button to add the selected group name to the Add an Extended Entry dialog box.
Cancel button	Click this button to cancel the object group you selected.
Help button	Click this button to open the context-sensitive help for this dialog box.

CHAPTER 17

Router Properties

Router properties let you define the overall attributes of the router, such as the router name, domain name, password, Simple Network Management Protocol (SNMP) status, Domain Name System (DNS) server address, user accounts, router log attributes, virtual type terminal (vty) settings, SSH settings, and other router access security settings.

Device Properties

The Properties—Device screen contains host, domain, and password information for your router.

How to Get to this Screen

Click **Configure** > **Router** > **Router Options**.

Field Reference

Table 17-1 Device Properties

Element	Description
Device Tab	
Host	Enter the name you want to give the router in this field.
Domain	Enter the domain name for your organization. If you do not know the domain name, obtain it from your network administrator.

Table 17-1 Device Properties

Element	Description
Enter the Text for Banner	Enter text for the router banner. The router text banner is displayed whenever anyone logs in to the router. We recommend that the text banner include a message indicating that unauthorized access is prohibited.
Password Tab	
Enable Secret Password	Cisco Configuration Professional (Cisco CP) supports the enable secret password. The enable secret password allows you to control who is able to enter configuration commands on this router. We strongly recommend that you set an enable secret password. The password will not be readable in the Cisco CP Device Properties window, and it will appear in encrypted form in the router configuration file. Therefore, you should record this password in case you forget it. The Cisco IOS release that the router is running may also support the enable password. The enable password functions like the enable secret password, but was encrypted in the configuration file. If an enable password is configured using the command-line interface (CLI), it is ignored if an enable secret password is configured.
Current Password	If a password has already been set, this area contains asterisks (*).
Enter New Password	Enter the new enable password in this field.
Reenter New Password	Reenter the password exactly as you entered it in the New Password field.

Date and Time: Clock Properties

Use this window to view and edit the date and time settings on the router.

How to Get to this Screen

Click **Configure** > **Router** > **Time** > **Date** and **Time**.

Related Links

- Date and Time Properties

Field Reference

Table 17-2 Clock Properties

Element	Description
Date/Time	You can see the router date and time settings on the right side of the Cisco CP status bar. The time and date settings in this part of the Clock Properties window are not updated.
Router Time Source	This field can contain the following values: • NTP – The router receives time information from an NTP server. • User Configuration – The time and date values are set manually, using Cisco CP or the CLI. • No time source – The router is not configured with time or date settings.
Change Settings	Click to change the date and time settings on the router.

Date and Time Properties

Use this window to set the router date and time. You can have Cisco CP synchronize the settings with the PC, or you can set them manually.

How to Get to this Screen

Click **Configure** > **Router** > **Time** > **Date** and **Time** > **Change Settings**.

Related Links

- Date and Time: Clock Properties

Field Reference

Table 17-3 Date and Time Properties

Element	Description
Synchronize with my local PC clock	Check to set up Cisco CP to synchronize router date and time settings with the date and time settings on the PC.
Synchronize	Click to have Cisco CP synchronize time settings. Cisco CP adjusts date and time settings in this way only when you click Synchronize. Cisco CP does not automatically resynchronize them with the PC during subsequent sessions. This button is disabled if you have not checked Synchronize with my local PC clock. **Note** You must make the Time Zone and Daylight Savings settings on the PC before starting Cisco CP so that Cisco CP will receive the correct settings when you click **Synchronize**.
Edit Date and Time	Use this area to set the date and time manually. You can choose the month and the year from the drop-down lists, and choose the day of the month in the calendar. The fields in the Time area require values in 24-hour format. You can choose your time zone based on Greenwich mean time (GMT), or you can browse the list for major cities in your time zone. If you want the router to adjust time settings for daylight saving time and standard time, check **Automatically adjust clock for daylight savings changes**.
Apply	Click to apply the date and time settings you have made in the Date, Time, and Time Zone fields.

Voice Timezone Configuration

In this screen, synchronize the Call Manager Express (Cisco Unified CME) and Cisco Unity Express (CUE) timezones with the router timezone. To prevent inadvertant desynchronization with the router time zone, CME or CUE time zones are not configured separately using Cisco CP.

Note After you synchronize the CUE timezone with the router timezone, you must reload CUE for the timezone synchronization to take effect. See the procedure in Reloading Cisco Unity Express for instructions.

How to Get to this Screen

This screen is displayed automatically when you have changed the router timezone, and you have confirmed that you want to synchronize the CME and CUE time zones with the router time zone.

Field Reference

Table 17-4 Voice Timezone Configuration

Element	Description
CME Timezone	In this list, choose the CME timezone that matches the configured router timezone.
CUE Timezone	In this list, choose the CUE timezone that matches the configured router timezone.
Reset the IP phones	To cause the synchronized CME time zone to take effect, you must check **Reset the IP phones**.

Reloading Cisco Unity Express

This section of the help topic provides a procedure for reloading CUE.

Note Reloading CUE takes more than 3 minutes, and during reload, all CUE related features are disabled on the device being configured. You may prefer to complete all configuration tasks for this device before reloading CUE. After the reload completes, the device must be rediscovered for the CUE features to be enabled.

To reload CUE, complete the following steps:

Step 1 In the Application menu, click **Reload Cisco Unity Express**.

Step 2 When the confirmation popup appears, choose the device from the device list, and click **Yes** to reload CUE on that device.

Step 3 To be able to cross-launch CUE on the device after CUE reloads so that you can perform CUE configuration or monitoring tasks, return to the Community Information window and rediscover the device.

NTP

Network Time Protocol (NTP) allows routers on your network to synchronize their time settings with an NTP server. A group of NTP clients that obtains time and date information from a single source will have more consistent time settings. This window allows you to view the NTP server information that has been configured, add new information, or edit or delete existing information.

Note If your router does not support NTP commands, this branch will not appear in the Router Properties tree.

How to Get to This Screen

Click **Configure** > **Router** > **Time** > **NTP** and **SNTP**.

Related Links

- Add an NTP Server
- Add or Edit NTP Server Details

Field Reference

Table 17-5 Network Time Protocol

Element	Description
IP Address	The IP address of an NTP server. If your organization does not have an NTP server, you may want to use a publicly available server, such as the servers described at the following URL: http://www.pool.ntp.org
Interface	The interface over which the router will communicate with the NTP server.
Prefer	This column contains Yes if this NTP server has been designated as a preferred NTP server. Preferred NTP servers will be contacted before non preferred servers. There can be more than one preferred NTP server.
Add	Click to add NTP server information.
Edit	Click to edit a specified NTP server configuration.
Delete	Click to delete a specified NTP server configuration.

Add or Edit NTP Server Details

Add or edit NTP server information in this window.

How to Get to this Screen

Click **Configure** > **Router** > **Time** > **NTP** and **SNTP** > **Add** or **Edit**.

Field Reference

Table 17-6 Add or Edit NTP Server Details

Element	Description
IP Address	Enter or edit the IP address of an NTP server.
Prefer	Click this box if this is to be the preferred NTP server.

Table 17-6 Add or Edit NTP Server Details (continued)

Element	Description
Interface	Choose the router interface that will provide access to the NTP server. You can use the **show IP routes** CLI command to determine which interface has a route to this NTP server. **Note** An extended access rule will be created for port 123 traffic and applied to the interface that you choose in this window. If an access rule is already in place for this interface, Cisco CP will add statements to permit port 123 traffic on this interface. If the existing rule is a standard access rule, Cisco CP changes it to an extended rule in order to be able to specify traffic type and destination.
Authentication Key	Check this box if the NTP server uses an authentication key, and enter the information required in the fields. The information in these fields must match the key information on the NTP server.
Key Number	Enter the number for the authentication key. The key number range is 0 to 4294967295.
Key Value	Enter the key used by the NTP server. The key value can use any of the letters A to Z, uppercase or lowercase, and can be no more than 32 characters.
Confirm Key Value	Reenter the key value to confirm accuracy.

Add an NTP Server

Enter the IP address of an NTP server in this window.

Note An extended access rule will be created for port 123 traffic and applied to the interface that you choose in this window. If an access rule was already in place for this interface, Cisco CP will add statements to permit port 123 traffic on this interface. If the existing rule was a standard access rule, Cisco CP changes it to an extended rule in order to be able to specify traffic type and destination.

How to Get to this Screen

Click **Configure > Router > Time.**

Field Reference

Table 17-7 NTP Server

Element	Description
IP Address	Enter the IP address of the NTP server in dotted-decimal format. For more information, see IP Addresses and Subnet Masks.

Logging

Use this window to enable logging of system messages, and to specify logging hosts where logs can be kept. You can specify the level of logging messages that you want to send and to collect, and enter the hostname or IP address of multiple logging hosts.

How to Get to this Screen

Click **Configure > Router > Logging**.

Field Reference

Table 17-8 Logging

Element	Description
IP Address/Hostname	Click **Add**, and enter the IP address or hostname of a network host to which you want the router to send logging messages for storage. The Edit and Delete buttons enable you to modify information that you entered and to delete entries. Specify the types of messages that are sent to logging hosts by choosing the logging level from the Logging Level drop-down list. See Logging Level for more information.

Table 17-8 Logging (continued)

Element	Description
Logging Level	The following logging levels are available in **Logging Level** drop-down lists: • emergencies (0) • alerts (1) • critical (2) • errors (3) • warnings (4) • notifications (5) • informational (6) • debugging (7) The log collects all messages of the level you choose plus all messages of lower levels, or the router sends all messages of the level you choose plus all messages of lower levels to the logging hosts. For example, if you choose notifications (5), the log collects or sends messages of levels 0 through 5. Firewall logging messages require a logging level of debugging(7), and Application Security logging messages require a level of informational(6).
Logging to Buffer	If you want system messages to be logged to the router buffer, check the **Logging Buffer** check box in the dialog that Cisco CP displays when you click **Edit**, then enter the buffer size in the Buffer Size field. The larger the buffer, the more entries can be stored before the oldest ones are deleted to make room for new entries. However, you should balance logging needs against router performance. Specify the types of messages that are collected in the log by choosing the logging level from the Logging Level drop-down list. See Logging Level in this help topic for more information.

SNMP

This window lets you enable SNMP, set SNMP community strings, and enter SNMP trap manager information.

How to Get to this Screen

Click **Configure** > **Router** > **SNMP**.

Field Reference

Table 17-9 SNMP

Element	Description
Enable SNMP	Check this check box to enable SNMP support. Uncheck to disable SNMP support. SNMP is enabled by default.
Community String	SNMP community strings are embedded passwords to Management Information Bases (MIBs). MIBs store data about router operation and are meant to be available to authenticated remote users. The two types of community strings are "public" community strings, which provide read-only access to all objects in the MIB except community strings, and "private" community strings, which provide read-and-write access to all objects in the MIB except community strings. The community string table lists all of the configured community strings and their types. Use the **Add** button to display the Add a Community String dialog box and create new community strings. Click the **Edit** or **Delete** buttons to edit or delete the community string you chose in the table.
Trap Receiver	Enter the IP addresses and community strings of the trap receivers—that is, the addresses where the trap information should be sent. These are normally the IP addresses of the SNMP management stations monitoring your domain. Check with your site administrator to determine the address if you are unsure of it. Click the **Add**, **Edit**, or **Delete** buttons to administer trap receiver information.
SNMP Server Location	Text field you can use to enter the SNMP server location. It is not a configuration parameter that will affect the operation of the router.
SNMP Server Contact	Text field you can use to enter contact information for a person managing the SNMP server. It is not a configuration parameter that will affect the operation of the router.

Netflow

This window shows how your router is configured to monitor Netflow top talkers on interfaces that have Netflow configured. For more information on the items shown, see Netflow Talkers.

How to Get to this Screen

Click **Configure** > **Router** > **Netflow**.

You can monitor Netflow parameters on your router and view top-talker statistics in **Monitor > Interface Status** and **Monitor > Traffic Status > Top N Traffic Flows**. If you do *not* enable Netflow top talkers, then the top ten talkers are monitored.

Netflow Talkers

In this window you can configure Netflow top talkers.

How to Get to this Screen

Click **Configure** > **Router** > **Netflow** > **Edit**.

Field Reference

Table 17-10 Netflow Talkers

Element	Description
Enable Top Talkers	Check the **Enable Top Talkers** check box to enable monitoring of the top talkers on the interfaces that have Netflow configured.
Top Talkers	Set the number of top talkers in the **Top Talkers** number box. Choose a number in the range 1–200. Cisco CP will track and record data on up to the number of top talkers that you set.
Cache Timeout	Set the timeout, in milliseconds, for the top-talkers cache in the **Cache timeout** number box. Choose a number in the range 1–3600000. The top-talkers cache will refresh when the timeout is reached.
Sort By	Choose how to sort the top talkers by choosing bytes or packets from the **Sort by** drop-down list.

Router Access

This window explains which features are included in router access.

User Accounts/View

This window allows you to define accounts and passwords that will enable users to authenticate themselves when logging in to the router using HTTP, Telnet, PPP, or some other means.

How to Get to this Screen

Click **Configure > Router > Router Access > User Accounts/View**.

Field Reference

Table 17-11 Router Access User Accounts

Element	Description
Username	User account name.
Password	User account password, displayed as asterisks (*). **Note** The user password is not the same as the enable secret password configured in the Device Properties—Password tab. The user password enables the specified user to log in to the router and enter a limited set of commands.

Table 17-11 Router Access User Accounts (continued)

Element	Description
Privilege Level	Privilege level for the user.
View Name	If a CLI view has been associated with the user account, the view name appears in this column. Views define the user's access to Cisco CP based on the user's role. Click Associate a View with the User for more information. **Note** If Cisco CP is launched with a user-defined view, or with an altered Cisco CP-defined view, Cisco CP operates in Monitor mode, and the user has read-only privileges. The Cisco CP features available to be monitored depend on the commands present in the view. Not all features may be available for monitoring by the user.

Add or Edit a Username

Add or edit a user account in the fields provided in this window.

How to Get to this Screen

Click **Configure > Router > Router Access > User Accounts/View > Add** or **Edit**.

Related Links

- User Accounts/View
- See "Things To Know About Discovering Devices" in Community Online Help.

Field Reference

Table 17-12 Username Fields

Element	Description
Username	Enter or edit the username in this field.
Password	Enter or edit the password in this field.

Table 17-12 Username Fields (continued)

Element	Description
Confirm Password	Reenter the password in this field. If the password and the confirm password do not match, an error message window appears when you click **OK**. When you click **OK**, the new or edited account information appears in the Configure User Accounts for Telnet window.
Encrypt password using MD5 hash algorithm Check Box	Check if you want the password to be encrypted using the one-way Message Digest 5 (MD5) algorithm, which provides strong encryption protection. **Note** Protocols that require the retrieval of clear text passwords, such as CHAP, cannot be used with MD5-encrypted passwords. MD5 encryption is not reversible. To restore the password to clear text, you must delete the user account and re-create it without checking the **Encrypt password** option.
Privilege Level	Enter the privilege level for the user. When applied to a CLI command, that command can only be executed by users with a privilege level equal to or higher than the level set for the command.
Associate a View with the User	This field is displayed when you are setting up user accounts for router access. It may not be visible if you are working in a different area of Cisco CP. Check the **Associate a View with the user** option if you want to restrict user access to a specific view. If you associate a view with any user for the first time, you are prompted to enter the view password.

Table 17-12 Username Fields (continued)

Element	Description
View Name	Choose the view you want to associate with this user from the following: • CCP_Administrator—A user associated with the view type CCP_Administrator has complete access to Cisco CP and can perform all operations supported by Cisco CP. • CCP_Monitor—A user associated with the view type CCP_Monitor can monitor all features supported by Cisco CP. The user is not able to deliver configurations using Cisco CP. The user is able to navigate the various areas of Cisco CP, such as Interfaces and Connections, Firewall, and VPN. However, the user interface components in these areas are disabled. • CCP_Firewall—A user associated with the view type CCP_Firewall can use the Cisco CP Firewall and Monitor features. The user can configure firewalls and ACLs using the Firewall wizard, Firewall Policy View, and ACL Editor. User interface components in other areas are disabled for this user. • CCP_EasyVPN_Remote—A user associated with the view type CCP_EasyVPN_Remote can use the Cisco CP Easy VPN Remote features. The user is able to create Easy VPN Remote connections and edit them. User interface components in other areas are disabled for this user. **Caution** If Cisco Router and Security Device Manager was used to configure views on the router, view names beginning with "SDM_," such as "SDM_Monitor" will appear in the list. However, do not assign a view beginning with "SDM_" to the user. If a user with an "SDM_" view attempts to discover a device, discovery will fail. If you are editing a user account with an "SDM_" view assigned to the account, change that view to a "CCP_" view, such as "CCP_Monitor."

Table 17-12 Username Fields (continued)

Element	Description
View Details	The "Associate a View with the user" area displays details of the specified view. Click **View Details** to see which commands are allowed for the specified view.

View Password

When you associate a view with any user for the first time, you are prompted to enter the view password for Cisco CP-defined views. Use this password to switch between other views.

Field Reference

Table 17-13 View Password

Element	Description
Enter the View Password	Enter the view password in the View Password field.

VTY Settings

This window displays the virtual terminal (vty) settings on your router. The Property column contains configured line ranges and configurable properties for each range. The settings for these properties are contained in the Value column.

This table shows your router vty settings and contains the columns described in VTY Settings.

How to Get to this Screen

Click **Configure > Router > Router Access > VTY**.

Table Reference

Table 17-14 VTY Settings

Element	Description
Line Range	Displays the range of vty connections to which the rest of the settings in the row apply.
Input Protocols Allowed	Shows the protocols configured for input. Can be Telnet, SSH, or both Telnet and SSH. **Note** To use SSH as an input or output protocol, you must enable it by clicking **SSH** in the Router Access tree and generating an RSA key.
Output Protocols Allowed	Shows the protocols configured for output. Can be Telnet, SSH, or both Telnet and SSH.
EXEC Timeout	Number of seconds of inactivity after which a session is terminated.
Inbound Access-class	Name or number of the access rule applied to the inbound direction of the line range.
Outbound Access-class	Name or number of the access rule applied to the outbound direction of the line range.
ACL	If configured, shows the ACL associated with the vty connections.
Authentication Policy	The AAA authentication policy associated with this vty line. This field is visible if AAA is configured on the router.
Authorization Policy	The AAA authorization policy associated with this vty line. This field is visible if AAA is configured on the router.

Edit VTY Lines

This window lets you edit virtual terminal (vty) settings on your router.

How to Get to this Screen

Click **Configure** > **Router** > **Router Access** > **VTY** > **Edit**.

Field Reference

Table 17-15 vty Line Dialog

Element	Description
Line Range	Enter the range of vty lines to which the settings made in this window will apply.
Time Out	Enter the number of minutes of inactivity allowed to pass before an inactive connection is terminated.
Input Protocol	Choose the input protocols by clicking the appropriate check boxes.
Telnet	Check to enableTelnet access to your router.
SSH	Check to enable SSH clients to log in to the router.
Output Protocol	Choose the output protocols by clicking the appropriate check boxes.
Telnet	Check to enable Telnet as an output protocol for your router.
SSH	Check to enable SSH as an output protocol for your router.
Access Rule	You can associate access rules to filter inbound and outbound traffic on the vty lines in the range.
Inbound	Enter the name or number of the access rule you want to filter inbound traffic, or click the button and browse for the access rule.
Outbound	Enter the name or number of the access rule you want to filter outbound traffic, or click the button and browse for the access rule.
Authentication/Authorization	These fields are visible when AAA is enabled on the router. AAA can be enabled by clicking **Configure > Router > AAA > AAA Summary > Enable AAA**.
Authentication Policy	Choose the authentication policy that you want to use for this vty line.
Authorization Policy	Choose the authorization policy that you want to use for this vty line.

Configure Management Access Policies

Use this window to review existing management access policies and to choose policies for editing. Management access policies specify which networks and hosts will be able to access the router command-line interface. In the policy, you can specify which protocols the host or network in the policy can use, and which router interface will carry the management traffic.

How to Get to this Screen

Click **Configure > Router > Router Access > Management Access**.

Field Reference

Table 17-16 Management Access Policies

Element	Description
Host/Network	A network address or host IP address. If a network address is given, the policy applies to all hosts on that network. If a host address is given, the policy applies to that host. A network address is shown in the format network number/network bits, as in the following example: `172.23.44.0/24` For more information on this format, and on how IP addresses and subnet masks are used, see IP Addresses and Subnet Masks.
Management Interface	The router interface over which management traffic will flow.

Table 17-16 Management Access Policies (continued)

Element	Description
Permitted Protocols	This column lists the protocols that the specified hosts can use when communicating with the router. The following protocols can be configured: • Cisco CP—Specified hosts can use Cisco CP. • Telnet—Specified hosts can use Telnet to access the router CLI. • SSH—Specified hosts can use Secure Shell to access the router CLI. • HTTP—Specified hosts can use Hypertext Transfer Protocol to access the router. If Cisco CP is specified, either HTTP or HTTPS must also be specified. • HTTPS—Specified hosts can use Hypertext Transfer Protocol Secure to access the router. • RCP—Specified hosts can use Remote Copy Protocol to manage files on the router. • SNMP—Specified hosts can use Simple Network Management Protocol to manage the router.
Add	Click to add a management policy, and specify the policy in the Add a Management Policy window.
Edit	Click to edit a management policy, and specify the policy in the Edit a Management Policy window.
Delete	Click to delete a specified management policy.
Apply	Click to apply changes you made in the Add or Edit a Management Policy window to the router configuration.
Discard Changes	Click to discard changes you made in the Add or Edit a Management Policy window to the router configuration. The changes you made are discarded and removed from the Configure Management Access Policies window.

Add or Edit a Management Policy

Use this window to add or edit a management policy.

How to Get to this Screen

Click **Configure** > **Router** > **Router Access** > **Management Access** > **Add** or **Edit**.

Field Reference

Table 17-17 Management Policy Dialog

Element	Description
Type	Specify whether the address you provide is the address of a host or a network.
IP Address/Subnet Mask	If you specified **Network** in the Type field, enter the IP address of a host, or the network address and subnet mask. For more information, see IP Addresses and Subnet Masks.
Interface	Choose the interface through which you want to allow management traffic. The interface should be the most direct route from the host or network to the local router.
Management Protocols	Specify the management protocols allowed for the host or network.
Allow Cisco CP	Check to allow the specified host or network to access Cisco CP. When you check this box, the following protocols are automatically checked: Telnet, SSH, HTTP, HTTPS, and RCP. Checking this option does not prevent you from allowing additional protocols. If you want to make users employ secure protocols when logging in to Cisco CP, check **Allow secure protocols only**. When you check this box, the following protocols are automatically checked: SSH, HTTPS, RCP. If you then check a nonsecure protocol such as Telnet, Cisco CP unchecks **Allow secure protocols only**.

Table 17-17 Management Policy Dialog (continued)

Element	Description
Allow secure protocols only	If you want to make users employ secure protocols when logging in to Cisco CP, check **Allow secure protocols only**. When you check this box, the following protocols are automatically checked: SSH, HTTPS, RCP. If you then check a nonsecure protocol such as Telnet, Cisco CP unchecks **Allow secure protocols only**. **Note** The options **Allow secure protocols only** and **HTTPS** are disabled if the Cisco IOS release on the router does not support HTTPS
Telnet, SSH, HTTP, RCP, and SNMP	If you want to specify individual protocols that the host or network can use, you can check the boxes next to the protocols that you want. If Telnet and SSH are not enabled (checked) in the VTYs window, and SNMP is not enabled in the SNMP Properties window, Cisco CP will advise you to enable those protocols when they are specified in this window.

Management Access Error Messages

The following error messages may be generated by the Management Access feature.

Error Message

```
SDM Warning: ANY Not Allowed
```

Explanation A management policy is read-only if any of its source or destination rule entries contain the “any” keyword. Such policies cannot be edited in the Management Access window. A policy containing the “any” keyword can create a security risk for the following reasons:

- If “any” is associated with source, it allows traffic from any network to enter the router.

– If “any” is associated with destination, it allows access to any node on the network supported by the router.

Recommended Action You can remove the access entry that caused this message to appear by choosing the rule in the Rules window and clicking **Edit**. Alternatively, in the Interfaces and Connections window, you can disassociate the rule from the interface it is applied to.

Error Message

```
SDM Warning: Unsupported Access Control Entry
```

Explanation A management policy will be read only if unsupported access control entries (ACEs) are associated with the interface or vty line to which you applied the management policy. You can use the CLI to remove the unsupported ACEs. Unsupported ACEs are those that contain keywords or syntax that Cisco CP does not support.

Error Message

```
SDM Warning: SDM Not Allowed
```

Explanation This message is displayed if you still have not configured a management access policy to allow a host or network to access Cisco CP on this router.

Recommended Action You must provide such a policy in order to make Cisco CP on this router accessible. You cannot navigate to other features or deliver commands to the router until you configure a management access policy to allow access to Cisco CP for a host or network.

Error Message

```
SDM Warning: Current Host Not Allowed
```

Explanation This message is displayed if you have not configured a management access policy to allow the current host or network to access Cisco CP on this router.

Recommended Action You should create such a policy in order to make Cisco CP on this router accessible from the current host or network. If you do not, you will lose the connection to the router when you deliver the configuration to the router. Click **Yes** to add to a management access policy now for the current host or network. Click **No** to proceed without adding a policy for the current host or network. You will lose contact with the router during command delivery, and you will have to log in to Cisco CP using a different host or network.

SSH

This router implements Secure Shell (SSH) Server, a feature that enables an SSH client to make a secure, encrypted connection to a Cisco router. This connection provides functionality similar to that of an inbound Telnet connection, but which provides strong encryption to be used with Cisco IOS software authentication. The SSH server in Cisco IOS software will work with publicly and commercially available SSH clients. This feature is disabled if the router is not using an IPsec DES or 3DES Cisco IOS release, and if the SSH branch of the Router Access tree does not appear.

SSH uses an RSA cryptographic key to encrypt data traveling between the router and the SSH client. Generating the RSA key in this window enables SSH communication between the router and the SSH clients.

How to Get to this Screen

Click **Configure > Router > Router Access > SSH**.

Field Reference

Table 17-18 SSH Screen

Element	Description
Status Messages	
Crypto key is not set on this device	Appears if there is no cryptographic key configured for the device. If there is no key configured, you can enter a modulus size and generate a key.
RSA key is set on this router	Appears if a cryptographic key was generated. SSH is enabled on this router.
Key modulus size Button	Visible if no cryptographic key has been generated. Click this button and enter the modulus size you want to give the key. If you want a modulus value between 512 and 1024, enter an integer value that is a multiple of 64. If you want a value higher than 1024, you can enter 1536 or 2048. If you enter a value greater than 512, key generation may take a minute or longer.
Generate RSA Key Button	Click to generate a cryptographic key for the router using the modulus size you entered. If the cryptographic key was generated, this button is disabled.

DHCP Configuration

This window explains how you can manage DHCP configurations on your router.

DHCP Pools

This window displays the DHCP pools configured on the router.

How to Get to this Screen

Click **Configure > Router > DHCP > DHCP Pools**.

Field Reference

Table 17-19 DHCP Pools List

Element	Description
Pool Name	The name of the DHCP pool.
Interface	The interface on which the DHCP pool is configured. Clients attached to this interface will receive IP addresses from this DHCP pool.
Details of DHCP Pool *name*	This area provides the following details about the pool identified in *name*: • DHCP Pool Range—Range of IP addresses that can be granted to clients. • Default Router IP Address—If the router has an IP address in the same subnet as the DHCP pool, it is shown here. • DNS Servers—IP addresses of the DNS servers that the router will provide to DHCP clients. • WINS Servers—IP addresses of the WINS servers that the router will provide to DHCP clients. • Domain Name—Domain name configured on the router. • Lease Time—Amount of time that the router will lease an IP address to a client.
Add	Choose this option to create a new DHCP pool. The user must specify the DHCP pool name, DHCP pool network, DHCP pool IP address range, and lease time. Optionally, DNS servers, WINS server, the domain name, and the default router can also be configured in the DHCP pool.
Edit	Choose this option to edit an existing DHCP pool.
Delete	Choose this option to delete a DHCP pool.

Add or Edit DHCP Pool

Add or edit a DHCP pool in this window. You cannot edit Cisco CP-default pools.

How to Get to this Screen

Click **Configure > Router > DHCP > DHCP Pools > Add** or **Edit**.

Field Reference

Table 17-20 DHCP Pool Dialog

Element	Description
DHCP Pool Name	Provide a name for the DHCP pool in this field.
DHCP Pool Network	Enter the network from which the IP addresses in the pool will be taken, for example, 192.168.233.0. This cannot be the IP address of an individual host.
Subnet Mask	Enter the subnet mask. The subnet mask of 255.255.255.0 provides 255 IP addresses.
DHCP Pool	Enter the starting and ending IP addresses in the range. For example, if the network is 192.168.233.0 and the subnet mask is 255.255.255.0, the starting address is 192.168.233.1 and the ending address is 192.168.233.254.
Lease Length	Enter the amount of time that addresses are to be leased to clients. You can specify that leased addresses never expire, or you can specify the lease time in days, hours, and minutes. Do not exceed 365 days, 23 hours, or 59 minutes.
DHCP Options	Enter information for the DNS servers, WINS servers, the domain name, and the default router in the DHCP options fields. These values are sent to DHCP clients when they request an IP address.
Import all DHCP Options into the DHCP Server Database	Click this option if you want to import DHCP option parameters into the DHCP server database and also send this information to DHCP clients on the LAN when they request IP addresses.

DHCP Bindings

This window shows existing manual DHCP bindings. A manual DHCP binding allows you to allocate the same IP address to a specific client each time the client requests an IP address from the available DHCP pools.

You can also add new bindings, edit existing bindings, or delete existing bindings.

How to Get to this Screen

Click **Configure > Router > DHCP > DHCP Bindings**.

Field Reference

Table 17-21 DHCP Bindings List

Element	Description
Binding Name	Name assigned to the DHCP binding.
Host/IP Mask	IP address and mask bound to the client.
MAC Address	MAC address of the client.
MAC Address Type	Type of MAC address is one of the following: • Ethernet—Client has a hardware address. • IEEE802—Client has a hardware address. • <None>—Client has a client identifier.
Client Name	Optional name assigned to the client.
Add	Click to add a new manual DHCP binding.
Edit	Click to edit the specified manual DHCP binding.
Delete	Click to delete the specified manual DHCP binding.

Add or Edit DHCP Binding

This window allows you to add or edit existing manual DHCP bindings.

How to Get to this Screen

Click **Configure > Router > DHCP > DHCP Bindings > Add** or **Edit.**

Field Reference

Table 17-22 DHCP Bindings Dialog

Element	Description
Name	Enter the name you want for the DHCP binding. If you are editing the DHCP binding, the name field is read-only.
Host IP address	Enter the IP address you want to bind to the client. The address should be from the DHCP pool available to the client. Do not enter an address in use by another DHCP binding.
Mask	Enter the mask used for the host IP address.
Identifier	From the drop-down menu, choose a method for identifying the client with a MAC address.
MAC Address	Enter the MAC address of the client. Do not enter an address in use by another DHCP binding.
Type	If you chose **Hardware Address** from the Identifier drop-down menu, choose **Ethernet** or **IEEE802** to set the MAC address type of the client.
Client Name (Optional)	Enter a name to identify the client. The name should be a hostname only, not a domain-style name. For example, *router* is an acceptable name, but *router.cisco.com* is not.

DNS Properties

The Domain Name System (DNS) is a database of Internet hostnames with their corresponding IP addresses distributed over designated DNS servers. It enables network users to refer to hosts by name, rather than by IP addresses, which are harder to remember. Use this window to enable the use of DNS servers for hostname-to-address translation.

How to Get to this Screen

Click **Configure** > **Router** > **DNS** > **DNS**.

Field Reference

Table 17-23 DNS Properties

Element	Description
Enable DNS-Based Hostname to Address Translation	Check to enable the router to use DNS. Uncheck if you do not want to use DNS.
DNS IP Address	Enter the IP addresses of the DNS servers that you want the router to send DNS requests to.Click the **Add**, **Edit**, or **Delete** buttons to administer DNS IP address information.

Dynamic DNS Methods

This window shows a list of dynamic DNS methods.

Each dynamic DNS method shown will send with its update the hostname and domain name configured in **Configure > Router > DNS > Dynamic DNS**. However, if you create a dynamic DNS method when configuring a WAN interface, you can override the hostname and domain name configured in **Configure > Router > DNS > Dynamic DNS**. The new hostname and domain name will apply only to that dynamic DNS method.

Some dynamic DNS methods are read-only. These were configured in the Cisco IOS software through the CLI, and cannot be edited or deleted. To make these read-only methods editable, use the CLI to change the internal cache or host group options to HTTP or IETF.

How to Get to this Screen

Click **Configure** > **Router** > **DNS** > **Dynamic DNS**.

Field Reference

Table 17-24 Dynamic DNS Method Screen Buttons

Element	Description
Add Button	Click the **Add** button to create a new dynamic DNS method.

Table 17-24 Dynamic DNS Method Screen Buttons (continued)

Element	Description
Edit Button	To edit a dynamic DNS method, choose it from the list of existing dynamic DNS methods and then click **Edit**.
Delete Button	To edit a dynamic DNS method, choose it from the list of existing dynamic DNS methods and then click **Delete**. **Note** A warning appears if you attempt to delete a dynamic DNS method that is associated with one or more interfaces.

Add or Edit Dynamic DNS Method

This window allows you to add or edit a dynamic DNS method. Set the type of method by choosing **HTTP** or **IETF**.

How to Get to this Screen

Click **Configure > Router > DNS > Dynamic DNS > Add** or **Edit**.

Field Reference

Table 17-25 Dynamic DNS Method

Element	Description
HTTP	HTTP is a dynamic DNS method type that updates a DNS service provider with changes to the associated interface's IP address.
Server	If using HTTP, choose the domain address of the DNS service provider from the drop-down menu.
Username	If using HTTP, enter a username for accessing the DNS service provider.

Table 17-25 Dynamic DNS Method (continued)

Element	Description
Password	If using HTTP, enter a password for accessing the DNS service provider.
IETF	IETF is a dynamic DNS method type that updates a DNS server with changes to the associated interface's IP address. If using IETF, configure a DNS server for the router in **Configure > Router > DNS > Dynamic DNS**.

CHAPTER 18

Network Address Translation

Network Address Translation (NAT) is a robust form of address translation that extends addressing capabilities by providing both static address translations and dynamic address translations. NAT allows a host that does not have a valid registered IP address to communicate with other hosts through the Internet. The hosts may be using private addresses or addresses assigned to another organization; in either case, NAT allows these addresses that are not Internet-ready to continue to be used but still allow communication with hosts across the Internet.

Network Address Translation Wizards

You can use a wizard to guide you in creating a Network Address Translation (NAT) rule. Choose one of the following wizards:

- Basic NAT

  Choose the Basic NAT wizard if you want to connect your network to the Internet (or the outside), and your network has hosts but no servers. Look at the sample diagram that appears to the right when you choose **Basic NAT**. If your network is made up only of PCs that require access to the Internet, choose **Basic NAT** and click the **Launch** button.

- Advanced NAT

  Choose the Advanced NAT wizard if you want to connect your network to the Internet (or the outside), and your network has hosts and servers, *and* the servers must be accessible to outside hosts (hosts on the Internet). Look at the sample diagram that appears to the right when you choose **Advanced NAT**.

If your network has e-mail servers, web servers, or other types of servers and you want them to accept connections from the Internet, choose **Advanced NAT** and click the **Launch** button.

Note If you do not want your servers to accept connections from the Internet, you can use the Basic NAT wizard.

Basic NAT Wizard: Welcome

The Basic NAT welcome window shows how the wizard will guide you through configuring NAT for connecting one or more LANs, but no servers, to the Internet.

Basic NAT Wizard: Connection

Choose an Interface

From the drop-down menu, choose the interface that connects to the Internet. This is the router WAN interface.

Choose Networks

The list of available networks shows the networks connected to your router. Choose which networks will share the WAN interface in the NAT configuration you set up. To choose a network, check its check box in the list of available networks.

Note Do not choose a network connected to the WAN interface set up in this NAT configuration. Remove that network from the NAT configuration by unchecking its check box.

The list shows the following information for each network:

- IP address range allocated to the network
- Network LAN interface
- Comments entered about the network

To remove a network from the NAT configuration, uncheck its check box.

Note If Cisco CP detects a conflict between the NAT configuration and an existing VPN configuration for the WAN interface, it will inform you with a dialog box after you click **Next**.

Summary

This window shows you the NAT configuration you created, and allows you to save the configuration. The summary will appear similar to the following:

```
Interface that is connected to the Internet or to your Internet
service provider:
    FastEthernet0/0

IP address ranges that share the Internet connection:
    108.1.1.0 to 108.1.1.255
    87.1.1.0 to 87.1.1.255
    12.1.1.0 to 12.1.1.255
    10.20.20.0 to 10.20.20.255
```

If you used the Advanced NAT wizard, you may also see additional information similar to the following:

```
NAT rules for servers:
    Translate 10.10.10.19 TCP port 6080 to IP address of interface
FastEthernet0/0 TCP port 80
    Translate 10.10.10.20 TCP port 25 to 194.23.8.1 TCP port 25
```

Advanced NAT Wizard: Welcome

The Advanced NAT welcome window shows how the wizard will guide you through configuring NAT for connecting your LANs and servers to the Internet.

Advanced NAT Wizard: Connection

Choose an Interface

From the drop-down menu, choose the interface that connects to the Internet. This is the router WAN interface.

Additional Public IP Addresses

Click **Add** to enter public IP addresses that you own. You will be able to assign these IP address to servers on your network that you want to make available to the Internet.

To delete an IP address from the list, choose the IP address and click **Delete**.

Add IP Address

Enter a public IP address that you own. You will be able to assign this IP address to a server on your network that you want to make available to the Internet.

Advanced NAT Wizard: Networks

Choose Networks

The list of available networks shows the networks connected to your router. Choose which networks will share the WAN interface in the NAT configuration you set up. To choose a network, check its check box in the list of available networks.

Note Do not choose a network connected to the WAN interface set up in this NAT configuration. Remove that network from the NAT configuration by unchecking its check box.

The list shows the following information for each network:

- IP address range allocated to the network
- Network LAN interface

- Comments entered about the network

To remove a network from the NAT configuration, uncheck its check box.

To add a network not directly connected to your router to the list, click **Add Networks**.

Note If Cisco CP does not allow you to place a check mark next to a network for which you want to configure a NAT rule, the interface associated with the network has already been designated as a NAT interface. This status will be indicated by the word *Designated* in the Comments column. If you want to configure a NAT rule for that interface, exit the wizard, click the **Edit NAT** tab, click **Designate NAT Interfaces**, and uncheck the interface. Then return to the wizard and configure the NAT rule.

Add Network

You can add a network to the list of networks made available in the Advanced NAT wizard. You must have the network IP address and network mask. For more information, see IP Addresses and Subnet Masks.

IP Address

Enter the network IP address.

Subnet Mask

Enter the network subnet mask in this field, or choose the number of subnet bits from the scrolling field on the right. The subnet mask tells the router which bits of the IP address designate the network address and which bits designate the host address.

Advanced NAT Wizard: Server Public IP Addresses

This window allows you to translate public IP addresses to the private IP addresses of internal servers that you want to make accessible from the Internet.

The list shows the private IP addresses and ports (if used) and the public IP addresses and ports (if used) to which they are translated.

To reorder the list based on the private IP addresses, click the column head **Private IP Address**. To reorder the list based on the public IP addresses, click the column head **Public IP Address**.

Add Button

To add a translation rule for a server, click **Add**.

Edit Button

To edit a translation rule for a server, choose it in the list and click **Edit**.

Delete Button

To delete a translation rule, choose it in the list and click **Delete**.

Add or Edit Address Translation Rule

In this window you can enter or edit the IP address translation information for a server.

Private IP Address

Enter the IP address that the server uses on your internal network. This is an IP address that cannot be used externally on the Internet.

Public IP Address

From the drop-down menu, choose the public IP address to which the server's private IP address will be translated. The IP addresses that appear in the drop-down menu include the IP address of the router WAN interface and any public IP addresses you own that were entered in the connections window (see Advanced NAT Wizard: Connection).

Type of Server

Choose one of the following server types from the drop-down menu:

- Web server

  An HTTP host serving HTML and other WWW-oriented pages.

- E-mail server

  An SMTP server for sending Internet mail.

- Other

  A server which is not a web or e-mail server, but which requires port translation to provide service. This choice activates the Translated Port field and the Protocol drop-down menu.

If you do not choose a server type, all traffic intended for the public IP address you choose for the server will be routed to that address, and no port translation will be done.

Original Port

Enter the port number used by the server to accept service requests from the internal network.

Translated Port

Enter the port number used by the server to accept service requests from the Internet.

Protocol

Choose **TCP** or **UDP** for the protocol used by the server with the original and translated ports.

Advanced NAT Wizard: ACL Conflict

If this window appears, Cisco CP has detected a conflict between the NAT configuration and an existing ACL on the WAN interface. This ACL may be part of a firewall configuration, a VPN configuration, or the configuration of another feature.

Choose to modify the NAT configuration to remove the conflict, or choose to *not* modify the NAT configuration. If you choose to *not* modify the NAT configuration, the conflict may cause other features you have configured to stop working.

View Details

Click the **View Details** button to see the proposed modifications to the NAT configuration to resolve the conflict. This button is not displayed with all feature conflicts.

Details

This window lists the changes Cisco CP will make to the NAT configuration to resolve conflicts between NAT and another feature configured on the same interface.

Network Address Translation Rules

The Network Address Translation Rules window lets you view NAT rules, view address pools, and set translation timeouts. From this window you can also designate interfaces as inside or outside interfaces.

For more information on NAT, follow the link More About NAT.

Designate NAT Interfaces

Click to designate interfaces as inside or outside. NAT uses the inside/outside designations as reference points when interpreting translation rules. Inside interfaces are those interfaces connected to the private networks that the router serves. Outside interfaces connect to the WAN or to the Internet. The designated inside and outside interfaces are listed above the NAT rule list.

Address Pools

Click this button to configure or edit address pools. Address pools are used with dynamic address translation. The router can dynamically assign addresses from the pool as they are needed. When an address is no longer needed, it is returned to the pool.

Translation Timeouts

When dynamic NAT is configured, translation entries have a timeout period after which they expire and are purged from the translation table. Click this button to configure the timeout values for NAT translation entries and other values.

Network Address Translation Rules

This area shows the designated inside and outside interfaces and the NAT rules that have been configured.

Inside Interfaces

The inside interfaces are the interfaces that connect to the private networks the router serves. NAT uses the inside designation when interpreting a NAT translation rule. You can designate interfaces as inside by clicking **Designate NAT interfaces**.

Outside Interfaces

The outside interfaces are the router interfaces that connect to the WAN or the Internet. NAT uses the outside designation when interpreting a NAT translation rule. You can designate interfaces as outside by clicking **Designate NAT interfaces**.

Original Address

This is the private address or set of addresses that is used on the LAN.

Translated Address

This is the legal address or range of addresses that is used on the Internet or the external network.

Rule Type

Rules are either static address translation rules or dynamic address translation rules.

Static address translation allows hosts with private addresses to access the Internet and to be publicly accessible from the Internet. It statically maps one private IP address to one public or global address. If you wanted to provide static translation to ten private addresses, you would create a separate static rule for each address.

Dynamic address translation. There are two methods of dynamic addressing using NAT. One method maps multiple private addresses to a single public address and the port numbers of host sessions to determine which host to route returning traffic to. The second method uses named address pools. These address pools contain public addresses. When a host with a private address needs to establish communication outside the LAN, it is given a public address from this pool. When the host no longer needs it, the address is returned to the pool.

Clone selected entry on Add

If you want to use an existing rule as the basis for a new rule that you want to create, choose the rule and check this check box. When you click **Add**, the addresses in the rule you chose appear in the Add Address Translation Rule window. You can edit these addresses to obtain the ones you need for the new rule instead of entering the entire address into each field.

What Do You Want to Do?

If you want to:	Do this:
Designate the inside and outside interfaces. You must designate at least one inside interface and one outside interface in order for the router to perform NAT.	Click **Designate NAT interfaces**, and designate interfaces as inside or outside in the NAT Interface Setting window. Interfaces can also be designated as inside or outside interfaces in the Interfaces and Connections window.
Add, edit, or delete an address pool. Dynamic rules can use address pools to assign addresses to devices as they are needed.	Click **Address Pools**, and configure address pool information in the dialog box.
Set the translation timeout.	Click **Translation Timeouts**, and set the timeout in the Translation Timeouts window.
Add a NAT rule.	Click **Add**, and create the NAT rule in the Add Address Translation Rule window. If you want to use an existing NAT rule as a template for the new rule, choose the rule, click **Clone selected entry on Add**, and then click **Add**.

If you want to:	Do this:
Edit a NAT rule.	Choose the NAT rule that you want to edit, click **Edit**, and edit the rule in the Edit Address Translation Rule window.
Delete a NAT rule.	Choose the NAT rule that you want to delete, and click **Delete**. You must confirm deletion of the rule in the Warning box displayed.
View or edit route maps. If virtual private network (VPN) connections are configured on the router, the local IP addresses in the VPN must be protected from NAT translations. When both a VPN and NAT are configured, Cisco Configuration Professional (Cisco CP) creates route maps to protect IP addresses in a VPN from being translated. Additionally, route maps can be configured using the command-line interface (CLI). You can view configured route maps and edit the access rule they use.	Click **View Route MAP**.
Find out how to perform related configuration tasks.	See one of the following procedures: • How Do I Configure NAT Passthrough for a VPN? • How Do I Configure NAT on an Unsupported Interface? • How Do I Configure NAT Passthrough for a Firewall?

Note Many conditions cause previously configured NAT rules to appear as read-only in the Network Address Translation Rules list. Read-only NAT rules are not editable. For more information, see the help topic Reasons that Cisco CP Cannot Edit a NAT Rule.

Designate NAT Interfaces

Use this window to designate the inside and outside interfaces that you want to use in NAT translations. NAT uses the inside and outside designations when interpreting translation rules, because translations are performed from inside to outside, or from outside to inside.

Once designated, these interfaces are used in all NAT translation rules. The designated interfaces appear above the Translation Rules list in the main NAT window.

Interface

All router interfaces are listed in this column.

Inside (trusted)

Check to designate an interface as an inside interface. Inside interfaces typically connect to a LAN that the router serves.

Outside (untrusted)

Check to designate an interface as an outside interface. Outside interfaces typically connect to your organization's WAN or to the Internet.

Translation Timeout Settings

When you configure dynamic NAT translation rules, translation entries have a timeout period after which they expire and are purged from the translation table. Set the timeout values for various translations in this window.

DNS Timeout

Enter the number of seconds after which connections to DNS servers time out.

ICMP Timeout

Enter the number of seconds after which Internet Control Message Protocol (ICMP) flows time out. The default is 60 seconds.

PPTP Timeout

Enter the number of seconds after which NAT Point-to-Point Tunneling Protocol (PPTP) flows time out. The default is 86400 seconds (24 hours).

Dynamic NAT Timeout

Enter the maximum number of seconds that dynamic NAT translations should live.

Max Number of NAT Entries

Enter the maximum number of NAT entries in the translation table.

UDP flow timeouts

Enter the number of seconds that translations for User Datagram Protocol (UDP) flows should live. The default is 300 seconds (5 minutes).

TCP flow timeouts

Enter the number of seconds that translations for Transmission Control Protocol (TCP) flows should live. The default is 86400 seconds (24 hours).

Reset Button

Clicking this button resets translation and timeout parameters to their default values.

Edit Route Map

When VPNs and NAT are both configured on a router, packets that would normally meet the criteria for an IPSec rule will not do so if NAT translates their IP addresses. In this case, NAT translation will cause packets to be sent without being encrypted. Cisco CP may create route maps to prevent NAT from translating IP addresses that you want to be preserved.

Although Cisco CP only creates route maps to limit the action of NAT, route maps can be used for other purposes as well. If route maps have been created using the CLI, they will be visible in this window as well.

Name

The name of this route map.

Route map entries

This box lists the route map entries.

Name

The name of the route map entry.

Seq No.

The sequence number of the route map.

Action

Route maps created by Cisco CP are configured with the **permit** keyword. If this field contains the value **deny**, the route map was created using the CLI.

Access Lists

The access lists that specify the traffic to which this route map applies.

To Edit a Route Map Entry

Choose the entry, click **Edit**, and edit the entry in the Edit Route Map Entry window.

Edit Route Map Entry

Use this window to edit the access list specified in a route map entry.

Name

A read-only field containing the name of the route map entry.

Seq No.

A read-only field containing the sequence number for the route map. When Cisco CP creates a route map, it automatically assigns it a sequence number.

Action

Either **permit** or **deny**. Route maps created by Cisco CP are configured with the **permit** keyword. If this field contains the value **deny**, the route map was created using the CLI.

Access Lists

This area shows the access lists associated with this entry. The route map uses these access lists to determine which traffic to protect from NAT translation.

To Edit an Access List in a Route Map Entry

Choose the access list, and click **Edit**. Then edit the access list in the windows displayed.

Address Pools

The Address Pools window shows the configured address pools that can be used in dynamic NAT translation.

Pool Name

This field contains the name of the address pool. Use this name to refer to the pool when configuring a dynamic NAT rule.

Address

This field contains the IP address range in the pool. Devices whose IP addresses match the access rule specified in the Add Address Translation Rule window will be given private IP addresses from this pool.

What Do You Want to Do?

If you want to:	Do this:
Add an address pool to the router configuration.	Click **Add**, and configure the pool in the Add Address Pool window. If you want to use an existing pool as a template for the new pool, choose the existing pool, check **Clone selected entry on Add**, and click **Add**.
Edit an existing address pool.	Choose the pool entry, click **Edit**, and edit the pool configuration in the Edit Address Pool window.
Delete an address pool.	Choose the pool entry, click **Delete**, and confirm deletion in the Warning box displayed.

Note If Cisco CP detects a previously configured NAT address pool that uses the "type" keyword, that address pool will be read-only and cannot be edited.

Add or Edit Address Pool

Use this window to specify an address pool for dynamic address translation, an address for Port Address Translation (PAT), or a TCP load-balancing rotary pool.

Pool Name

Enter the name of the address pool.

Port Address Translation (PAT)

There may be times when most of the addresses in the pool have been assigned, and the IP address pool is nearly depleted. When this occurs, PAT can be used with a single IP address to satisfy additional requests for IP addresses. Check this check box if you want the router to use PAT when the address pool is close to depletion.

IP Address

Enter the lowest-numbered IP address in the range in the left field; enter the highest-numbered IP address in the range in the right field. For more information, see Available Interface Configurations.

Network Mask

Enter the subnet mask or the number of network bits that specify how many bits in the IP addresses are network bits.

Add or Edit Static Address Translation Rule: Inside to Outside

Use this help topic when you have chosen From Inside to Outside in the Add or the Edit Static Address Translation Rule window.

Use this window to add or edit a static address translation rule. If you are editing a rule, the rule type (static or dynamic) and the direction are disabled. If you need to change these settings, delete the rule, and re-create it using the settings you want.

Two types of static address translations use NAT: simple static and extended static.

Note If you create a NAT rule that would translate addresses of devices that are part of a VPN, Cisco CP will prompt you to allow it to create a route map that protects those addresses from being translated by NAT. If NAT is allowed to translate addresses of devices on a VPN, their translated addresses will not match the IPSec rule used in the IPSec policy, and traffic will be sent unencrypted. You can view route maps created by Cisco CP or created using the CLI by clicking the **View Route Maps** button in the NAT window.

Direction

This help topic describes how to use the Add Address Translation Rule fields when **From inside to outside** is chosen.

From inside to outside

Choose this option if you want to translate private addresses on the LAN to legal addresses on the Internet or on your organization's intranet. You may want to choose this option if you use private addresses on your LAN that are not globally unique on the Internet.

Translate from Interface

This area shows the interfaces from which packets needing address translation come in to the router. It provides fields for you to specify the IP address of a single host, or a network address and subnet mask that represent the hosts on a network.

Inside Interface(s)

If you chose **From inside to outside** for Direction, this area lists the designated inside interfaces.

Note If this area contains no interface names, close the Add Address Translation Rule window, click **Designate NAT interfaces** in the NAT window, and designate the router interfaces as inside or outside. Then return to this window and configure the NAT rule.

IP Address

Do one of the following:

- If you want to create a one-to-one static mapping between the address of a single host and a translated address, known as the *inside global address*, enter the IP address for that host. Do not enter a subnet mask in the Network Mask field.
- If you want to create *n*-to-*n* mappings between the private addresses in a subnet to corresponding inside global addresses, enter any valid address from the subnet whose addresses you want translated, and enter a network mask in the next field.

Network Mask

If you want Cisco CP to translate the addresses of a subnet, enter the mask for that subnet. Cisco CP determines the network and subnet number and the set of addresses needing translation from the IP address and mask that you supply.

Translate to Interface

This area shows the interfaces from which packets with translated addresses exit the router. It also provides fields for specifying the translated address and other information.

Outside Interface(s)

If you chose **From inside to outside** for Direction, this area contains the designated outside interfaces.

Type

- Choose **IP Address** if you want the address to be translated to the address defined in the IP Address field.
- Choose **Interface** if you want the *Translate from* address to use the address of an interface on the router. The *Translate from* address will be translated to the IP address assigned to the interface that you specify in the Interface field.

Interface

This field is enabled if Interface is chosen in the Type field. This field lists the interfaces on the router. Choose the interface whose IP address you want the local inside address translated to.

Note If **Interface** is chosen in the Type field, only translations that redirect TCP/IP ports are supported. The Redirect Port check box is automatically checked and cannot be unchecked.

IP Address

This field is enabled if you chose **IP Address** in the Type field. Do one of the following:

- If you are creating a one-to-one mapping between a single inside local address and a single inside global address, enter the inside global address in this field.
- If you are mapping the inside local addresses of a subnet to the corresponding inside global addresses, enter any IP address that you want to use in the translation in this field. The network mask entered in the *Translate from* Interface area will be used to calculate the remaining inside global addresses.

Note If you do not enter a network mask in the Translate from Interface area, Cisco CP will perform only one translation.

Redirect Port

Check this check box if you want to include port information for the inside device in the translation. This enables you to use the same public IP address for multiple devices, as long as the port specified for each device is different. You must create an entry for each port mapping for this "Translated to" address.

Click **TCP** if this is a TCP port number; click **UDP** if it is a UDP port number.

In the Original Port field, enter the port number on the inside device.

In the Translated Port field, enter the port number that the router is to use for this translation.

Configuration Scenarios

Click Static Address Translation Scenarios for examples that illustrate how the fields in this window are used.

Add or Edit Static Address Translation Rule: Outside to Inside

Use this help topic when you have chosen From Outside to Inside in the Add or the Edit Static Address Translation Rule window.

Use this window to add or edit a static address translation rule. If you are editing a rule, then the rule type (static or dynamic) and the direction are disabled. If you need to change these settings, delete the rule, and re-create it using the settings you want.

Two types of static address translations use NAT: simple static and extended static.

Note If you create a NAT rule that would translate addresses of devices that are part of a VPN, Cisco CP will prompt you to allow it to create a route map that protects those addresses from being translated by NAT. If NAT is allowed to translate

addresses of devices on a VPN, their translated addresses will not match the IPSec rule used in the IPSec policy, and traffic will be sent unencrypted. You can view route maps created by Cisco CP or created using the CLI by clicking the **View Route Maps** button in the NAT window.

Direction

Choose the traffic direction for this rule.

From outside to inside

Choose this option if you want to translate incoming addresses to addresses that will be valid on your LAN. You may want to do this when you are merging networks and must make one set of incoming addresses compatible with an existing set on the LAN served by the router.

This help topic describes how the remaining fields are used when From outside to inside is chosen.

Translate from Interface

This area shows the interfaces from which packets needing address translation come in to the router. It provides fields for you to specify the IP address of a single host, or a network address and subnet mask that represent the hosts on a network.

Outside Interfaces

If you choose **From outside to inside**, this area contains the designated outside interfaces.

Note If this area contains no interface names, close the Add Address Translation Rule window, click **Designate NAT interfaces** in the NAT window, and designate the router interfaces as inside or outside. Then return to this window and configure the NAT rule.

IP Address

Do one of the following:

- If you want to create a one-to-one static mapping between the outside global address of a single remote host and a translated address, known as the *outside local address*, enter the IP address for the remote host.

- If you want to create *n*-to-*n* mappings between the addresses in a remote subnet to corresponding outside local addresses, enter any valid address from the subnet whose addresses you want translated, and enter a network mask in the next field.

Network Mask

If you want Cisco CP to translate the addresses in a remote subnet, enter the mask for that subnet. Cisco CP determines the network and subnet number and the set of addresses needing translation from the IP address and mask that you supply.

Translate to Interface

This area shows the interfaces from which packets with translated addresses exit the router. It also provides fields for specifying the translated address and other information.

Inside Interface(s)

If you choose **From outside to inside**, this area contains the designated inside interfaces.

IP Address

Do one of the following:

- If you are creating a one-to-one mapping between a single outside global address and a single outside local address, enter the outside local address in this field.
- If you are mapping the outside global addresses of a remote subnet to the corresponding outside local addresses, enter any IP address that you want to use in the translation in this field. The network mask entered in the Translate from Interface area will be used to calculate the remaining outside local addresses.

Note If you do not enter a network mask in the Translate from Interface area, Cisco CP will perform only one translation.

Redirect Port

Check this check box if you want to include port information for the outside device in the translation. This enables you to use extended static translation and to use the same public IP address for multiple devices, as long as the port specified for each device is different.

Click **TCP** if this is a TCP port number; click **UDP** if it is a UDP port number.

In the Original Port field, enter the port number on the outside device.

In the Translated Port field, enter the port number that the router is to use for this translation.

Configuration Scenarios

Click Static Address Translation Scenarios for examples that illustrate how the fields in this window are used.

Add or Edit Dynamic Address Translation Rule: Inside to Outside

Use this help topic when you have chosen From Inside to Outside in the Add or the Edit Dynamic Address Translation Rule window.

Add or edit an address translation rule in this window. If you are editing a rule, the rule type (static or dynamic) and the direction are disabled. If you need to change these settings, delete the rule, and re-create it using the settings you want.

A dynamic address translation rule dynamically maps hosts to addresses, using addresses included in a pool of addresses that are globally unique in the destination network. The pool is defined by specifying a range of addresses and giving the range a unique name. The configured router uses the available addresses in the pool (those not used for static translations or for its own WAN IP address) for connections to the Internet or other outside network. When an address is no longer in use, it is returned to the address pool to be dynamically assigned to another device later.

Note If you create a NAT rule that would translate addresses of devices that are part of a VPN, Cisco CP will prompt you to allow it to create a route map that protects those addresses from being translated by NAT. If NAT is allowed to translate addresses of devices on a VPN, their translated addresses will not match the IPSec rule used in the IPSec policy, and traffic will be sent unencrypted.

Direction

Choose the traffic direction for this rule.

From inside to outside

Choose this option if you want to translate private addresses on the LAN to legal (globally unique) addresses on the Internet or on your organization's intranet.

This help topic describes how the remaining fields are used when From inside to outside is chosen.

Translate from Interface

This area shows the interfaces from which packets needing address translation come in to the router. It provides fields for specifying the IP address of a single host, or a network address and subnet mask that represent the hosts on a network.

Inside Interface(s)

If you chose **From inside to outside** for Direction, this area contains the designated inside interfaces.

Note If this area contains no interface names, close the Add Address Translation Rule window, click **Designate NAT interfaces** in the NAT window, and designate the router interfaces as inside or outside. Then return to this window and configure the NAT rule.

Access Rule

Dynamic NAT translation rules use access rules to specify the addresses that need translation. If you choose **From inside to outside**, these are the inside local addresses. Enter the name or number of the access rule that defines the addresses

you want to translate. If you do not know the name or number, you can click the **...** button and choose an existing access rule, or you can create a new access rule to use.

Translate to Interface

This area shows the interfaces from which packets with translated addresses exit the router. It also provides fields for specifying the translated address.

Outside Interface(s)

If you chose **From inside to outside** for Direction, this area contains the designated outside interfaces.

Type

Choose **Interface** if you want the *Translate from* addresses to use the address of an interface on the router. They will be translated to the address that you specify in the Interface field, and PAT will be used to distinguish each host on the network. Choose **Address Pool** if you want the addresses to be translated to addresses defined in a configured address pool.

Interface

If you choose **Interface** in the Type field, this field lists the interfaces on the router. Choose the interface whose IP address you want the local inside addresses translated to. PAT will be used to distinguish each host on the network.

Address Pool

If you choose **Address Pool** in the Type field, you can enter the name of a configured address pool in this field, or you can click **Address Pool** to choose or create an address pool.

Configuration Scenarios

Click Dynamic Address Translation Scenarios for examples that illustrate how the fields in this window are used.

Add or Edit Dynamic Address Translation Rule: Outside to Inside

Use this help topic when you have chosen From Outside to Inside in the Add or the Edit Dynamic Address Translation Rule window.

Add or edit an address translation rule in this window. If you are editing a rule, the rule type (static or dynamic) and the direction are disabled. If you need to change these settings, delete the rule, and re-create it using the settings you want.

A dynamic address translation rule dynamically maps hosts to addresses, using addresses included in a pool of addresses that are globally unique in the destination network. The pool is defined by specifying a range of addresses and giving the range a unique name. The configured router uses the available addresses in the pool (those not used for static translations or for its own WAN IP address) for connections to the Internet or other outside network. When an address is no longer in use, it is returned to the address pool to be dynamically assigned to another device later.

Note If you create a NAT rule that would translate addresses of devices that are part of a VPN, Cisco CP will prompt you to allow it to create a route map that protects those addresses from being translated by NAT. If NAT is allowed to translate addresses of devices on a VPN, their translated addresses will not match the IPSec rule used in the IPSec policy, and traffic will be sent unencrypted.

Direction

Choose the traffic direction for this rule.

From outside to inside

Choose this option if you want to translate incoming addresses to addresses that will be valid on your LAN. You may want to do this when you are merging networks and must make one set of incoming addresses compatible with an existing set on the LAN served by the router.

This help topic describes how the remaining fields are used when From outside to inside is chosen.

Translate from Interface

This area shows the interfaces from which packets needing address translation come in to the router. It provides fields for specifying the IP address of a single host, or a network address and subnet mask that represent the hosts on a network.

Outside Interfaces

If you chose **From outside to inside**, this area contains the designated outside interfaces.

Note If this area contains no interface names, close the Add Address Translation Rule window, click **Designate NAT interfaces** in the NAT window, and designate the router interfaces as inside or outside. Then return to this window and configure the NAT rule.

Access Rule

Dynamic NAT translation rules use access rules to specify the addresses that need translation. If you choose **From outside to inside**, these are the outside global addresses. Enter the name or number of the access rule that defines the addresses you want to translate. If you do not know the name or number, you can click the **...** button and choose an existing access rule, or you can create a new access rule to use.

Translate to Interface

This area shows the interfaces from which packets with translated addresses exit the router. It also provides fields for specifying the translated address.

Inside Interface(s)

If you choose **From outside to inside**, this area contains the designated inside interfaces.

Type

Choose **Interface** if you want the *Translate from* addresses to use the address of an interface on the router. They will be translated to the address that you specify in the Interface field, and PAT will be used to distinguish each host on the network. Choose **Address Pool** if you want the addresses to be translated to addresses defined in a configured address pool.

Interface

If you choose **Interface** in the Type field, this field lists the interfaces on the router. Choose the interface whose IP address you want the local inside addresses translated to. PAT will be used to distinguish each host on the network.

Address Pool

If you choose Address Pool in the Type field, you can enter the name of a configured address pool in this field, or you can click **Address Pool** to choose or create an address pool.

Configuration Scenarios

Click Dynamic Address Translation Scenarios for examples that illustrate how the fields in this window are used.

How Do I . . .

This section contains procedures for tasks that the wizard does not help you complete.

How do I Configure Address Translation for Outside to Inside

The NAT wizard allows you to configure a Network Address Translation (NAT) rule to translate addresses from inside to outside. To configure a NAT rule to translate addresses from outside to inside, follow the directions in one of the following sections:

- Add or Edit Dynamic Address Translation Rule: Outside to Inside
- Add or Edit Static Address Translation Rule: Outside to Inside

How Do I Configure NAT With One LAN and Multiple WANs?

The NAT wizard allows you to configure a Network Address Translation (NAT) rule between one LAN interface on your router and one WAN interface. If you want to configure NAT between one LAN interface on your router and multiple WAN interfaces, first use the NAT wizard to configure an address translation rule between the LAN interface on your router and one WAN interface. Then follow the directions in one of the following sections:

- Add or Edit Static Address Translation Rule: Inside to Outside
- Add or Edit Dynamic Address Translation Rule: Inside to Outside

Each time you add a new address translation rule using the directions in one of these sections, choose the same LAN interface and a new WAN interface. Repeat this procedure for all WAN interfaces that you want to configure with address translation rules.

CHAPTER 19

Quality of Service

You can use Cisco Configuration Professional (CP) to configure and edit quality of service (QoS) policies on the router's WAN interfaces. You can also use Cisco CP to enable QoS policies on the router's IPSec VPN interfaces and tunnels.

The following sections provide more information:

- Understanding QoS, page 19-1
- Working with QoS Policies, page 19-3
- Create QoS Policy Reference, page 19-17
- Edit QoS Policy Reference, page 19-30

Understanding QoS

Quality of service (QoS) is a set of capabilities that allow you to deliver differentiated services for network traffic, thereby providing better service for selected network traffic. QoS expedites the handling of mission-critical applications, while sharing network resources with noncritical applications.

QoS also ensures the available bandwidth and minimum delays that are required by time-sensitive multimedia and voice applications. This allows you to use expensive network connections more efficiently and to establish service level agreements with customers of the network.

QoS features provide better and more predictable network service by:

- Supporting dedicated bandwidth for critical users and applications

- Controlling jitter and latency (required by real-time traffic)
- Avoiding and managing network congestion
- Shaping network traffic to smooth the traffic flow
- Setting traffic priorities across the network

You can use the QoS configuration wizard in Cisco CP to create QoS policies on the router's WAN interfaces. You can also use Cisco CP to configure QoS policies on the router's IPSec VPN interfaces and tunnels.

When you configure QoS policies on a per-tunnel basis, Cisco CP treats each security association tunnel as a separate traffic class and allows you to configure a unique policy map for each class.

Note The configuring QoS policies per-tunnel feature (Dynamic Multipoint Virtual Private Network [DMVPN] QoS feature) is supported on routers that are running the Cisco IOS Release 12.4(22)T and later advanced security images.

QoS Policy Terms

The following QoS policy terms are used in the QoS configuration wizard pages:

- DSCP Marking (trusted)—Cisco network devices such as IP phones and switches add differentiated services code point (DSCP) markings to packets. Configuring DSCP on the router allows these markings to be used to classify traffic.
- NBAR Protocol Discovery (untrusted)—When an application is recognized and classified by Network Based Application Recognition (NBAR), a network can invoke services for that specific application. By classifying packets and then applying QoS to the classified traffic, NBAR ensures that network bandwidth is used efficiently.
- Queuing—Traffic queuing aggregates packet streams to multiple queues and provides different service to each queue.
- Shaping—Traffic shaping retains excess packets in a queue and then reschedules the excess packets for later transmission over increments of time.
- Policing—Traffic policing propagates bursts. When the traffic rate reaches the configured maximum rate, excess traffic is dropped or re-marked.

Working with QoS Policies

This section contains the following topics:

- Creating QoS Policies, page 19-3
- Editing QoS Policies, page 19-7

Creating QoS Policies

You can use the QoS wizard to create QoS policies on the router's WAN interfaces. You can also use Cisco CP to create QoS policies on the router's IPSec VPN interfaces and tunnels. See the following topics for more information:

- Creating QoS Policies on a WAN Interface, page 19-3
- Creating QoS Policies on a DMVPN Spoke Tunnel Interface, page 19-5

Creating QoS Policies on a WAN Interface

Before You Begin

- From the Select Community Member drop-down list, choose the router on which you want to create a QoS policy.
- If you are creating a policy on the router's DMVPN hub tunnel interface, make sure that DMVPN is configured on it. See Dynamic Multipoint VPN, page 29-1.

Note The configuring QoS policies per-tunnel feature (DMVPN QoS feature) is supported on routers that are running the Cisco IOS Release 12.4(22)T and later advanced security images.

Procedure

Use this procedure to create a QoS policy on a QoS configurable WAN interface.

Step 1 Choose **Configure > Router > QoS**. The Quality of Service page opens with the Create QoS Policy tab selected by default.

Step 2 Click the **Launch QoS Wizard** button to start the QoS wizard. The QoS Configuration Wizard page opens.

Step 3 Click **Next**. The Interface Selection page opens. See Interface Selection Page, page 19-18.

Step 4 From the Interface Selection page, choose the WAN or the DMVPN hub tunnel interface as appropriate, and then click **Next**.

The Classification page opens. See Classification Page, page 19-21.

Step 5 From the Classification page, click the DSCP Marking (trusted) radio button or the NBAR Protocol Discovery (untrusted) radio button as appropriate, and then click **Next**.

The Queuing With Shaping for Outbound Traffic page opens. See Queuing With Shaping for Outbound Traffic Page, page 19-22.

Step 6 In the Queuing With Shaping for Outbound Traffic page, make the configuration settings, and then click **Next**. The Policing for Outbound Traffic page opens. See Policing for Outbound Traffic Page, page 19-26.

Step 7 In the Policing for Outbound Traffic page, enter the values, and then click **Next**.

Note If you are configuring a DMVPN hub tunnel interface on a router that supports the DMVPN QoS feature, the QoS Group Name field is displayed in the Policing for Outbound Traffic page. If you are configuring another type of interface, such as site-to-site VPN tunnel interface or GREoIPSec tunnel interface, the QoS Group Name field is not displayed.

The QoS Configuration Summary page opens, displaying a summary of the configurations you made. See QoS Configuration Summary Page, page 19-29.

Step 8 Review the configuration. If you need to make changes, click the **Back** button to return to the page in which you need to make the changes, and then return to the QoS Configuration Summary page.

Step 9 In the QoS Configuration Summary page, click **Finish**. The Deliver Configuration to Router page opens.

Step 10 Click **Deliver**. The Commands Delivery Status window opens.

Step 11 Click **OK** to send the configuration to the router.

Related Topics

- Create QoS Configuration Wizard, page 19-17

Creating QoS Policies on a DMVPN Spoke Tunnel Interface

Before You Begin

- From the Select Community Member drop-down list, choose the router on which you want to create a QoS policy.
- Make sure that the DMVPN spoke tunnel interface (configured for a hub and spoke topology) is configured on the router. See Dynamic Multipoint VPN, page 29-1.

Note The configuring QoS policies per-tunnel feature (DMVPN QoS feature) is supported on routers that are running the Cisco IOS Release 12.4(22)T and later advanced security images.

Procedure

Use this procedure to create a QoS policy for a DMVPN spoke tunnel interface.

Step 1 Choose **Configure > Router > QoS**. The Quality of Service page opens with the Create QoS Policy tab selected by default.

Step 2 Click the **Launch QoS Wizard** button to start the QoS wizard. The QoS Configuration Wizard page opens.

Step 3 Click **Next**. The Interface Selection page opens. See Interface Selection Page, page 19-18.

Step 4 From the Interface Selection page, choose the DMVPN spoke tunnel interface (configured for a hub and spoke topology), and then click **Next**.

The QoS Group Name page opens. See QoS Group Name Page—Appears for DMVPN Spoke Tunnel Interface, page 19-20.

Step 5 Do one of the following:

- If you know the group name that is configured for the DMVPN hub tunnel interface, do the following:
  - Choose the **Yes** radio button, and then enter the group name in the QoS Group name field.
  - Click **Next**. The QoS Configuration Summary page opens, displaying a summary of the configurations you made. See QoS Configuration Summary Page, page 19-29.
  - Go to Step 9.
- If you do not know the group name that is configured for the DMVPN hub tunnel interface, choose the **No** radio button, and then click **Next**. The Classification page opens. See Classification Page, page 19-21.

Step 6 From the Classification page, click the DSCP Marking (trusted) radio button or NBAR Protocol Discovery (untrusted) radio button as appropriate, and then click **Next**.

The Queuing With Shaping for Outbound Traffic page opens. See Queuing With Shaping for Outbound Traffic Page, page 19-22.

Step 7 In the Queuing With Shaping for Outbound Traffic page, make the configuration settings, and then click **Next**. The Policing for Outbound Traffic page opens. See Policing for Outbound Traffic Page, page 19-26.

Step 8 In the Policing for Outbound Traffic page, enter the values in the Policing for Outbound Traffic pane, and then click **Next**.

The QoS Configuration Summary page opens displaying a summary of the configurations you made. See QoS Configuration Summary Page, page 19-29.

Step 9 Review the configuration. If you need to make changes, click the **Back** button to return to the page in which you need to make the changes, and then return to the QoS Configuration Summary page.

Step 10 In the QoS Configuration Summary page, click **Finish**. The Deliver Configuration to Router page opens.

Step 11 Click **Deliver**. The Commands Delivery Status window opens.

Step 12 Click **OK** to send the configuration to the router.

Related Topics

- Create QoS Configuration Wizard, page 19-17

Editing QoS Policies

Before You Begin

From the Select Community Member drop-down list, choose the router for which you want to edit QoS policies.

Procedure

Use this procedure to add, edit, or delete a QoS class; to view policies; to associate or disassociate policies; or to add a service policy to a selected interface.

Step 1 Choose **Configure > Router > QoS**. The Quality of Service page opens.

Step 2 Click the **Edit QoS Policy** tab to open the Edit QoS Policy page. See Edit QoS Policy Page, page 19-31.

Step 3 To add a QoS class, click the **Add** button. See Adding a QoS Class, page 19-10.

Step 4 To change the QoS class information, select a class, and then click the **Edit** button. See Editing the QoS Class Information, page 19-11.

Step 5 To delete a QoS class, select the class, and then click the **Delete** button. See Deleting a QoS Class, page 19-12.

Step 6 To associate or disassociate QoS policies, see Associating and Disassociating QoS Policies, page 19-8.

Step 7 To add a service policy, click the **Add Service Policy** button. See Adding Service Policy to a Class, page 19-9.

Step 8 To view associated QoS policies on a DMVPN hub tunnel interface, click the **Show Policies** button. See Viewing Associated QoS Policies, page 19-16.

Step 9 To modify the QoS group name on a DMVPN hub tunnel interface, click the **Edit QoS Group Name** button, which is located next to the QoS group name field. Then change the group name. See Add or Edit QoS Group Name Dialog Box—Appears for DMVPN Hub Tunnel Interface, page 19-52.

Step 10 To add the QoS group name for a DMVPN spoke tunnel interface, see Configure QoS Group Name Dialog Box—Appears for DMVPN Spoke Tunnel Interface, page 19-51.

Step 11 After you make the changes, click **Apply Changes**. The Deliver Configuration to Router page opens.

Step 12 Click **Deliver**. The Commands Delivery Status window opens.

Step 13 Click **OK** to send the configuration to the router.

Related Topics

- Edit QoS Policy Reference, page 19-30

Associating and Disassociating QoS Policies

Before You Begin

- From the Select Community Member drop-down list, choose the router on which you want to associate or disassociate a QoS policy.
- Make sure that a QoS policy is created on the router's interface. See Creating QoS Policies, page 19-3.

Procedure

Use this procedure to associate or disassociate a QoS policy to the interface.

You can associate a QoS policy to outbound traffic only. If you try to associate a QoS policy to inbound traffic, you will see a warning message.

Step 1 Choose **Configure > Router > QoS**. The Quality of Service page opens.

Step 2 Click the **Edit QoS Policy** tab to open the Edit QoS Policy page. See Edit QoS Policy Page, page 19-31.

Step 3 From the View Policy on Interface drop-down list, choose the interface on which you want to associate or disassociate the QoS policy.

Note If you choose the interface that Cisco CP uses to communicate with the router, the connection between Cisco CP and the router might be lost.

Step 4 From the In Direction drop-down list, choose Inbound or Outbound as appropriate.

Step 5 To associate the policy, click the **Associate** button, and then choose **Associate Policy** from the drop-down list.

The Associate a Policy Map to Interface page opens. See Associate a Policy Map to Interface, page 43-3.

Step 6 To disassociate a policy, click the **Associate** button, and then choose **Disassociate Policy** from the drop-down list. The Cisco CP Warning page opens, asking you if you are sure that you want to disassociate the policy. Click **Yes**.

Step 7 Click **Apply Changes**. The Deliver Configuration to Router page opens.

Step 8 Click **Deliver**. The Commands Delivery Status window opens.

Step 9 Click **OK** to send the configuration to the router.

Related Topics

- Edit QoS Policy Reference, page 19-30

Adding Service Policy to a Class

Procedure

Use this procedure to add a service policy to a class.

Note The Add Service Policy and the Remove Service Policy buttons are enabled when:

- QoS policy is configured with Shaping value.
- If you choose to add a service policy to a default class.

Step 1 Choose **Configure > Router > QoS**. The Quality of Service page opens.

Step 2 Click the **Edit QoS Policy** tab.

Step 3 Select a class, and then click the **Add Service Policy** button.

Step 4 To add a new service policy, choose **Add New** from the drop-down list. The Add Class for a New Policy Page opens. See Add Class for the New Service Policy Dialog Box, page 19-37.

Step 5 To add an existing service policy, choose **Add Existing** from the drop-down list. The Add Service Policy to Class page opens. See Add Service Policy to Class Dialog Box, page 19-38.

Step 6 Add the information, and then click **OK**.

Step 7 Click **Apply Changes**. The Deliver Configuration to Router page opens.

Step 8 Click **Deliver**. The Commands Delivery Status window opens.

Step 9 Click **OK** to send the configuration to the router.

Related Topics

- Edit QoS Policy Reference, page 19-30

Adding a QoS Class

Before You Begin

- From the Select Community Member drop-down list, choose the router on which you want to add a QoS class.
- Make sure that a QoS policy is created on the router's interface. See Creating QoS Policies, page 19-3.

Procedure

Use this procedure to add a class to a QoS policy.

Step 1 Choose **Configure > Router > QoS**. The Quality of Service page opens.

Step 2 Click the **Edit QoS Policy** tab to open the Edit QoS Policy page, and then click **Add**.

The Add a QoS Class page opens. See Add or Edit a QoS Class Dialog Box, page 19-40.

Step 3 Enter the class name in the Class Name field.

Step 4 In the Classification pane, choose the values for which you want the router to examine traffic.

Step 5 In the Action pane, choose the action that the router must take when the router finds the traffic that matches the specified value.

Step 6 Click **OK**.

Step 7 Click **Apply Changes**. The Deliver Configuration to Router page opens.

Step 8 Click **Deliver**. The Commands Delivery Status window opens.

Step 9 Click **OK** to send the configuration to the router.

Related Topics

- Editing QoS Policies, page 19-7
- Edit QoS Policy Page, page 19-31
- Add or Edit a QoS Class Dialog Box, page 19-40

Editing the QoS Class Information

Before You Begin

- From the Select Community Member drop-down list, choose the router for which you want to edit the QoS class information.
- Make sure that a QoS policy is created on the router's interface. See Creating QoS Policies, page 19-3.

Procedure

Use this procedure to edit the QoS class information.

Step 1 Choose **Configure > Router > QoS**. The Quality of Service page opens.

Step 2 Click the **Edit QoS Policy** tab to open the Edit QoS Policy page, and then click **Edit**.

The Edit a QoS Class page opens. See Add or Edit a QoS Class Dialog Box, page 19-40.

Step 3 To edit the values in the Classification pane, click the value, and then click the **Edit** button next to it. See Editing DSCP, Protocols, and ACL Classification Values, page 19-13

Step 4 To edit the Queuing, Shaping, or Policing parameters in the Action pane, select the parameter, and then click the **Configure Queuing**, **Configure Shaping**, or **Configure Policing** button as appropriate. See Editing Queuing, Policing, and Shaping Action Parameters, page 19-15.

Step 5 Click **OK**.

Step 6 Click **Apply Changes**. The Deliver Configuration to Router page opens.

Step 7 Click **Deliver**. The Commands Delivery Status window opens.

Step 8 Click **OK** to send the configuration to the router.

Related Topics

- Editing QoS Policies, page 19-7
- Edit QoS Policy Page, page 19-31
- Add or Edit a QoS Class Dialog Box, page 19-40

Deleting a QoS Class

Before You Begin

- From the Select Community Member drop-down list, choose the router for which you want to delete a QoS class.
- Make sure that a QoS policy is created on the router's interface. See Creating QoS Policies, page 19-3.

Procedure

Use this procedure to delete a QoS class.

Step 1 Choose **Configure > Router > QoS**. The Quality of Service page opens.

Step 2 Click the **Edit QoS Policy** tab to open the Edit QoS Policy page.

Step 3 Select the class you want to delete, and then click **Delete**.

Related Topics

- Editing QoS Policies, page 19-7
- Edit QoS Policy Page, page 19-31

Editing DSCP, Protocols, and ACL Classification Values

Before You Begin

- From the Select Community Member drop-down list, choose the router for which you want to edit the classification values.
- Make sure that a QoS policy is created on the router's interface. See Creating QoS Policies, page 19-3.

Procedure

Use this procedure to edit DSCP, protocols, and access control list (ACL) classification values.

Step 1 Choose **Configure > Router > QoS**. The Quality of Service page opens.

Step 2 Click the **Edit QoS Policy** tab to open the Edit QoS Policy page, and then click **Edit**.

The Edit a QoS Class page opens. See Add or Edit a QoS Class Dialog Box, page 19-40.

Step 3 To edit the DSCP values, choose **DSCP** from the Classification pane, and then click the **Edit** button. The Edit Match DCSP Values dialog box opens. See Edit Match DSCP Values Dialog Box, page 19-42.

Step 4 To edit the protocol values, choose **Protocol** from the Classification pane, and then click the **Edit** button. The Edit Match Protocol Values dialog box opens. See Edit Match Protocol Values Dialog Box, page 19-43.

To add custom protocols that are not available in the Edit Match Protocol Values window, click the **Custom Protocol** button. See Add Custom Protocols Dialog Box, page 19-44.

Step 5 To edit the ACL values, choose **ACL** from the Classification pane, and then click the **Edit** button. The Edit Match ACL dialog box opens. For details, see Edit Match ACL Dialog Box, page 19-45.

Step 6 Click **OK**.

Step 7 Click **Apply Changes**. The Deliver Configuration to Router page opens.

Step 8 Click **Deliver**. The Commands Delivery Status window opens.

Step 9 Click **OK** to send the configuration to the router.

Related Topics

- Editing QoS Policies, page 19-7
- Edit QoS Policy Page, page 19-31
- Adding Custom Protocols, page 19-14

Adding Custom Protocols

Before You Begin

- From the Select Community Member drop-down list, choose the router on which you want to add custom protocols.
- Make sure that a QoS policy is created on the router's interface. See Creating QoS Policies, page 19-3.

Procedure

Use this procedure to add custom protocols that are not available in the Edit Match Protocol Values dialog box.

Step 1 Choose **Configure > Router > QoS**. The Quality of Service page opens.

Step 2 Click the **Edit QoS Policy** tab to open the Edit QoS Policy page, and then click **Edit**.

The Edit a QoS Class page opens. See Add or Edit a QoS Class Dialog Box, page 19-40.

Step 3 To add custom protocols that are not available in the Edit Match Protocol Values window, click the **Custom Protocol** button. The Custom Protocols page opens. See Add Custom Protocols Dialog Box, page 19-44.

Step 4 Choose the name of the custom protocol from the Name list.

Step 5 Click the TCP or UDP radio button as appropriate.

Step 6 Define the port numbers that this protocol should use. Enter a port number in the New Port Number field, and then click **Add** to add it to the Port Numbers list.

Step 7 To remove a port number from the list, choose the port number, and then click **Remove**.

Related Topics

- Editing QoS Policies, page 19-7
- Edit QoS Policy Page, page 19-31
- Editing DSCP, Protocols, and ACL Classification Values, page 19-13
- Configure Policing Dialog Box, page 19-46

Editing Queuing, Policing, and Shaping Action Parameters

Before You Begin

- From the Select Community Member drop-down list, choose the router for which you want to edit the action parameters.
- Make sure that a QoS policy is created on the router's interface. See Creating QoS Policies, page 19-3.

Procedure

Use this procedure to edit queuing, shaping, or policing action parameters.

Step 1 Choose **Configure > Router > QoS**. The Quality of Service page opens.

Step 2 Click the **Edit QoS Policy** tab to open the Edit QoS Policy page, and then click **Edit**.

The Edit a QoS Class page opens. See Add or Edit a QoS Class Dialog Box, page 19-40.

Step 3 From the Action pane, do the following:

- To edit the Queuing parameter, choose **Queuing**, and then click the **Configure Queuing** button. See Configure Queuing Dialog Box, page 19-49.
- To edit the Shaping parameter, choose **Shaping**, and then click the **Configure Queuing** button. See Configure Shaping Dialog Box, page 19-48.
- To edit the Policing parameter, choose **Policing**, and then click the **Configure Queuing** button. See Configure Policing Dialog Box, page 19-46.

Step 4 Make the changes, and then click **OK**.

Step 5 Click **Apply Changes**. The Deliver Configuration to Router page opens.

Step 6 Click **Deliver**. The Commands Delivery Status window opens.

Step 7 Click **OK** to send the configuration to the router.

Related Topics

- Editing QoS Policies, page 19-7
- Edit QoS Policy Page, page 19-31

Viewing Associated QoS Policies

Before You Begin

- From the Select Community Member drop-down list, choose the router for which you want to view the associated QoS policies.
- Make sure that a QoS policy is created on the router's interface. See Creating QoS Policies, page 19-3.

Procedure

Use this procedure to view the QoS policies that are associated with the chosen tunnel interface.

If more than one QoS policy is associated with a DMVPN hub tunnel interface, the Show Policies button is enabled. Click this button to view all of the policies associated with that tunnel interface.

Step 1 Choose **Configure > Router > QoS**. The Quality of Service page opens.

Step 2 Click the **Edit QoS Policy** tab to open the Edit QoS Policy page, and then click the **Show Policies** button.

The Policies Associated Details page opens providing a list of the policies that are associated with the group name on the chosen tunnel interface. See Policies Associated Details Dialog Box.

Related Topics

- Editing QoS Policies, page 19-7
- Edit QoS Policy Page, page 19-31
- Policies Associated Details Dialog Box, page 19-51

Create QoS Policy Reference

This section describes the pages and dialog boxes that you can use when working with the Create QoS Policy wizard and includes the following topic:

- Create QoS Configuration Wizard

Create QoS Configuration Wizard

Use the QoS configuration wizard to create (enable) quality of service (QoS) policies on the router's WAN interfaces. You can also use Cisco CP to create QoS policies on the router's IPSec VPN interfaces and tunnels.

To understand the QoS policy terms used in the QoS configuration wizard pages, see QoS Policy Terms, page 19-2.

Note The QoS policy is applied to outgoing traffic on the interface.

The QoS policy wizard includes the following pages:

- QoS Configuration Wizard Page, page 19-18
- Interface Selection Page, page 19-18

- QoS Group Name Page—Appears for DMVPN Spoke Tunnel Interface, page 19-20
- Classification Page, page 19-21
- Queuing With Shaping for Outbound Traffic Page, page 19-22
- Policing for Outbound Traffic Page, page 19-26
- QoS Configuration Summary Page, page 19-29

How to Get to This Wizard

1. Choose **Configure > Router > QoS**. The Quality of Service page opens with the Create QoS Policy tab selected by default.
2. Click the **Launch QoS Wizard** button to start the QoS wizard.

QoS Configuration Wizard Page

The QoS Configuration Wizard page is the "welcome" page. It summarizes the information that you must provide in the QoS configuration wizard pages.

Click **Next** to begin configuring a QoS policy. The Interface Selection page opens.

How to Get to This Page

1. Choose **Configure > Router > QoS**. The Quality of Service page opens with the Create QoS Policy tab selected by default.
2. Click the **Launch QoS Wizard** button to start the QoS wizard.

Related Topics

- Creating QoS Policies, page 19-3
- Create QoS Configuration Wizard, page 19-17

Interface Selection Page

Use the Interface Selection page to choose the interface on which you want to configure the QoS policy.

How to Get to This Page

1. Choose **Configure > Router > QoS**. The Quality of Service page opens with the Create QoS Policy tab selected by default.

2. Click the **Launch QoS Wizard** button to start the QoS wizard, and then click **Next**.

Related Topics

- Creating QoS Policies, page 19-3
- Create QoS Configuration Wizard, page 19-17

Field Reference

Table 19-1 Interface Selection Page

Element	Description
Interface	The interface on which you want to configure the QoS policy. This field lists WAN interfaces and interfaces that do not have a configured outbound QoS policy. VPN interfaces such as DMVPN hub and spoke tunnel interfaces are included in the list, but interfaces used for Easy VPN clients and interfaces with an existing QoS policy are not included. **Note** If the router Cisco IOS image release is 12.4(11)T or later, virtual template tunnel interfaces may appear in this list. If you choose a VTI interface, you will be able to configure shaping and queuing parameters. **Note** The configuring QoS policies per-tunnel feature (DMVPN QoS feature) is supported on routers that are running the Cisco IOS Release 12.4(22)T and later advanced security images.
Details button	Click this button to view configuration details about the chosen interface. The window displays the interface's IP address and subnet mask, names of access rules and policies applied to the interface, and connections that the interface is used for.
Next button	Click this button to open the next wizard page. • For WAN interface and DMVPN hub tunnel interface—When you click **Next**, the Classification page opens. • For DMVPN spoke tunnel interface—When you click **Next**, the the QoS Group Name page opens.

QoS Group Name Page—Appears for DMVPN Spoke Tunnel Interface

Use the QoS Group Name page to provide the group name of the DMVPN hub tunnel interface.

Note

- The QoS Group Name page is displayed when you choose the DMVPN spoke tunnel interface (configured for hub and spoke topology) in the Interface Selection page.
- The configuring QoS policies per-tunnel feature (DMVPN QoS feature) is supported on routers that are running the Cisco IOS Release 12.4(22)T and later advanced security images.

How to Get to This Page

1. Choose **Configure > Router > QoS**. The Quality of Service page opens with the Create QoS Policy tab selected by default.
2. Click the **Launch QoS Wizard** button to start the QoS wizard.
3. Click **Next** until you reach the QoS Group Name page.

Related Topics

- Creating QoS Policies, page 19-3
- Create QoS Configuration Wizard, page 19-17
- Configure QoS Group Name Dialog Box—Appears for DMVPN Spoke Tunnel Interface, page 19-51

Field Reference

Table 19-2 QoS Group Name Page

Element	Description
Yes radio button	Click this radio button if you know the group name that is configured for the DMVPN hub tunnel interface. Then enter the group name in the QoS Group Name field.
No radio button	Click this radio button if you do not know the group name that is configured for the DMVPN hub tunnel interface.

Table 19-2 QoS Group Name Page

Element	Description
QoS Group Name	The QoS group name configured for the DMVPN hub tunnel interface. This field is enabled when you choose the Yes radio button. Make sure that the group name you enter in this field matches with the group name that is configured for the DMVPN hub tunnel interface.
Next button	Click this button to open the next wizard page. • If you click the Yes radio button, provide the QoS group name, and then click Next, the QoS Configuration Summary page opens. • If you click the No radio button, and then click Next, the Classification page opens.
Back button	Click this button to go back to the previous wizard page.

Classification Page

Use the Classification page to choose whether the outbound traffic is based on DCSP markings (trusted) or is based on NBAR protocol discovery (untrusted).

How to Get to This Page

1. Choose **Configure > Router > QoS**. The Quality of Service page opens with the Create QoS Policy tab selected by default.
2. Click the **Launch QoS Wizard** button to start the QoS wizard.
3. Click **Next** until you reach the Classification page.

Related Topics

- Creating QoS Policies, page 19-3
- Create QoS Configuration Wizard, page 19-17

Field Reference

Table 19-3 Classification Page

Element	Description
DSCP marking (trusted) radio button	Click this radio button to use differentiated services code point (DSCP) markings to classify traffic. Cisco network devices such as IP phones and switches add DSCP markings to packets. Configuring DSCP on the router allows these markings to be used to classify traffic. **Note** If the Cisco IOS image on the router does not support DSCP marking, this option will not appear.
NBAR protocol discovery (untrusted) radio button	Click this radio button to use Networked-Based Application Recognition (NBAR) protocol discovery to classify traffic. When an application is recognized and classified by NBAR, a network can invoke services for that specific application. By classifying packets and then applying QoS to the classified traffic, NBAR ensures that network bandwidth is used efficiently. **Note** If the Cisco IOS image on the router does not support NBAR protocol discovery, this option will not appear.
Next button	Click this button to open the Queuing With Shaping for Outbound Traffic page.
Back button	Click this button to go back to the previous wizard page.

Queuing With Shaping for Outbound Traffic Page

Use the Queuing With Shaping for Outbound Traffic page to configure queuing and shaping for outbound traffic.

Queuing—Traffic queuing aggregates packet streams to multiple queues and provides different service to each queue.

Shaping—Traffic shaping retains excess packets in a queue and then reschedules the excess packets for later transmission over increments of time.

How to Get to This Page

1. Choose **Configure > Router > QoS**. The Quality of Service page opens with the Create QoS Policy tab selected by default.

2. Click the **Launch QoS Wizard** button to start the QoS wizard.
3. Click **Next** until you reach the Queuing With Shaping for Outbound Traffic page.

Related Topics

- Creating QoS Policies, page 19-3
- Create QoS Configuration Wizard, page 19-17

Field Reference

Table 19-4 Queuing With Shaping for Outbound Traffic Page

Element	Description
Configure Shaping radio button	Click this radio button to configure shaping for outbound traffic. If you are configuring QoS policy on a tunnel interface (such as DMVPN hub tunnel, DMVPN spoke tunnel, site-to-site VPN tunnel, GREoIPSec tunnel, or virtual template interface), you must configure shaping and provide the committed information rate (CIR) value.
Committed Information Rate	The CIR is the rate at which the interface is to transfer data. Enter the CIR in kilobits per second.
Bandwidth Allocation Pane	
Traffic Class	Specific type of traffic, such as voice traffic or routing traffic. The Cisco CP default traffic classes and user-created traffic classes are listed in this column.
Bandwidth Percentage	Bandwidth percentage for a traffic class. Enter the percentage value for a traffic class. Traffic types that depend on high transmission rates, such as voice traffic, should be given a higher percentage than traffic classes that do not need high transmission rates, such as routing traffic. The Cisco CP default traffic classes are displayed with suggested values. When you change the percentage value of any traffic class, the best effort class adjusts to a higher or lower value. The total bandwidth of all classes other than best effort cannot exceed 75%.

Table 19-4 Queuing With Shaping for Outbound Traffic Page (continued)

Element	Description
Allotted Bandwidth	Cisco CP displays the Allotted Bandwidth column when you configure a QoS policy for a non-VTI interface. It displays the kilobits per second allotted to the traffic class, based on the CIR and the bandwidth percentage entered.
Add Class button	Click this button to add a traffic class to the policy. Then enter the class information in the displayed dialog box. See Add a New Traffic Class Dialog Box, page 19-24.
Remove button	Click this button to remove a traffic class from the list that you have created. **Note** You cannot remove the Cisco CP default classes.
Next button	Click this button to open the Policing for Outbound Traffic page.
Back button	Click this button to go back to the previous wizard page.

Add a New Traffic Class Dialog Box

Use the Add a New Traffic Class dialog box to add a new QoS traffic class.

How to Get to This Dialog Box

1. Choose **Configure > Router > QoS**. The Quality of Service page opens with the Create QoS Policy tab selected by default.
2. Click the **Launch QoS Wizard** button to start the QoS wizard.
3. Click **Next** until you reach the Queuing With Shaping for Outbound Traffic page.
4. From the Queuing With Shaping for Outbound Traffic page, click the **Add Class** button to open the Add a New Traffic Class page.

Related Topics

- Queuing With Shaping for Outbound Traffic Page, page 19-22
- Creating QoS Policies, page 19-3

Field Reference

Table 19-5 Add New Traffic Class Fields

Element	Description
Class Name	Enter a name for the traffic class.
Classification Pane	
Match	Specify whether the QoS class is to look for matches to Any or to All of the selected criteria. If you choose Any, traffic must meet only one of the match criteria. If you choose All, traffic must meet all of the match criteria. The DSCP values chosen are displayed in the DSCP column. Any radio button—Click **Any** to specify that the traffic must meet only one of the criteria specified in the classification list that you create. All radio button—Click **All** to specify that traffic must meet all the criteria specified in the classification list that you create.
Item Name	This column displays the types of criteria that you can include in this traffic class. If the QoS policy uses NBAR protocol discovery, you can specify protocol and ACL values. If the QoS policy uses DSCP marking, you can specify DSCP values as well as protocol and ACL values.
Item Value	This column displays the values configured for the particular type, separated by commas. For example, the Protocol row might show the following values: `http, edonkey, dhcp`
Edit button	To add or edit the values for a particular type of entry, select the type, and click **Edit**. Then, add or modify entries for type in the displayed dialog.
Bandwidth Percentage	Enter the bandwidth percentage that you want to give to the class. Cisco CP displays a message if you enter a value that causes the total percentage value of all traffic types other than best effort to exceed 75%. If that occurs, lower the percentage value.
Use LLQ (Low Latency Queuing) check box	Select this check box to use LLQ for this traffic class.

Policing for Outbound Traffic Page

Use the Policing for Outbound Traffic page to configure policing for outbound traffic.

Policing—Traffic policing propagates bursts. When the traffic rate reaches the configured maximum rate, excess traffic is dropped or re-marked.

How to Get to This Page

1. Choose **Configure > Router > QoS**. The Quality of Service page opens with the Create QoS Policy tab selected by default.
2. Click the **Launch QoS Wizard** button to start the QoS wizard.
3. Click **Next** until you reach the Policing for Outbound Traffic page.

Related Topics

- Creating QoS Policies, page 19-3
- Create QoS Configuration Wizard, page 19-17

Field Reference

Table 19-6 Policing for Outbound Traffic Page

Element	Description
QoS Group Name	The name of the QoS group. You can either use the default group name provided by Cisco CP or enter a new group name. Cisco CP uses the value that you entered in the CIR field in the Queuing With Shaping for Outbound Traffic page, and then appends the word SHAPE to create the default group name. For example, if you entered the CIR value of 768k, Cisco CP uses that value and names the group SHAPE_768k. **Note** This field is displayed when you are creating a QoS policy on a DMVPN hub tunnel interface. **Note** This field is displayed on routers that are running the Cisco IOS Release 12.4(22)T and later advanced security images.
Policing for Outbound Traffic Pane	
Configure policing for outbound traffic radio button	Click this radio button if you want the QoS policy to include policing for outbound traffic. Then enter the values in the configuration fields. Otherwise, click **Next** to proceed to the next screen. Policing causes packets that exceed the CIR to be dropped.
Traffic Class	The traffic classes included in the QoS policy. The traffic classes are: Voice, Call Signalling, Routing, Management, Transactional, and Best Effort.

Table 19-6 Policing for Outbound Traffic Page (continued)

Element	Description
Committed Information Rate (CIR)	The CIR for each traffic class. Use these fields to allocate the bandwidth to the different types of traffic carried on the selected interface. The percentage value that you enter represents 1000 Kbps. For example, if you enter 5%, a bandwidth of 5000 Kbps is allocated. The total percentage value for all types of traffic excluding Best Effort cannot exceed 75%. The default values are: • Voice—Voice traffic. The default value is 33 percent of the bandwidth. • Call Signalling—Signalling needed to control voice traffic. The default value is 5 percent of the bandwidth. • Routing—Traffic generated by this and other routers to manage the routing of packets. The default value is 5 percent of the bandwidth. • Management—Telnet, SSH, and other traffic generated to manage the router. The default value is 5 percent of the bandwidth. • Transactional—Examples would be traffic generated for retail applications, or database updates. The default value is 5 percent of the bandwidth. • Best Effort—Remaining bandwidth for other traffic, such as e-mail traffic. The default value is 47 percent of the bandwidth. The value of Best Effort is dynamically updated based on the total percentage for the other types of traffic. Cisco CP displays a message if any entered value causes the total to exceed the link bandwidth.
Next button	Click this button to open the QoS Configuration Summary page.
Back button	Click this button to go back to the previous wizard page.

Bandwidth Allocation Dialog Box

Use this window to allocate the bandwidth to the different types of traffic carried on the chosen interface. The percentage value that you enter represents 1000 Kbps. For example, if you enter 5%, a bandwidth of 5000 Kbps is allocated. The total percentage value for all types of traffic excluding Best Effort cannot exceed 75%.

Field Reference

Table 19-7 QoS Policy Generation Dialog Box

Element	Description
Voice	Voice traffic. The default value is 33 percent of the bandwidth.
Call Signalling	Signalling needed to control voice traffic. The default value is 5 percent of the bandwidth
Routing	Traffic generated by this and other routers to manage the routing of packets. The default value is 5 percent of the bandwidth.
Management	Telnet, SSH and other traffic generated to manage the router. The default value is 5 percent of the bandwidth.
Transactional	Examples would be traffic generated for retail applications, or database updates. The default value is 5 percent of the bandwidth.
Best Effort	Remaining bandwidth for other traffic, such as e-mail traffic. The default value is 47 percent of the bandwidth. The value of Best Effort is dynamically updated based on the total percentage for the other types of traffic.

QoS Configuration Summary Page

The QoS Configuration Summary page displays a summary of the QoS policy that is created based on your choices in the wizard.

For WAN interface configuration (including DMVPN hub tunnel interface)—Each class that the Cisco CP QoS wizard configures is summarized.

For DMVPN spoke interface configuration—The NHRP group name is displayed.

Review the configuration. If you need to make changes, click the **Back** button to return to the page; otherwise, click **Finish**.

How to Get to This Page

1. Choose **Configure > Router > QoS**. The Quality of Service page opens with the Create QoS Policy tab selected by default.
2. Click the **Launch QoS Wizard** button to start the QoS wizard.
3. Configure the policy and then click **Next** until you reach the QoS Configuration Summary page.

Related Topics

- Creating QoS Policies, page 19-3
- Create QoS Configuration Wizard, page 19-17

Edit QoS Policy Reference

This section describes the pages and dialog boxes that you can use when working with the Edit QoS Policy page and includes the following topics:

- Edit QoS Policy Page, page 19-31
- Add Class for the New Service Policy Dialog Box, page 19-37
- Add Service Policy to Class Dialog Box, page 19-38
- Associate a Policy Map to Interface Dialog Box, page 19-39
- Add or Edit a QoS Class Dialog Box, page 19-40
- Edit Match DSCP Values Dialog Box, page 19-42
- Edit Match Protocol Values Dialog Box, page 19-43
- Add Custom Protocols Dialog Box, page 19-44
- Edit Match ACL Dialog Box, page 19-45
- Configure Policing Dialog Box, page 19-46
- Configure Shaping Dialog Box, page 19-48
- Configure Queuing Dialog Box, page 19-49
- Policies Associated Details Dialog Box, page 19-51
- Configure QoS Group Name Dialog Box—Appears for DMVPN Spoke Tunnel Interface, page 19-51

- Add or Edit QoS Group Name Dialog Box—Appears for DMVPN Hub Tunnel Interface, page 19-52

Edit QoS Policy Page

Use the Edit QoS Policy page to view and change configured QoS policies and to associate policies with router interfaces.

To get to this help page, choose **Configure > Router > QoS**. The Quality of Service page opens. Then click the **Edit QoS Policy** tab.

This help topic contains separate sections for different parts of the page. To view the information for a section, click the section heading.

Policy Selection Area Field Reference

Table 19-8 Edit QoS Policy Page—Policy Selection Area

Element	Description
View Policy on Interface	Choose the interface whose QoS policies you want to view.
In Direction	Choose the traffic direction on which the policy that you want to view is applied.
Go	To view the policy for the interface and traffic direction that you chose, click **Go**.
Associate	To change the association of a QoS policy with an interface, click **Associate**. If the policy is currently associated with an interface, you can disassociate the policy or change the traffic direction that the policy is applied to. The Associate button is disabled when a Frame Relay serial interface is displayed in the View Policy on Interface field. **Note** For DMVPN hub tunnel interfaces—You can associate service policies only that have shaping parameters configured on them; otherwise, you will see an error message. **Note** For DMVPN hub tunnel interfaces——You can associate policy only on the outbound traffic. If you try to associate a policy with the inbound traffic, you will see a warning message.

Table 19-8 Edit QoS Policy Page—Policy Selection Area (continued)

Element	Description
Policy Name	This field displays the name of the policy associated with the interface.
QoS Group Name	The name of the QoS group. **Note** This field is displayed when you choose to edit a class that is associated with the DMVPN hub tunnel interface. Cisco CP uses the value that you entered in the CIR field in the Queuing With Shaping for Outbound Traffic page, and then appends the word SHAPE to create the default group name. For example, if you entered the CIR value of 768k, Cisco CP uses that value and names the group SHAPE_768k. To change this group name, click the **Edit QoS Group Name** button located next to the group name.
Edit QoS Group Name button	Click this button to open the Edit QoS Group Name dialog box, in which you can change the name of the QoS group. See Add or Edit QoS Group Name Dialog Box—Appears for DMVPN Hub Tunnel Interface, page 19-52. **Note** This button is displayed when you choose to edit a class from a DMVPN hub tunnel interface.
Show Policies button	Click this button to view the QoS policies that are associated with the group name on the chosen tunnel interface. The Edit QoS policy page displays one policy at a time, which you can edit. To view all the policies associated with the tunnel interface, click the **Show Policies** button. **Note** This button is displayed when you choose to edit a class from a DMVPN hub tunnel interface.

QoS Class Buttons Area Field Reference

Note The following QoS class buttons are not displayed if you choose to edit a class for a DMVPN spoke tunnel interface.

Table 19-9 Edit QoS Policy Page—QoS Buttons

Element	Description
Add	To add a QoS class to the policy, click **Add**.
Edit	To edit a QoS class in this screen, choose the class and click **Edit**. The Edit button is disabled when a read-only QoS class is selected.
Delete	To remove a QoS class from this policy, select a class and click **Delete**. The Delete button is disabled when a read-only QoS class is selected.
Cut	To remove a class from its current position in the list, select the class and click **Cut**. Use the Paste button to place the class in the position that you want. The Cut button is disabled when a read-only QoS class is selected.
Copy	To copy class information, select the class and click **Copy**. The Copy button is disabled when a read-only QoS class is selected.
Paste	To edit copied class information and provide a new name for the class, click **Paste**. If you choose **Add this class to the policy**, the class will be placed with the enabled polices in the class. The Paste button is disabled when a read-only QoS class is selected.
Move Up	To move a class up the class list, choose a class and click **Move Up**. This button can only be used to move enabled classes. The Move Up button is disabled when a read-only QoS class is selected.
Move Down	To move a class down the class list, choose a class and click **Move Down**. This button can only be used to move enabled classes. The Move Down button is disabled when a read-only QoS class is selected.

Table 19-9 Edit QoS Policy Page—QoS Buttons (continued)

Element	Description
Add Service Policy	To add a service policy, select an existing class from the policy, click **Add Service Policy**, and then choose whether to add a new service policy or to use an existing policy. See Add Class for the New Service Policy Dialog Box, page 19-37 and Add Service Policy to Class Dialog Box, page 19-38. The Add Service Policy button is enabled when: • QoS policy is configured with Shaping value. • If you choose to add a service policy to a default class.
Remove Service Policy	To remove a service policy, choose the top-level class-default entry, and then click **Remove Service Policy**. The Remove Service Policy button is enabled when: • QoS policy is configured with Shaping value. • If you choose to add a service policy to a default class.

Class List Display Area Field Reference

Note The following class information is not displayed if you choose to edit a class from for a DMVPN spoke tunnel interface.

Table 19-10 Edit QoS Policy Page—Class List Display Area

Element	Description
	If this icon appears next to the QoS class, it is read-only, and it cannot be edited, deleted, or moved to another position in the class list.
Class Name	The name of the QoS class. Cisco CP predefines names for QoS classes.

Table 19-10 Edit QoS Policy Page—Class List Display Area (continued)

Element	Description
Match	Whether the QoS class looks for matches to Any or to All of the selected DSCP values. If you choose Any, traffic must meet only one of the match criteria. If you choose All, traffic must meet all of the match criteria. The DSCP values chosen are displayed in the DSCP column.
Classification	This portion of the display contains the following columns: • DSCP—The DSCP values that are chosen for possible match. • Protocols—The protocols included in this QoS class. A video traffic QoS class might have protocols such as cuseeme, netshow, and vdolive. A routing traffic QoS class might have protocols such as BGP, EIGRP, and OSPF. • ACL—The name or number of an ACL that specifies the traffic that this QoS class applies to.
Action	This portion of the display contains the following columns: • Queuing—This column lists the queuing type, Class Based Weighted Fair Queuing (CBWFQ), Low Latency Queuing (LLQ), or Fair Queuing, and displays the bandwidth allocated to the class. • Shaping—This column displays Yes if shaping is configured for this policy, or No if shaping is not configured. • Policing—This column displays Yes if policing is configured for this policy, or No if policing is not configured. • Set DSCP—The DSCP value that is given to this type of traffic by the QoS class. • Drop—The column displays Yes if this type of traffic is to be dropped, or No if it is not to be dropped.
Apply Changes button	Changes that you make in this window are not immediately delivered to the router. To deliver changes that you make, click **Apply Changes**. The Deliver Configuration to Router page opens. Click **Deliver**. The Commands Delivery Status window opens. Click **OK** to send the configuration to the router.

Table 19-10 Edit QoS Policy Page—Class List Display Area (continued)

Element	Description
Discard Changes button	If you do not want the changes that you have made in this window to be sent to the router, click **Discard Changes**.

QoS Group Name Display Area Field Reference—Appears for DMVPN Spoke Tunnel Interface

Note The following information is displayed if you choose to edit a DMVPN spoke tunnel interface only. This information is displayed if you provided the QoS group name in the QoS configuration wizard. See QoS Group Name Page—Appears for DMVPN Spoke Tunnel Interface, page 19-20.

Table 19-11 Edit QoS Policy Page—QoS Group Name Display Area

Element	Description
QoS Group Name	The name of the QoS group, which you can edit.

Related Topics

- Editing QoS Policies, page 19-7
- Associate a Policy Map to Interface Dialog Box, page 19-39
- Add or Edit a QoS Class Dialog Box, page 19-40
- Edit Match DSCP Values Dialog Box, page 19-42
- Edit Match Protocol Values Dialog Box, page 19-43
- Edit Match ACL Dialog Box, page 19-45
- Policies Associated Details Dialog Box, page 19-51
- Configure QoS Group Name Dialog Box—Appears for DMVPN Spoke Tunnel Interface, page 19-51
- Add or Edit QoS Group Name Dialog Box—Appears for DMVPN Hub Tunnel Interface, page 19-52

Add Class for the New Service Policy Dialog Box

Use the Add Class for the New Service Policy dialog box to add a traffic class for a new QoS policy.

Note The Add Service Policy and the Remove Service Policy buttons are enabled when:

- QoS policy is configured with Shaping value.
- If you choose to add a service policy to a default class.

How to Get to This Dialog Box

1. Choose **Configure > Router > QoS**. The Quality of Service page opens.
2. Click the **Edit QoS Policy** tab.
3. Click the **Add Service Policy** button. Then choose **Add New** from the drop-down list.

Related Topics

- Editing QoS Policies, page 19-7.
- Edit QoS Policy Page, page 19-31

Field Reference

Table 19-12 Add Class for New Policy Dialog Box

Element	Description
Policy Map Name	Enter a name for the QoS Policy.
Class Map Name	Enter a name for the traffic class.
Classification	

Table 19-12 Add Class for New Policy Dialog Box (continued)

Element	Description
Match	Specify whether the QoS class is to look for matches to Any or to All of the selected criteria. If you choose Any, traffic must meet only one of the match criteria. If you choose All, traffic must meet all of the match criteria. The DSCP values chosen are displayed in the DSCP column. • Any—Click **Any** to specify that traffic must meet only one of the criteria specified in the classification list that you create. • All—Click **All** to specify that traffic must meet all the criteria specified in the classification list that you create.
Name	This column displays the types of criteria that you can include in this traffic class. If the QoS policy uses NBAR protocol discovery, you can specify protocol and ACL values. If the QoS policy uses DSCP marking, you can specify DSCP values as well as protocol and ACL values.
Value	This column displays the values configured for the particular type, separated by commas. For example, the Protocol row might show the following values: `http, edonkey, dhcp`
Edit	To add or edit the values for a particular type of entry, select the type, and click **Edit**. Then, add or modify entries for type in the displayed dialog.

Add Service Policy to Class Dialog Box

Use the Add Service Policy dialog box to add an existing service policy to a QoS class.

Note The Add Service Policy and the Remove Service Policy buttons are enabled when:

- QoS policy is configured with Shaping value.
- If you choose to add a service policy to a default class.

How to Get to This Dialog Box

1. Choose **Configure > Router > QoS**. The Quality of Service page opens.
2. Click the **Edit QoS Policy** tab.
3. Click the **Add Service Policy** button. Then choose **Add Existing** from the drop-down list.

Field Reference

Table 19-13 Add Service Policy to Class Dialog Box

Element	Description
Existing service policy	Select an existing service policy from the list.

Associate a Policy Map to Interface Dialog Box

See Associate a Policy Map to Interface, page 43-3.

Associate or Disassociate the QoS Policy Dialog Box

Use the Associate or Disassociate the QoS Policy dialog box to change the associations that a QoS policy has to router interfaces and traffic directions.

Field Reference

Table 19-14 Associate or Disassociate QoS Policy Dialog Box

Element	Description
Interface	This column lists the router interfaces. To choose an interface to which you want to associate the QoS policy, check the box next to the interface name. **Note** If you choose the interface that Cisco CP uses to communicate with the router, the connection between Cisco CP and the router might be lost.

Table 19-14 Associate or Disassociate QoS Policy Dialog Box

Element	Description
Inbound	To associate the QoS policy to inbound traffic on the chosen interface, check the box in this column.
Outbound	To associate the QoS policy to outbound traffic on the chosen interface, check the box in this column.

Add or Edit a QoS Class Dialog Box

Use the Add or Edit a QoS class dialog box to create or edit QoS traffic classes and to specify whether the class is to be added to the QoS policy.

How to Get to This Dialog Box

1. Choose **Configure > Router > QoS**. The Quality of Service page opens.
2. Click the **Edit QoS Policy** tab, and then click **Add** or **Edit** as appropriate.

Related Topics

- Adding a QoS Class, page 19-10
- Editing the QoS Class Information, page 19-11

Field Reference

Table 19-15 Add or Edit a QoS Class Dialog Box

Element	Description
Add this class to the policy	To include this QoS class in QoS policy, check **Add this class to the policy**. If this option is not checked, and then the selected QoS class is marked as Disabled in the Edit QoS Policy window. **Note** You can configure QoS policies on an interface in the create mode (by using the QoS wizard) or in the edit mode. The Add This Class to the Policy field appears when a QoS policy is not associated with an interface.
Class Name	The QoS class name is displayed in this field if you are editing an existing class. You must enter a class name if you are adding a new class to a policy or pasting information from a QoS class that you have copied.
Class Default	This option appears when there is no class-default in the QoS policy. To add class-default—the default class—instead of creating a new class, click **Class Default**. There are several configuration parameters that you cannot set for class-default: • Classification box—You cannot specify classification criteria. • Action box—You cannot specify that traffic be dropped. Additionally, you can only specify that Fair Queuing be used.
Classification Pane	
Choose the types of items and values that you want the router to examine traffic for.	
Match	Includes two radio buttons: • All—Click to indicate that traffic must meet all criteria. • Any—Click to indicate that traffic need only meet one criteria.
DSCP	To specify that the traffic must contain specific DSCP markings, select **DSCP**, and click **Edit**. Then choose the DSCP markings in the displayed dialog. See Edit Match DSCP Values Dialog Box, page 19-42.
Protocol	To specify that the traffic must contain specific protocols, select **Protocol**, and click **Edit**. Then choose the protocols in the displayed dialog. See Edit Match Protocol Values Dialog Box, page 19-43.

Table 19-15 Add or Edit a QoS Class Dialog Box (continued)

Element	Description
Access Rule	To specify that the class must match traffic defined in an ACL, select **Access Rule**, and then click **Edit**. In the dialog that appears, choose an existing ACL, create a new one, or clear existing associations if you are editing a QoS class. See Edit Match ACL Dialog Box, page 19-45.
Action Pane	
Choose the action that the router is to take when it finds traffic that matches the specified DSCP values.	
Drop	To have the router drop the traffic, check **Drop**. If you check Drop, other options in the Action area are disabled.
Set DSCP	To have the router reset DSCP value for the traffic, check **Set DSCP** and choose the value that you want the traffic to be reset to.
Queuing	To configure queuing for this traffic class, check **Queuing** and then click **Configure Queuing**. Then configure traffic queuing in the displayed dialog. LLQ is available if the traffic uses the RTP protocol or has a DSCP value of EF. If the traffic does not have these attributes, the LLQ option is not available. If you are adding or editing the default class—class-default—only Fair Queuing is available. See Configure Queuing Dialog Box, page 19-49.
Shaping	To configure shaping for this traffic, check **Shaping** and then click **Configure Shaping** to display the shaping dialog and make settings. See Configure Shaping Dialog Box, page 19-48.
Policing	To configure policing for this traffic, check **Policing** and then click **Configure Policing** to display the policing dialog and make settings. See Configure Policing Dialog Box, page 19-46.

Edit Match DSCP Values Dialog Box

Use the Edit Match DCSP Values dialog box to edit the DSCP value for a QoS policy.

How to Get to This Dialog Box

1. Choose **Configure > Router > QoS**. The Quality of Service page opens.

2. Click the **Edit QoS Policy** tab, and then click **Add** or **Edit** as appropriate.
3. Choose **DSCP**, and then click **Edit.**

Related Topics

- Add or Edit a QoS Class Dialog Box
- Editing DSCP, Protocols, and ACL Classification Values, page 19-13

Field Reference

Table 19-16 Edit Match DSCP Value Dialog Box

Element	Description
Available DSCP Values	List of available DSCP values that you can choose.
>> >> button << << button	Click the >> >> button to add the chosen value from the Available DSCP Values area to the Selected DSCP Values area. Click the << << button to remove the chosen value from the Selected DSCP Values area and move it to the Available DSCP Values area.
Selected DSCP Values	Lists the DSCP values that you selected from the Available DSCP Values area.

Edit Match Protocol Values Dialog Box

Use the Edit Match Protocol Values dialog box to edit the protocol value for a QoS policy.

How to Get to This Dialog Box

1. Choose **Configure > Router > QoS**. The Quality of Service page opens.
2. Click the **Edit QoS Policy** tab, and then click **Add** or **Edit** as appropriate.
3. Choose **Protocol**, and then click **Edit.**

Related Topics

- Add or Edit a QoS Class Dialog Box
- Editing DSCP, Protocols, and ACL Classification Values, page 19-13
- Adding Custom Protocols, page 19-14

Field Reference

Table 19-17 Edit Match Protocol Value Dialog Box

Element	Description
Available Protocol Values	List of available protocol values that you can choose.
>> >> button << << button	Click the **>> >>** button to add the chosen value from the Available Protocol Values area to the Selected Protocol Values area. Click the << << button to remove the chosen value from the Selected Protocol Values area and move it to the Available Protocol Values area.
Selected Protocol Values	Lists the Protocol values that you selected from the Available Protocol Values area.
Add Custom Protocols button	Click this button to add custom protocols that are not available in the Available Match Protocol Values area. See Add Custom Protocols Dialog Box, page 19-44.

Add Custom Protocols Dialog Box

Use the Add Custom Protocols dialog box to add custom protocols that are not available in the Edit Match Protocol Values dialog box.

How to Get to This Dialog Box

1. Choose **Configure > Router > QoS**. The Quality of Service page opens.
2. Click the **Edit QoS Policy** tab, and then click **Add** or **Edit** as appropriate.
3. Choose **Protocol**, and then click **Edit.**

Related Topics

- Add or Edit a QoS Class Dialog Box, page 19-40
- Edit Match Protocol Values Dialog Box, page 19-43
- Adding Custom Protocols, page 19-14

Field Reference

Table 19-18 Add Custom Protocols Dialog Box

Element	Description
Name	Choose the name of the custom protocol from the drop-down list.
Protocol	Select the appropriate radio button. Options are TCP and UDP.
New Port Number	The port numbers that this protocol should use. Valid port number range is 1 to 65535.
Add >> button	Click this button to add the new port number that you entered to the Port Number(s) area.
Port Number(s)	Lists the port numbers that you added in the New Port Number field.

Edit Match ACL Dialog Box

Use the Edit Match ACL dialog box to edit the access rule for a QoS policy.

How to Get to This Dialog Box

1. Choose **Configure > Router > QoS**. The Quality of Service page opens.
2. Click the **Edit QoS Policy** tab, and then click **Add** or **Edit** as appropriate.
3. Choose **Access Rule**, and then click **Edit.**

Related Topics

- Add or Edit a QoS Class Dialog Box
- Editing DSCP, Protocols, and ACL Classification Values, page 19-13

Field Reference

Table 19-19 Edit Match ACL Dialog Box

Element	Description
Access Rule	List of available protocol values that you can choose.
... button	Click this button, and then choose one of these options: • Select an existing rule (ACL)—Choose to select an existing rule. When clicked, opens the Select a Rule dialog box. See Select a Rule, page 15-17. • Create a new rule (ACL) and select—Choose to add a new rule. When clicked, opens the Add a Rule dialog box. See Add or Edit a Rule, page 15-7. • None (clear associations)—Choose to clear existing rule associations.

Configure Policing Dialog Box

Use the Configure Policing dialog box to configure policing for a QoS policy.

How to Get to This Dialog Box

1. Choose **Configure > Router > QoS**. The Quality of Service page opens.
2. Click the **Edit QoS Policy** tab, and then click **Add** or **Edit** as appropriate.
3. Check **Policing**, and then click **Configure Policing**.

Related Topics

- Add or Edit a QoS Class Dialog Box
- Editing Queuing, Policing, and Shaping Action Parameters, page 19-15

Field Reference

Table 19-20 Configure Policing Dialog Box

Element	Description
Specify the access rate parameters for policing	
Committed Information Rate (CIR)	Enter the CIR to be used for the policy in kilobits per second. When the traffic rate reaches the CIR, excess traffic is dropped or remarked.
Normal Burst Size (BC)	Optional. Enter the normal burst size in kilobits per second. The normal burst size determines how large traffic bursts can be before some traffic exceeds the CIR.
Excess Burst Size (BE)	Optional. Enter the excess burst size in kilobits per second. The excess burst size determines how large traffic bursts can be before all traffic exceeds the rate limit. Traffic that falls between the normal burst size and the excess burst size exceeds the rate limit with a probability that increases as the burst size increases.
Action Type	This column lists the names of the actions that you can choose for traffic that conforms to, exceeds, or violates the configured CIR, BC, and BE parameters.

Table 19-20 Configure Policing Dialog Box (continued)

Element	Description
Action	Choose what you want the router to do when traffic conditions conform, exceed or violate configured policing parameters. The conform and the exceed actions are mandatory and have default values. The violate action is optional. The available actions are the following: • Drop—(Default for exceed action) Discard the packet. • None—(Available for violate action) • Set DSCP Transmit—Set the DSCP and transmit. • Transmit—(Default for conform action) Send the packet. • Unsupported—Cisco CP adds and selects this option in the following cases: – If Cisco CP detects that actions other than transmit, drop, or set DSCP transmit have been configured. Actions other than those are not supported. – If Cisco CP detects that more than one action has been configured for the same action type. When Cisco CP encounters either of these configurations, Unsupported is the only available action, and Cisco CP displays a tooltip popup indicating that an unsupported policing action has been configured.
DSCP Values	Options in this column are enabled when you choose the Set DSCP Transmit action. The options displayed are the available DSCP markings.

Configure Shaping Dialog Box

Use the Configure Shaping dialog box to configure shaping for a QoS policy.

How to Get to This Dialog Box

1. Choose **Configure > Router > QoS**. The Quality of Service page opens.
2. Click the **Edit QoS Policy** tab, and then click **Add** or **Edit** as appropriate.

3. Check **Shaping**, and then click **Configure Shaping**.

Related Topics

- Add or Edit a QoS Class Dialog Box
- Editing Queuing, Policing, and Shaping Action Parameters, page 19-15

Field Reference

Table 19-21 Configure Shaping Dialog Box

Element	Description
Committed Information Rate (CIR)	Enter the CIR to be used for the policy in kilobits per second. When the traffic rate reaches the CIR, excess traffic is dropped or remarked.
Normal Burst Size (BC)	Optional. Enter the normal burst size in kilobits per second. The normal burst size determines how large traffic bursts can be before some traffic exceeds the CIR.
Excess Burst Size (BE)	Optional. Enter the excess burst size in kilobits per second. The excess burst size determines how large traffic bursts can be before all traffic exceeds the rate limit. Traffic that falls between the normal burst size and the excess burst size exceeds the rate limit with a probability that increases as the burst size increases.

Configure Queuing Dialog Box

Use the Configure Queuing dialog box to configure queuing for a QoS policy. The fields displayed change based on the queuing method you choose. You can choose the following queuing methods:

- LLQ— Low Latency Queuing
- CBWFQ—Class-Based Weighted Fair Queuing
- Fair Queue—Weighted Fair Queuing (WFQ)

How to Get to This Dialog Box

1. Choose **Configure > Router > QoS**. The Quality of Service page opens.
2. Click the **Edit QoS Policy** tab, and then click **Add** or **Edit** as appropriate.
3. Check **Queuing**, and then click **Configure Queuing**.

Related Topics

- Add or Edit a QoS Class Dialog Box
- Editing Queuing, Policing, and Shaping Action Parameters, page 19-15

Field Reference

Table 19-22 Configure Queuing Dialog Box

Element	Description
LLQ Chosen	
Priority Percentage	Bandwidth is allocated as an absolute percentage of the total bandwidth of the interface or tunnel. Enter a percentage value from 1 to 100 to specify the amount of bandwidth that you want to use.
CBWFQ Chosen	
Bandwidth	Enter a percentage value from 1 to 100 to specify the amount of bandwidth that you want to use. Bandwidth is allocated as an absolute percentage of the total bandwidth of the interface or tunnel.
Bandwidth Remaining	Enter a percentage value from 1 to 100 to specify the amount of available bandwidth that you want to use for this traffic class. Bandwidth is allocated as a relative percentage of the total bandwidth available on the interface. You can specify that 30 percent of the available bandwidth be allocated to one class, and 60 percent of the bandwidth be allocated to another QoS class. To use this option, all other classes must use this option.
Random Detect	To enable Weighted Random Early Detection (WRED) and Distributed WRED (DWRED), click **Random Detect**. WRED drops packets during periods of high congestion, thus telling the source host to decrease the transmission rate.
Fair Queue Chosen	
Random Detect	To enable WRED and DWRED, click **Random Detect**. WRED drops packets during periods of high congestion, thus telling the source host to decrease the transmission rate.

Policies Associated Details Dialog Box

Use the Policies Associated Details dialog box to view the QoS policies that are associated with the group name on a selected tunnel interface.

The Edit QoS policy page displays one policy at a time. To view all the policies associated with the tunnel interface, click the **Show Policies** button.

How to Get to This Dialog Box

1. Choose **Configure > Router > QoS**. The Quality of Service page opens.
2. Click the **Edit QoS Policy** tab, and then click the **Show Policies** button.

Related Topics

- Edit QoS Policy Page
- Editing QoS Policies

Field Reference

Table 19-23 Policies Associated Details Dialog Box

Element	Description
QoS Group Name	The group name of the QoS policy.
Policy Name	The name of the policy associated with the group name.

Configure QoS Group Name Dialog Box—Appears for DMVPN Spoke Tunnel Interface

Use the Configure QoS Group Name dialog box to provide the group name of the DMVPN hub tunnel interface.

Note This page is displayed for spoke tunnel interfaces in the following scenario: You configured QoS policies on a spoke tunnel interface using the QoS configuration wizard pages and did not provide the group name at that time. Later, when you try to edit the spoke tunnel interface, the Configure QoS Group Name page is displayed, where you can enter the QoS group name.

How to Get to This Dialog Box

1. Choose **Configure > Router > QoS**. The Quality of Service page opens.
2. Choose a DMVPN spoke tunnel interface to edit.
3. Click the **Edit QoS Policy** tab.

Related Topics

- Editing QoS Policies, page 19-7
- Edit QoS Policy Page, page 19-31
- QoS Group Name Page—Appears for DMVPN Spoke Tunnel Interface, page 19-20

Field Reference

Table 19-24 Configure QoS Group Name Dialog Box

Element	Description
Yes radio button	Choose this radio button if you know the group name that is configured for the DMVPN hub tunnel interface. Then enter the group name in the QoS Group Name field.
No radio button	Choose this radio button if you do not know the group name that is configured for the DMVPN hub tunnel interface.
QoS Group Name	The group name configured for the DMVPN hub tunnel interface. This field is enabled when you choose the Yes radio button. Make sure that the group name you enter in this field matches with the group name that is configured for the DMVPN hub tunnel interface.

Add or Edit QoS Group Name Dialog Box—Appears for DMVPN Hub Tunnel Interface

Use the Edit QoS Group Name dialog box to add or change the group name for a policy in a DMVPN hub tunnel interface.

How to Get to This Dialog Box

This dialog box appears in two scenarios:

Scenario 1

1. Choose **Configure > Router > QoS**. The Quality of Service page opens.
2. Choose a DMVPN hub tunnel interface to edit.
3. Click the **Edit QoS Policy** tab.
4. From the Policy Selection Area, click the **Edit QoS Group Name** button.

Scenario 2

1. Choose **Configure > Router > QoS**. The Quality of Service page opens.
2. Click the **Edit QoS Policy** tab.
3. From the Policy Selection Area, choose the DMVPN hub tunnel interface that does not have QoS policies associated with it.
4. From the In Direction field, choose **Outbound**, and then click the **Go** button.

Note If no QoS policies are associated with the DMVPN hub tunnel interface, the Add button is enabled and the Policy Name displays the No Policy Available status.

5. Choose **Add**. The Add a QoS Class page opens.
6. In the The Add a QoS Class page, enter the QoS class name, the classification parameters, and the action that the router must take when it finds traffic that matches the specified values, and the click **OK**. The Enter QoS Group Name dialog box opens where you can enter the QoS group name.

Related Topics

- Editing QoS Policies, page 19-7
- Edit QoS Policy Page, page 19-31
- Add or Edit a QoS Class Dialog Box, page 19-40

Field Reference

Table 19-25 Enter or Edit QoS Group Name Dialog Box

Element	Description
QoS Group Name	The name of the QoS group. Use this field to either add a new group name or to edit an existing group name. Make sure that you provide a unique group name. If you provide an existing group name, you will see a warning message.

CHAPTER 20

Router Provisioning

You can provision your router using a USB device attached directly to your router, or using Secure Device Provisioning (SDP). SDP must be supported by your Cisco IOS release to be available in Cisco CP.

Secure Device Provisioning

This window allows you to use Secure Device Provisioning (SDP) to complete tasks such as enrolling your router with a CA server and configuring your router. Click the **Launch SDP** button to transfer to the SDP web-browser application to complete the process.

If you are obtaining certificates, Cisco CP displays the Certificates window where you can view the certificates after they are obtained from the CA.

To learn what you need to do to prepare for SDP enrollment, see SDP Troubleshooting Tips.

For more information on SDP, click the following link:

http://www.cisco.com/en/US/products/sw/iosswrel/ps5207/products_feature_guide09186a008028afbd.html#wp1043332

Note If the **Launch SDP** button is absent, you router Cisco IOS release does not support SDP. If the **Launch SDP** button is disabled, you are logged in to Cisco CP as a nonroot view user.

Router Provisioning from USB

This window tells you if Cisco CP has detected a USB token or USB flash device connected to your router. You can click the **Router Provisioning** button to choose a configuration file from the USB token or USB flash device.

If you choose to provision your router this way, the configuration file from the USB token or USB flash device is merged with your router's running configuration file to create a new running configuration file.

Router Provisioning from USB (Load File)

This window allows you to load a configuration file from a USB token or USB flash device connected to your router. The file will be merged with your router's running configuration file to create a new running configuration file.

To load a configuration file, follow these steps:

Step 1 Choose the device type from the drop-down menu.

Step 2 Enter the configuration filename in Filename, including the full path, or click **Browse** and choose the file from the File Selection window.

Step 3 If the device type is a USB token, enter the password to log in to the token in Token PIN.

Step 4 If you want to preview the file, click **Preview File** to display the contents of the file in the details pane.

Step 5 Click **OK** to load the chosen file.

SDP Troubleshooting Tips

Use this information before enrolling using Secure Device Provisioning (SDP) to prepare the connection between the router and the certificate server. If you experience problems enrolling, you can review these tasks to determine where the problem is.

Guidelines

- When SDP is launched, you must minimize the browser window displaying this help topic so that you can view the SDP web application.
- If you are planning to configure the router using SDP, you should do so immediately after configuring your WAN connection.
- When you complete the configuration changes in SDP, you must return to Cisco CP and click Refresh on the toolbar to view the status of the trustpoint in the Router Certificates window in the VPN Components tree.

Troubleshooting Tips

These recommendations involve preparations on the local router and on the CA server. You need to communicate these requirements to the administrator of the CA server. Ensure the following:

- The local router and the CA server have IP connectivity between each other. The local router must be able to ping the certificate server successfully, and the certificate server must be able to successfully ping the local router.
- The CA server administrator uses a web browser that supports JavaScript.
- The CA server administrator has enable privileges on the local router.
- The firewall on the local router will permit traffic to and from the certificate server.
- If a firewall is configured on the Petitioner and/or on the Registrar, you must ensure that the Firewall permits HTTP or HTTPS traffic from the PC from which the Cisco CP /SDP application is invoked.

For more information about SDP, see the following web page:

http://www.cisco.com/en/US/products/sw/iosswrel/ps5207/products_feature_guide09186a008028afbd.html#wp1043332

CHAPTER 21

Performance Routing

For information about how to use Cisco Configuration Professional (Cisco CP) to configure the Performance Routing feature, see the screencast at: http://www.cisco.com/en/US/docs/net_mgmt/cisco_configuration_professional/scrcst/ccpsc.html.

Note You must have internet access to view the screencast.

PART 4

Configuring Security Features

This section provides information about how to configure security features on the router.

CHAPTER 22

Create Firewall

A firewall is a set of rules used to protect the resources of your LAN. These rules filter the packets arriving at the router. If a packet does not meet the criteria specified in the rule, it is dropped. If it does meet the criteria, it is allowed to pass through the interface that the rule is applied to. This wizard enables you to create a firewall for your LAN by answering prompts in a set of screens.

In this window, select the type of firewall that you want to create.

Note

- The router that you are configuring must be using a Cisco IOS image that supports the Firewall feature set in order for you to be able to use Cisco Configuration Professional (Cisco CP) to configure a firewall on the router.
- The LAN and WAN configurations must be complete before you can configure a firewall.

Basic Firewall

Click this if you want Cisco CP to create a firewall using default rules. The use case scenario shows a typical network configuration in which this kind of firewall is used.

Advanced Firewall

Click this if you want Cisco CP to lead you through the steps of configuring a firewall. You have the option to create a Demilitarized Zone (DMZ) network, and to specify an inspection rule. The use case scenario shown when you select this option shows you a typical configuration for an Internet of firewall.

Switch to Classic Firewall

Click this link if you want to use the older Classic Firewall.

What Do You Want to Do?

If you want to:	Do this:
Have Cisco CP create a firewall for me. You might want to select this option if you do not want to configure a DMZ network, or if there is only one outside interface.	Click **Basic Firewall**. Then, click **Launch the Selected Task**. Cisco CP asks you to identify the interfaces on your router, and then it uses Cisco CP default access rules and inspection rules to create the firewall.
Have Cisco CP help me create an Advanced Firewall. If your router has multiple inside and outside interfaces, and you want to configure a DMZ, you should select this option.	Click **Advanced Firewall**. Then, click **Launch the Selected Task**. Cisco CP will show you the default inspection rule and allow you to use it in the firewall. Or, you can create your own inspection rule. Cisco CP will use a default access rule in the firewall

If you want to:	Do this:
Have Cisco CP switch to Classic Firewall.	Click **Switch to Classic Firewall**. Cisco CP displays a warning message if Zone Based Firewall is configured on the router and asks you to delete the existing Zone Based Firewall policies to switch to Classic Firewall. If Zone Based Firewall is not configured, Cisco CP displays a warning message informing you that Zone Based Firewall is the new form of configuring firewall with zones and policies and that Classic Firewall does not support category based Content Filtering. Click **Yes** to switch to Classic Firewall. The Create Firewall, Edit Firewall Policy/ACL, and Application Security tabs are displayed.

If you want to:	Do this:
Get information about a task that this wizard does not help me complete.	Select a topic from the following list: • How Do I View Activity on My Firewall? • How Do I Configure a Firewall on an Unsupported Interface? • How Do I Configure a Firewall After I Have Configured a VPN? • How Do I Permit Specific Traffic Through a DMZ Interface? • How Do I Modify an Existing Firewall to Permit Traffic from a New Network or Host? • How Do I Configure NAT on an Unsupported Interface? • How Do I Configure NAT Passthrough for a Firewall? • How Do I Permit Traffic Through a Firewall to My Easy VPN Concentrator? • How Do I Associate a Rule with an Interface? • How Do I Disassociate an Access Rule from an Interface • How Do I Delete a Rule That Is Associated with an Interface? • How Do I Create an Access Rule for a Java List? • How Do I View the IOS Commands I Am Sending to the Router? • How Do I Permit Specific Traffic onto My Network if I Don't Have a DMZ Network?

Basic Firewall Configuration Wizard

Cisco CP will protect the LAN with a default firewall when you select this option. For Cisco CP to do this, you must specify the inside and outside interfaces in the next window. Click **Next** to begin configuration.

Basic Firewall Interface Configuration

Identify the interfaces on the router so that the firewall will be applied to the correct interface.

Outside (untrusted) Interface

Select the router interface that is connected to the Internet or to your organization's WAN.

Note Do not select the interface through which you accessed Cisco CP as the outside (untrusted) interface. Doing so will cause you to lose your connection to Cisco CP. Because it will be protected by a firewall, you will not be able to launch Cisco CP from the outside (untrusted) interface after the Firewall Wizard completes.

Allow secure Cisco CP access from outside interfaces check box

Check this box if you want users outside the firewall to be able to access the router using Cisco CP. The wizard will display a screen that allows you to specify a host IP address or a network address. The firewall will be modified to allow access to the address you specify. If you specify a network address, all hosts on that network will be allowed through the firewall.

Inside (trusted) Interfaces

Check the physical and logical interfaces connecting to the LAN. You can select multiple interfaces.

Configuring Firewall for Remote Access

Creating a firewall can block access to the router that remote administrators may need. You can specify the router interfaces to use for remote management access and the hosts from which administrators can log on to Cisco CP to manage the router. The firewall will be modified to allow secure remote access from the host or network that you specify.

Select the outside interface

If you are using the Advanced Firewall wizard, select the interface through which users are to launch Cisco CP. This field does not appear in the Basic Firewall wizard.

Source Host/Network

If you want to allow a single host access through the firewall, choose **Host Address** and enter the IP address of a host. Choose **Network Address** and enter the address of a network and a subnet mask to allow hosts on that network access through the firewall. The host or network must be accessible from the interface that you specified. Choose **Any** to allow any host connected to the specified interfaces secure access to the network.

Advanced Firewall Configuration Wizard

Cisco CP will help you create an Internet firewall by asking you for information about the interfaces on the router, whether you want to configure a DMZ network, and what rules you want to use in the firewall.

Click **Next** to begin configuration.

Advanced Firewall Interface Configuration

Identify the router's inside and outside interfaces and the interface that connects to the DMZ network.

Check **outside** or **inside** to identify each interface as an outside or an inside interface. Outside interfaces connect to your organizations's WAN or to the Internet. Inside interfaces connect to your LAN.

Allow secure Cisco CP access from outside interfaces check box

Check this box if you want users outside the firewall to be able to access the router using Cisco CP. The wizard will display a screen that allows you to specify a host IP address or a network address. The firewall will be modified to allow access to the address you specify. If you specify a network address, all hosts on that network will be allowed through the firewall.

DMZ Interface

Select the router interface that connects to a DMZ network, if one exists. A DMZ network is a buffer zone used to isolate traffic that comes from an untrusted network. If you have a DMZ network, select the interface that connects to it.

Advanced Firewall DMZ Service Configuration

This window allows you to view rule entries that specify which services available inside the DMZ you want to make available through the router's outside interfaces. Traffic of the specified service types will be allowed through the outside interfaces into the DMZ network.

DMZ Service Configuration

This area shows the DMZ service entries configured on the router.

Start IP Address

The first IP address in the range that specifies the hosts in the DMZ network.

End IP Address

The last IP address in the range that specifies the hosts in the DMZ network. If there is no value listed in this column, the IP address in the Start IP address column is presumed to be the only host in the DMZ network. The range can specify a maximum of 254 hosts.

Service Type

The type of service, either Transmission Control Protocol (TCP) or User Datagram Protocol (UDP).

Service

The name of the service, such as Telnet, or File Transfer Protocol (FTP), or a protocol number.

To configure a DMZ service entry:

Click **Add**, and create the entry in the DMZ Service Configuration window.

To edit a DMZ service entry:

Select the service entry, and click **Edit**. Then, edit the entry in the DMZ Service Configuration window.

DMZ Service Configuration

Create or edit a DMZ service entry in this window.

Host IP Address

Enter the address range that will specify the hosts in the DMZ that this entry applies to. The firewall will allow traffic for the specified TCP or UDP service to reach these hosts.

Start IP Address

Enter the first IP address in the range; for example, 172.20.1.1. If Network Address Translation (NAT) is enabled, you must enter the NAT-translated address, known as the *inside global address*.

End IP Address

Enter the last IP address in the range; for example, 172.20.1.254. If NAT is enabled, you must enter the NAT-translated address.

Service

TCP

Click this option if you want to allow traffic for a TCP service.

UDP

Click this option if you want to allow traffic for a UDP service.

Service

Enter the service name or number in this field. If you do not know the name or number, click the button and select the service from the list displayed.

Application Security Configuration

Cisco CP provides preconfigured application security policies that you can use to protect the network. Use the slider bar to select the security level that you want and to view a description of the security it provides. The wizard summary screen displays the policy name, SDM_HIGH, SDM_MEDIUM, or SDM_LOW and the configuration statements in the policy. You can also view the details of the policy by clicking the Application Security tab and choosing the name of the policy.

Preview Commands Button

Click to view the IOS commands that make up this policy.

Custom Application Security Policy Button

This button and the Policy Name field are visible if you are completing the Advanced Firewall wizard. Choose this option if you want to create your own application security policy. If the policy already exists, enter the name in the field, or click the button on the right, choose **Select an existing policy**, and select the policy. To create a policy, click the button, choose **Create a New Policy**, and create the policy in the dialog displayed.

Domain Name Server Configuration

The router must be configured with the IP address of at least one DNS server for application security to work. Click **Enable DNS-based hostname-to-address** translation, and provide the IP address of the primary DNS server. If a secondary DNS server is available, enter it's IP address in the **Secondary DNS Server** field.

The IP addresses that you enter will be visible in the DNS Properties window under Additional Tasks.

URL Filter Server Configuration

URL filter servers are capable of storing and maintaining much more URL filtering information than a router configuration file can contain. If there are URL filter servers on the network, you can configure the router use them. You can configure additional URL filter server parameters by going to **Configure > Advanced Security > URL Filtering > URL Filter Servers**. See URL Filtering for more information.

Filter HTTP Request through URL Filter Server

Check the **Filter HTTP Request through URL Filter Server** box to enable URL filtering by URL filter servers.

URL Filter Server Type

Cisco CP supports the Secure Computing and Websense URL filter servers. Choose either **Secure Computing** or **Websense** to specify the type of URL filter server on the network.

IP Address/Hostname

Enter the IP address or the hostname of the URL filter server.

Select Interface Zone

This window appears if a router interface other than the one you are configuring is a member of a Zone-Based Policy Firewall (ZPF) security zone. For more information about this topic, see Zone-Based Policy Firewall.

Select Zone

Select the security zone that you want the interface to be a member of. If you choose not to assign the interface to a zone, there is a strong possibility that traffic will not pass through the interface.

ZPF Inside Zones

Zones that include interfaces used in generic routing encapsulation (GRE) tunnels must be designated as inside (trusted) zones in order for GRE traffic to pass through the firewall.

This window lists the configured zones and their member interfaces. To designate a zone as inside, check the **inside** (**trusted**) column in the row for that zone.

Voice Configuration

Include voice traffic in the router firewall policy by providing the necessary information in this screen.

Field Reference

Table 22-1 describes the fields in this screen.

Table 22-1 Voice Configuration Fields

Element	Description
Enable Voice Configuration	Check **Enable Voice Configuration** to enable the other fields in this screen.
Interface	The name of a router interface, for example, GigabitEthernet0/1

Table 22-1 Voice Configuration Fields

Element	Description
Outside (untrusted)	Check **Outside** (**untrusted**) next to the interface name if you are using the interface to connect to the WAN.
Inside (trusted)	Check **Inside** (**trusted**) next to the interface name if you are using the interface to connect to the LAN or other trusted network.
Select the Lineside Protocol	The lineside protocol is the protocol used when sending traffic too and from the phones on the network. Choose one of the following options: • SIP—Session Initiation Protocol. • SCCP—Skinny Client Control Protocol.
Select the ide Protocol	The ide protocol is the protocol used when sending traffic over the Internet. Choose one of the following options: • SIP—Session Initiation Protocol. • H.323
Enable logging for voice traffic	To view logging messages related to voice traffic in the monitor screens, check **Enable logging for voice traffic**. To view these messages, click **Monitor** in the Cisco CP toolbar, and then click **Firewall**.

Summary

This screen summarizes the firewall information. You can review the information in this screen and use the Back button to return to screens in the wizard to make changes.

The summary screen uses plain-language to describe the configuration.

Inside (trusted) Interface(s)

Cisco CP lists the router's logical and physical interfaces that you designated as the inside interfaces in this wizard session, along with their IP addresses. Underneath, plain-language descriptions are given for each configuration statement applied to the inside interfaces. The following are examples:

```
Inside(trusted) Interfaces:
```

```
FastEthernet0/0 (10.28.54.205)
Apply access rule to the inbound direction to deny spoofing traffic.
Apply access rule to the inbound direction to deny traffic sourced
from broadcast, local loopback address.
Apply access rule to the inbound direction to permit all other
traffic.
Apply application security policy SDM_HIGH to the inbound direction.
```

This example shows the Cisco CP Application Security policy SDM_HIGH applied to inbound traffic on this interface.

Outside (untrusted) Interface(s)

Cisco CP lists the router logical and physical interfaces that you designated as outside interfaces in this wizard session, along with their IP addresses. Underneath, plain-language descriptions are given for each configuration statement applied to the outside interfaces. The following are examples:

```
FastEthernet0/1 (142.120.12.1)
Turn on unicast reverse path forwarding check for non-tunnel
interfaces.
Apply access rule to the inbound direction to permit IPSec tunnel
traffic if necessary.
Apply access rule to the inbound direction to permit GRE tunnel
traffic for interfaces if necessary.
Apply access rule to the inbound direction to permit ICMP traffic.
Apply access rule to the inbound direction to permit NTP traffic if
necessary.
Apply access rule to the inbound direction to deny spoofing traffic.
Apply access rule to the inbound direction to deny traffic sourced
from broadcast, local loopback and private address.
Apply access rule to the inbound direction to permit service traffic
going to DMZ interface.
Service ftp at 10.10.10.1 to 10.10.10.20
Apply access rule to the inbound direction to permit secure SDM access
from 140.44.3.0 255.255.255.0 host/network
Apply access rule to the inbound direction to deny all other traffic.
```

Note that this configuration turns on reverse path forwarding, a feature that allows the router to discard packets that lack a verifiable source IP address, and permits ftp traffic to the DMZ addresses 10.10.10.1 through 10.10.10.20.

DMZ Interface

If you configured an Advanced firewall, this area shows you the DMZ interface you designated, along with its IP address. Underneath, Cisco CP describes what access and inspection rules were associated with this interface. The following are examples:

```
FastEthernet (10.10.10.1)
Apply CBAC inspection rule to the outbound direction
Apply access rule to the inbound direction to deny all other traffic.
```

To save this configuration to the router's running configuration and leave this wizard:

Click **Finish**. Cisco CP saves the configuration changes to the router's running configuration. The changes will take effect immediately, but will be lost if the router is turned off.

If you checked **Preview commands before delivering to router** in the User Preferences window, the Deliver configuration to router window appears. In this window, you can view the CLI commands you that are delivering to the router.

Cisco CP Warning: Cisco CP Access

This window appears when you have indicated that Cisco CP should be able to access the router from outside interfaces. It informs you that you must ensure that SSH and HTTPS are configured, and that at least one of the interfaces designated as outside be configured with a static IP address. To do this, you must ensure that an outside interface is configured with a static IP address, and then associate a management policy with that interface.

Determining if an Outside Interface is Configured with a Static IP Address

Complete the following steps to determine if an outside interface is configured with a static IP address.

Step 1 Click **Configure > Router > Interfaces and Connections > Edit Interface/Connection**.

Step 2 Review the IP column in the Interface list table to determine if an outside interface has a static IP addresses.

Step 3 If no outside interface has a static IP address, select one and click **Edit** to display a dialog that allows you to reconfigure the IP address information for the interface.

If there is an outside interface with a static IP address, note that interface name and complete the next procedure.

Configuring SSH and HTTPS

Complete the following steps to configure a management policy for SSH and HTTPS on the router.

Step 1 Click **Configure > Router > Router Access > Management Access**.

Step 2 If there is no management policy, click **Add**. If you want to edit an existing management policy, select the policy and click **Edit**.

Note If you are editing a management policy it must be associated with an interface that has a static IP address.

Step 3 In the displayed dialog, enter the address information in the Source Host/Network box. The IP address information that you enter must include the IP address of the PC you will use to manage the router.

Step 4 Choose an outside interface with a static IP address in the Management Interface box. This interface must have a route to the IP address you specified in the Source Host/Network box.

Step 5 In the Management Protocols box, check **Allow SDM**.

Step 6 Check **HTTPS** and **SSH** to allow those protocols.

Step 7 Click OK to close the dialog.

Step 8 Click **Apply Changes** in the window that displays management access policies.

How Do I...

This section contains procedures for tasks that the wizard does not help you complete.

How Do I View Activity on My Firewall?

Activity on your firewall is monitored through the creation of log entries. If logging is enabled on the router, whenever an access rule that is configured to generate log entries is invoked—for example, if a connection were attempted from a denied IP address—then a log entry is generated and can be viewed in Monitor mode.

Enable Logging

The first step to viewing firewall activity is to enable logging on the router. To enable logging:

Step 1 From the Feature bar, choose **Configure > Router > Logging.**

Step 2 Click **Edit**.

Step 3 In the Syslog screen, check **Logging to Buffer**.

Step 4 In the Buffer Size field, enter the amount of router memory that you want to use for a logging buffer. The default value is 4096 bytes. A larger buffer will store more log entries but you must balance your need for a larger logging buffer against potential router performance issues.

Step 5 Click **OK**.

Identify the Access Rules for Which You Want to Generate Log Entries

In addition to enabling logging, you must identify the access rules that you want to generate log entries. To configure access rules for generating log entries:

Step 1 From the Feature bar, choose **Configure > Router > ACL**.

Step 2 Click **ACL Editor**.

Each access rule appears in the upper table on the right side of the screen. The lower table shows the specific source and destination IP addresses and the services that are permitted or denied by the rule.

Step 3 In the upper table, choose the rule that you want to modify.

Step 4 Click **Edit**.

The Edit a Rule dialog box appears.

Step 5 The Rule Entry field shows each of the source IP/destination IP/service combinations that are permitted or denied by the rule. Click the rule entry that you want to configure to generate log entries.

Step 6 Click **Edit**.

Step 7 In the rule entry dialog box, check the **Log Matches Against this Entry** check box.

Step 8 Click **OK** to close the dialog boxes you have displayed.

The rule entry that you just modified will now generate log entries whenever a connection is attempted from the IP address range and services that the define the rule entry.

Step 9 Repeat Step 4 through Step 8 for each rule entry that you want to configure to generate log entries.

Once your logging configuration is complete, follow the steps below to view your firewall activity:

Step 1 From the Feature bar, choose **Monitor > Security**.

Step 2 Choose **Firewall Status**.

In the firewall statistics display, you can verify that your firewall is configured and view how many connection attempts have been denied.

The table shows each router log entry generated by the firewall, including the time and the reason that the log entry was generated.

How Do I Configure a Firewall on an Unsupported Interface?

Cisco CP can configure a firewall on an interface type unsupported by Cisco CP. Before you can configure the firewall, you must first use the router CLI to configure the interface. The interface must have, at a minimum, an IP address configured, and it must be working. For more information on how to configure an interface using the CLI, refer to the Software Configuration Guide for your router.

To verify that the connection is working, verify that the interface status is "Up" in the Interfaces and Connections window.

The following is an excerpt showing the configuration for an ISDN interface on a Cisco 3620 router:

```
!
isdn switch-type basic-5ess
!
interface BRI0/0
!  This is the data BRI WIC
 ip unnumbered Ethernet0/0
 no ip directed-broadcast
 encapsulation ppp
 no ip mroute-cache
 dialer map ip 100.100.100.100 name junky 883531601
 dialer hold-queue 10
 isdn switch-type basic-5ess
 isdn tei-negotiation first-call
 isdn twait-disable
 isdn spid1 80568541630101 6854163
 isdn incoming-voice modem
```

Other configurations are available in the Software Configuration Guide for your router.

After you have configured the unsupported interface using the CLI, you can use Cisco CP to configure the firewall. The unsupported interface will appear as "Other" in the fields listing the router interfaces.

How Do I Configure a Firewall After I Have Configured a VPN?

If a firewall is placed on an interface used in a VPN, the firewall must permit traffic between the local and remote VPN peers. If you use the Basic or Advanced Firewall wizard, Cisco CP will automatically permit traffic to flow between VPN peers.

If you create an access rule in the ACL Editor available in Additional Tasks, you have complete control over the permit and deny statements in the rule, and you must ensure that traffic is permitted between VPN peers. The following statements are examples of the types of statements that should be included in the configuration to permit VPN traffic:

```
access-list 105 permit ahp host 123.3.4.5 host 192.168.0.1
access-list 105 permit esp host 123.3.4.5 host 192.168.0.1
access-list 105 permit udp host 123.3.4.5 host 192.168.0.1 eq isakmp
access-list 105 permit udp host 123.3.4.5 host 192.168.0.1 eq
non500-isakmp
```

How Do I Permit Specific Traffic Through a DMZ Interface?

Follow the steps below to configure access through your firewall to a web server on a DMZ network:

Step 1 From the Feature bar, choose **Configure > Security > Firewall > Firewall.**

Step 2 Select **Advanced Firewall**.

Step 3 Click **Launch the Selected Task**.

Step 4 Click **Next**.

The Advanced Firewall Interface Configuration screen appears.

Step 5 In the Interface table, select which interfaces connect to networks inside your firewall and which interfaces connect to networks outside the firewall.

Step 6 From the DMZ Interface field, select the interface that connects to your DMZ network.

Step 7 Click **Next>**.

Step 8 In the IP Address field, enter the IP address or range of IP addresses of your web server(s).

Step 9 From the Service field, select TCP.

Step 10 In the Port field, enter **80** or **www**.

Step 11 Click **Next>**.

Step 12 Click **Finish**.

How Do I Modify an Existing Firewall to Permit Traffic from a New Network or Host?

You can use the Edit Firewall Policy tab to modify your firewall configuration to permit traffic from a new network or host.

Step 1 From the Feature bar, choose **Configure > Security > Firewall > Firewall.**

Step 2 Click the **Edit Firewall Policy** tab.

Step 3 In the traffic selection panel select a From interface and a To interface to specify the traffic flow to which the firewall has been applied, and click **Go**. A firewall icon will appear in the router graphic if a firewall has been applied to the traffic flow. If the traffic flow you select does not display the access rule you need to modify, select a different From interface or a different To interface.

Step 4 Examine the access rule in the Service area. Use the **Add** button to disp.lay a dialog for a new access rule entry.

Step 5 Enter a permit statement for the network or host you want to allow access to the network. Click **OK** in the rule entry dialog.

Step 6 The new entry appears in the service area.

Step 7 Use the **Cut** and **Paste** buttons to reorder the entry to a different position in the list if you need to do so.

How Do I Configure NAT on an Unsupported Interface?

Cisco CP can configure Network Address Translation (NAT) on an interface type unsupported by Cisco CP. Before you can configure the firewall, you must first use the router CLI to configure the interface. The interface must have, at a minimum, an IP address configured, and it must be working. To verify that the connection is working, verify that the interface status is “Up.”

After you have configured the unsupported interface using the CLI, you can configure NAT. The unsupported interface will appear as “Other” on the router interface list.

How Do I Configure NAT Passthrough for a Firewall?

If you have configured NAT and are now configuring your firewall, you must configure the firewall so that it permits traffic from your public IP address. To do this you must configure an ACL. To configure an ACL permitting traffic from your public IP address:

Step 1 From the Feature bar, choose **Configure > Router > ACL**.

Step 2 Choose **ACL Editor**.

Step 3 Click **Add**.

The Add a Rule dialog box appears.

Step 4 In the Name/Number field, enter a unique name or number for the new rule.

Step 5 From the Type field, choose **Standard Rule**.

Step 6 In the Description field, enter a short description of the new rule, such as "Permit NAT Passthrough."

Step 7 Click **Add**.

The Add a Standard Rule Entry dialog box appears.

Step 8 In the Action field, choose **Permit**.

Step 9 In the Type field, choose **Host**.

Step 10 In the IP Address field, enter your public IP address.

Step 11 In the Description field, enter a short description, such as "Public IP Address."

Step 12 Click **OK**.

Step 13 Click **OK**.

The new rule now appears in the Access Rules table.

How Do I Permit Traffic Through a Firewall to My Easy VPN Concentrator?

In order to permit traffic through your firewall to a VPN concentrator, you must create or modify access rules that permit the VPN traffic. To create these rules:

Step 1 From the Feature bar, choose **Configure > Router > ACL**.

Step 2 Choose **ACL Editor**.

Step 3 Click **Add**.

The Add a Rule dialog box appears.

Step 4 In the Name/Number field, enter a unique name or number for this rule.

Step 5 In the Description field, enter a description of the rule, such as "VPN Concentrator Traffic."

Step 6 Click **Add**.

The Add an Extended Rule Entry dialog box appears.

Step 7 In the Source Host/Network group, from the Type field, select **A Network**.

Step 8 In the IP Address and Wildcard Mask fields, enter the IP address and network mask of the VPN source peer.

Step 9 In the Destination Host/Network group, from the Type field, select **A Network**.

Step 10 In the IP Address and Wildcard Mask fields, enter the IP address and network mask of the VPN destination peer.

Step 11 In the Protocol and Service group, select **TCP**.

Step 12 In the Source port fields, select =, and enter the port number **1023**.

Step 13 In the Destination port fields, select =, and enter the port number **1723**.

Step 14 Click **OK**.

The new rule entry appears in the Rule Entry list.

Step 15 Repeat Step 7 through Step 15, creating rule entries for the following protocols and, where required, port numbers:

- Protocol **IP**, IP protocol **GRE**
- Protocol **UDP**, Source Port **500**, Destination Port **500**
- Protocol **IP**, IP Protocol **ESP**
- Protocol **UDP**, Source Port **10000**, Destination Port **10000**

Step 16 Click **OK**.

How Do I Associate a Rule with an Interface?

If you use the Cisco CP Firewall wizard, the access and inspection rules that you create are automatically associated with the interface for which you created the firewall. If you are creating a rule in Additional Tasks/ACL Editor, you can associate it with an interface from the Add or Edit a Rule window. If you do not associate it with an interface at that time, you can still do so later.

Step 1 From the Feature bar, click **Basic Router > Interfaces and Connections > Edit Interface/Connection**.

Step 2 Select the interface that you want to associate a rule with, and click **Edit**.

Step 3 In the Association tab, enter the rule name or number in the Inbound or Outbound field in the Access Rule or Inspection Rule boxes. If you want the rule to filter traffic before it enters the interface, use the Inbound field. If you want the rule to filter traffic that has already entered the router, but may exit the router through the selected interface, use the Outbound field.

Step 4 Click **OK** in the Association tab.

Step 5 In the Access Rules or the Inspection Rules window, examine the Used By column to verify that the rule has been associated with the interface.

How Do I Disassociate an Access Rule from an Interface

You may need to remove the association between an access rule and an interface. Removing the association does not delete the access rule. You can associate it with other interfaces if you want. To remove the association between an access rule and an interface, perform the following steps.

Step 1 From the Feature bar, click **Basic Router > Interfaces and Connections > Edit Interfaces and Connections**.

Step 2 Select the interface that you want to disassociate the access rule from.

Step 3 Click **Edit**.

Step 4 In the Association tab, find the access rule in the inbound or outbound field in the Access Rule box. The access rule may have a name, or a number.

Step 5 Click in the inbound or outbound field, and then click the button to the right.

Step 6 Click **None (clear rule association)**.

Step 7 Click **OK**.

How Do I Delete a Rule That Is Associated with an Interface?

Cisco CP does not allow you to delete a rule that is associated with an interface; you must first remove the association between the rule and the interface, and then delete the access rule.

Step 1 From the Feature bar, click **Basic Router > Interfaces and Connections > Edit Interfaces and Connections**.

Step 2 Select the interface that you want to disassociate the rule from.

Step 3 Click **Edit**.

Step 4 In the Association tab, find the rule in the Access Rule box or the Inspect Rule box. The rule may have a name or a number.

Step 5 Find the rule in the association tab. If it is an access rule, click **None (clear rule association).** If it is an Inspection rule, click **None**.

Step 6 Click **OK**.

Step 7 Click **Rules** in the left frame. Use the Rules tree to go to the Access Rule or the Inspection Rule window.

Step 8 Select the rule that you want to remove, and click **Delete**.

How Do I Create an Access Rule for a Java List?

Inspection rules allow you to specify Java lists. A Java list is used to permit Java applet traffic from trusted sources. These sources are defined in an access rule that the Java List references. To create this kind of access rule, and use it in a Java list, do the following:

Step 1 If you are at the Inspection Rules window, and you have clicked **Java List**, click the button to the right of the Number field and click **Create a new rule (ACL) and select.** The Add a Rule window opens.

If you are at the Access Rules window, click **Add** to open the Add a Rule window.

Step 2 From the Add a Rule window, create a standard access rule that permits traffic from the addresses you trust. For example, if you wanted to permit Java applets from hosts 10.22.55.3, and 172.55.66.1, you could create the following access rule entries in the Add a Rule window:

```
permit host 10.22.55.3
permit host 172.55.66.1
```

You can provide descriptions for the entries and a description for the rule.

You do not need to associate the rule with the interface to which you are applying the inspection rule.

Step 3 Click **OK** in the Add a Rule window.

Step 4 If you started this procedure from the Inspection Rules window, then click **OK** in the Java List window. You do not need to complete Step 5 and Step 6.

Step 5 If you started this procedure in the Access Rules window, go to the Inspection Rules window and select the inspection rule you want to create a Java list for, and click **Edit**.

Step 6 Check **http** in the Protocols column, and click **Java List**.

Step 7 In the Java List Number field, enter the number of the access list that you created. Click **OK**.

How Do I Permit Specific Traffic onto My Network if I Don't Have a DMZ Network?

The Firewall wizard, lets you specify the traffic that you want to allow onto the DMZ. If you do not have a DMZ network, you can still permit specified types of outside traffic onto your network, using the Firewall Policy feature.

Step 1 Configure a firewall by going to **Configure > Security > Firewall > Firewall**.

Step 2 Click **Edit Firewall Policy/ACL**.

Step 3 To display the access rule you need to modify, select the outside (untrusted) interface as the From interface, and the inside (trusted) interface as the To interface. The access rule applied to inbound traffic on the untrusted interface is displayed.

Step 4 To allow a particular type of traffic onto the network that is not already allowed, click **Add** in the Service area.

Step 5 Create the entries you need in the rule entry dialog.You must click **Add** for each entry you want to create.

Step 6 The entries you create will appear in the entry list in the Service area.

CHAPTER 23

Firewall Policy

The Firewall Policy feature lets you create, view, and modify firewall configurations—access rules and CBAC inspection rules—in the context of the interfaces whose traffic they filter. Using a graphical representation of the router and its interfaces, you can choose different interfaces on the router and determine whether an access rule or an inspection rule has been applied to that interface. You can also view the details of the rules displayed in the Edit Firewall Policy/ACL window.

Edit Firewall Policy/ACL

Use the Edit Firewall Policy/ACL window to view the access and inspection rules in a context that displays the interfaces the rules are associated with. Also, use it to modify the access and inspection rules that are displayed.

Configure a Firewall Before Using the Firewall Policy Feature

Before using the Edit Firewall Policy/ACL window, you should perform the following tasks:

1. **Configure LAN and WAN interfaces**. You must configure the LAN and WAN interfaces before you can create a firewall. You can use the LAN and WAN wizards to configure connections for your router.
2. **Use the Firewall wizard to configure a firewall and a Demilitarized Zone (DMZ)**. The Firewall wizard is the easiest way to apply access rules and inspection rules to the inside and outside interfaces you identify, and will allow you to configure a DMZ interface and specify the services that should be allowed onto the DMZ network.
3. **Use the Firewall Policy window to edit the firewall policy you created**. After configuring LAN and WAN interfaces and creating a firewall, you can open this window and get a graphical representation of the policy in a traffic flow. You can view the access rule and inspection rule entries and make any necessary changes.

Use the Firewall Policy View Feature

After you have created the firewall, you can use the Firewall Policy View window to get a graphical view of the firewall in the context of the router interfaces, and to modify it as needed.

For more information, click the appropriate action:

- Choose a Traffic Flow
- Examine the Traffic Diagram and Choose a Traffic Direction
- Make Changes to Access Rules
- Make Changes to Inspection Rules

Note If the router is using a Cisco IOS image that does not support the Firewall feature set, only the Services area is displayed, and you can only create access control entries.

Apply Changes Button

Click the Apply Changes button to deliver changes you have made in this window to the router. If you leave the Edit Firewall Policy/ACL window without clicking **Apply Changes**, Cisco CP displays a message indicating that you must either apply the changes or discard them.

Discard Changes Button

Click the Discard Changes button to discard changes you have made in this window. This button does not let you remove changes that you have delivered to the router using the **Apply Changes** button.

Choose a Traffic Flow

Traffic flow refers to traffic that enters the router on a specified interface (the *from* interface) and exits the router on a specified interface (the *to* interface). The Cisco CP traffic-flow display controls are located in a row at the top of the Edit Firewall Policy/ACL window.

Note There must be a least two configured interfaces on the router. If there is only one, Cisco CP displays a message telling you to configure an additional interface.

Table 23-1defines the Cisco CP traffic-flow display controls.

Table 23-1 Traffic-flow display Controls

From	Choose the interface from which the traffic flow originates. The firewall protects the network connected to the **From** interface. The **From** drop-down list contains only interfaces with configured IP addresses.
To	Choose the interface from which the traffic leaves the router. The **To** drop-down list contains only interfaces with configured IP addresses.
	Click the **Details** button to view details about the interface. Details such as IP address, encapsulation type, associated IPSec policy, and authentication type are provided.

Table 23-1 Traffic-flow display Controls

Go button	Click the **Go** button to update the traffic-flow diagram with information about the interfaces chosen. The diagram is not updated until you click **Go**. The **Go** button is disabled if you have not chosen a **From** interface or a **To** interface, or if the **From** and **To** interfaces are the same.
View Option	Choose **Swap From and To interface** to swap the interfaces that you originally chose in the **From** and **To** drop-down lists. You can use the swap option to create a firewall protecting both the network connected to the **From** interface and the network connected to the **To** interface. Choose **View all Access control lists in traffic flow** when one access rule has been applied to the **From** interface and another access rule has been applied to the **To** interface for a traffic direction you have chosen. The entries of both access rules are displayed in another window.

Cisco CP displays interfaces that have IP addresses in alphabetical order in both the **From** and **To** drop-down lists. By default, Cisco CP chooses the first interface in the **From** list, and the second interface in the **To** list. Use the **From** and **To** drop-down lists to choose a different traffic flow. The chosen traffic flow is displayed in the traffic diagram below the traffic-flow display controls.

For example, to view traffic flow from a network connected to the router interface Ethernet 0 and exiting on the router interface Serial 0, follow these steps:

Step 1 Choose Ethernet 0 in the **From** drop-down list.

Step 2 Choose Serial 0 in the **To** drop-down list.

Step 3 Click **Go**.

Step 4 To switch the interfaces in the **From** and **To** drop-down lists, choose **Swap From and To interface** from the **View Option** drop-down list.

Access rules applied to originating and returning traffic may be different. To learn more about how to switch between displaying originating and returning traffic in the traffic diagram, see Examine the Traffic Diagram and Choose a Traffic Direction.

Step 5 Click the **Details** button next to the **From** or **To** drop-down list to open a window showing the IP address, IPSec policy, and other information of an interface.

To work with the traffic diagram, see Examine the Traffic Diagram and Choose a Traffic Direction. To return to the main Firewall Policy window description see Edit Firewall Policy/ACL.

Examine the Traffic Diagram and Choose a Traffic Direction

The traffic diagram displays the router with the chosen From and To interfaces (see Choose a Traffic Flow for more information). It also displays the types of rules applied for the chosen traffic flow, as well as the direction in which they have been applied.

Originating Traffic

Click Originating Traffic to highlight the traffic flow that enters the router at the From interface and exits the router at the To interface. When this area is highlighted, you can see the details of rules applied in the direction of traffic flow.

Returning Traffic

Click Returning Traffic to highlight the traffic flow that enters the router on the To interface and exits the router on the From interface. When this area is highlighted, you can see the details of rules applied to returning traffic.

Icons

Rules are represented by icons in the traffic flow:

Table 23-2 Icons

	Filter symbol indicates that an access rule is being applied.
	Magnifying glass indicates that an inspection rule is being applied.
	Firewall icon in the router indicates that a firewall has been applied to the Originating traffic flow. Cisco CP displays a firewall icon if the following sets of criteria are met: • There is an inspection rule applied to Originating traffic on the inbound direction of the From interface, and there is an access rule applied to the inbound direction of the To interface. • The access rule on the inbound direction of the To interface is an extended access rule, and contains at least one access rule entry. No firewall icon is displayed when a firewall has been applied to Returning traffic. If the Firewall feature is available, but no firewall has been applied to the traffic flow, **IOS Firewall: Inactive** is displayed below the traffic diagram.

Table 23-2 Icons

	Rules applied to Originating traffic are indicated by a right arrow. An icon on the From interface traffic line indicates the presence of a rule filtering traffic inbound to the router. An icon placed on the To interface traffic line indicates a rule filtering traffic outbound from the router. If you place the mouse over this icon, Cisco CP displays the names of the rules that have been applied.
	Rules applied to Returning traffic are indicated by a left arrow. An icon on the To interface traffic line indicates the presence of a rule filtering traffic inbound to the router. An icon on the From interface traffic line indicates the presence of a rule filtering traffic outbound from the router. The names of the rules applied are displayed when you place the cursor over this icon.

Note Although the icons are shown on a particular interface in the diagram, a firewall policy might contain access control entries that affect traffic not represented by the diagram. For example, an entry that contains the wildcard icon in the Destination column (see Make Changes to Access Rules) might apply to traffic exiting interfaces other than the one represented by the currently chosen To interface. The wildcard icon appears as an asterisk and stands for any network or host.

To make changes to an access rule, see Make Changes to Access Rules. To return to the main Firewall Policy window description, see Edit Firewall Policy/ACL.

Make Changes to Access Rules

The Policy panel shows the details of the rules applied to the chosen traffic flow. The Policy panel is updated when the From and To interfaces are chosen and when the Traffic Diagram is toggled between Originating Traffic focus and Returning Traffic focus.

The Policy panel is blank if an access rule that contains no entries has been associated with an interface. For example, if a rule name was associated with an interface using the CLI, but entries for the rule were not created, this panel would be blank. If the Policy Panel is blank, you can use the **Add** button to create entries for the rule.

Service Area Header Fields

Table 23-3 Service Area Header Fields

Firewall Feature Availability	If the Cisco IOS image that the router is using supports the Firewall feature, this field contains the value **Available**.
Access Rule	Name or number of the access rule whose entries are being displayed.
Inspection Rule	Name of the inspection rule whose entries are being displayed.
	This icon appears when an access rule has been associated with an interface, but no access rule of that name or number has been created. Cisco CP informs you that the policy has no effect unless there is at least one access rule entry.

Service Area Controls

The following table describes the controls found in the Service Area.

Table 23-4 Service Area Controls

Add button	Click the **Add** button to add an access rule entry. Specify whether you want to add the entry before or after the entry currently chosen. Then, create the entry in the Add an Entry window. **Note** Remember that the order of entries is important. Cisco CP displays the Extended entry dialog when you add an entry from the Edit Firewall Policy/ACL window. To add a standard rule entry, go to **Configure > Router > ACL > ACL Editor**.
Edit button	Click the **Edit** button to edit a chosen access rule entry. Although you can only add extended rule entries in the Edit Firewall Policy/ACL window, you are not prevented from editing a standard rule entry that has already been applied to a chosen interface.
Cut button	Click the **Cut** button to remove a chosen access rule entry. The entry is placed on the clipboard and can be pasted to another position in the list, or it can be pasted to another access rule. If you want to reorder an entry, you can cut the entry from one location, choose an entry before or after the location that you want for the cut entry, and click **Paste**. The Paste context menu allows you to place the entry before or after the entry you chose.
Copy button	Choose a rule entry and click to put the rule entry on the clipboard.
Paste button	Click the Paste button to paste an entry on the clipboard to the chosen rule. You are prompted to specify whether to paste the entry before or after the currently chosen entry. If Cisco CP determines that an identical entry already exists in the access rule, it displays the Add an Extended Rule Entry window so that you can modify the entry. Cisco CP does not allow duplicate entries in the same access rule.

Table 23-4 Service Area Controls

Interface drop-down list	If the chosen traffic flow (Originating or Returning) contains an access rule on both the From interface and the To interface, you can use this list to toggle between the two rules.
Apply Firewall	If the chosen traffic flow does not have a firewall applied, you can apply a firewall by choosing Originating traffic and clicking the Apply Firewall button. By default, clicking Apply Firewall associates a Cisco CP-default inspection rule to the inbound direction of the From interface, and associates an access rule to the inbound direction of the To interface that denies traffic. If the Cisco IOS image that the router is using does not support the Firewall feature, this button is disabled. For example, to apply a firewall that protects the network connected to the **Ethernet 0** interface from traffic entering the **Ethernet 1** interface, choose **Ethernet 0** from the **From** drop-down list, and **Ethernet 1** from the **To** drop-down list. Then, click **Apply Firewall**. To apply a firewall that protects the network connected to the **Ethernet 1** interface from traffic entering the **Ethernet 0** interface, go to **Configure > Router > ACL > ACL Editor**.

Service area buttons are disabled if the rule is read-only. A rule is read-only when it contains syntax that Cisco CP does not support. Read-only rules are indicted by this icon: .

If there is an existing standard rule that filters the returning traffic flow to which you are applying the firewall, Cisco CP informs you that it will convert the standard access rule to an extended rule.

Service Area Entry Fields

The following table describes the icons and other data in the Service Area entries.

Table 23-5 Service Area Entry Fields

Field	Description	Icons	Meaning
Action	Whether the traffic is permitted or denied		Permit source traffic.
			Deny source traffic.
Source/ Destination	Network or host address, or any host or network.		The address of a network.
			The address of a host.
			Any network or host.
Service	Type of service filtered.		Examples: TCP, EIGRP, UDP, GRE. See IP Services.
			Examples: Telnet, http, FTP. See TCP Services.
			Examples: SNMP, bootpc, RIP. See UDP Services.
			Internet Group Management Protocol (IGMP).
			Examples: echo-reply, host-unreachable. See ICMP Message Types.
Log	Whether or not denied traffic is logged.		Log denied traffic. To configure logging for firewalls, see Firewall Log.
Option	Options configured using the CLI	No icons.	
Description	Any description provided.	No icons	

To make changes to inspection rules, see Make Changes to Inspection Rules. To return to the main Firewall Policy window description, see Edit Firewall Policy/ACL.

Make Changes to Inspection Rules

The Applications area appears if the Cisco IOS image running on the router supports CBAC Inspection rules. The Applications area displays the inspection rule entries that are filtering the traffic flow, and is updated whenever a new traffic flow is chosen. The inspection rule that affects the chosen direction of traffic is displayed.

The Applications area displays one of the following options for **Originating traffic**:

- The inspection rule that is applied to the inbound direction of the From interface, if one exists.
- The inspection rule that is applied to the outbound direction of the To interface, if the inbound direction of the From interface has no inspection rule applied.

Swap From and To Interfaces to Bring Other Rules into View

Inspection rules applied to **Returning traffic** are not displayed.You can display an inspection rule applied to **Returning traffic** by choosing **Swap From and To interfaces** in the View Options menu. You can also view inspection rules that are not displayed in the Edit Firewall Policy/ACL window by going to the Application Security window in the Firewall and ACL task.

Table 23-6 Swap From and To Interfaces

	This icon appears when two inspection rules are found in the chosen traffic direction. Cisco CP also displays a warning dialog, giving you the opportunity to dissociate one of the inspection rules from the interface.

Application Area Controls

The following is a description of the Application area controls:

Add—Click to add an inspection rule. If there is no inspection rule, you can add the Cisco CP default inspection rule, or you can create and add a custom inspection rule. If you add the Cisco CP default inspection rule to a traffic flow with no inspection rule, it will be associated with the inbound traffic to the From interface. You can add an entry for a specific application whether or not an inspection rule already exists.

Edit—Click to edit a chosen entry.

Delete—Click to delete a chosen entry.

Global Settings—Click to display a dialog box that enables you to set global timeouts and thresholds.

Summary—Click to display the application or protocol name and a description for each entry.

Detail—Click to display the application or protocol name, description, alert status, audit trail status, and timeout settings for each entry.

Application Area entry fields

The following list describes the Application area entry fields:

Application Protocol—Displays the name of the application or protocol. For example, **vdolive**.

Alert—Indicates whether or not an alert is on (default) or off.

Audit Trail—Indicates whether or not audit trail is on or off (default).

Timeout—Displays how long, in seconds, the router waits before blocking return traffic for this protocol or application.

Description—Displays a short description. For example, **VDOLive protocol**.

To return to the main Firewall Policy window description, see Edit Firewall Policy/ACL.

Add *App-Name* Application Entry

Use this window to add an application entry for the Cisco IOS firewall to inspect.

Alert Action

Choose one of the following:

- **default-on**—Leave as default. Default value is **on**.
- **on**—Enable alert.
- **off**—Disable alert.

Audit Action

Choose one of the following:

- **default-off**—Leave as default. Default value is **off**.
- **on**—Enable audit trail.
- **off**—Disable audit trail.

Timeout

Specify how long the router should wait before blocking return traffic for this protocol or application. The field is prefilled with the default value for the protocol or application.

Add rpc Application Entry

Add a Remote Procedure Call (RPC) program number in this window, and specify Alert, Audit, Timeout, and Wait time settings.

Alert Action

Choose one of the following:

- **default-on**—Leave as default. Default value is **on**.
- **on**—Enable alert.
- **off**—Disable alert.

Audit Action

Choose one of the following:

- **default-off**—Leave as default. Default value is **off**.
- **on**—Enable audit trail.
- **off**—Disable audit trail.

Timeout

Specify how long the router should wait before blocking return traffic for this protocol or application. The field is prefilled with the default value.

Program Number

Enter a single program number in this field.

Wait Time

You can specify how many minutes to allow subsequent RPC connections from the same source to be made to the same destination address and port. The default wait time is zero minutes.

Add Fragment application entry

In this window, you can add a fragment entry to an inspection rule that you are configuring in the Edit Firewall Policy/ACL window, and you can specify Alert, Audit, and Timeout settings. A fragment entry sets the maximum number of unreassembled packets that the router should accept before dropping them.

Alert Action

Choose one of the following:

- **default(on)**—Leave as default. Default value is **on**.
- **on**—Enable alert.
- **off**—Disable alert.

Audit Action

Choose one of the following:

- **default(off)**—Leave as default. Default value is **off**.
- **on**—Enable audit trail.
- **off**—Disable audit trail.

Timeout

Specify how long the router should wait before blocking return traffic for this protocol or application. The field is prefilled with the default value.

Range (optional)

Enter the maximum number of unreassembled packets the router should accept before dropping them. The range can have a value between 50 and 10000.

Add or Edit http Application Entry

Use this window to add an http application to the inspection rule.

Alert Action

Choose one of the following:

- **default-on**—Leave as default. Default value is **on**.
- **on**—Enable alert.
- **off**—Disable alert.

Audit Action

Choose one of the following:

- **default-off**—Leave as default. Default value is **off**.
- **on**—Enable audit trail.
- **off**—Disable audit trail.

Timeout

Specify how long the router should wait before blocking return traffic for this protocol or application. The field is prefilled with the default value.

Hosts/network for Java applet download

The source hosts or networks whose applet traffic is to be inspected. Multiple hosts and networks can be specified.

Click **Add** to display the Java Applet Blocking window in which you can specify a host or network.

Click **Delete** to remove an entry from the list.

Java Applet Blocking

Use this window to specify whether Java applets from a specified network or host should be permitted or denied.

Action

Choose one of the following:

- **Do Not Block (Permit)**—Permit Java applets from this network or host.
- **Block (Deny)**—Deny Java applets from this network or host.

Host/Network

Specify the network or the host.

Type

Choose one of the following:

- **A Network**—If you choose this option, provide a network address in the IP address field. Note that the wildcard mask enables you to enter a network number that may specify multiple subnets.
- **A Host Name or IP Address**—If you choose this option, provide a host IP address or host name in the next field.
- **Any IP address**—If you choose this option, the action you specified is applied to any host or network.

IP Address/Wildcard Mask

Enter a network address and then the wildcard mask to specify how much of the network address must match exactly.

For example, if you entered a network address of 10.25.29.0 and a wildcard mask of 0.0.0.255, any Java applet with a source address containing 10.25.29 would be filtered. If the wildcard mask were 0.0.255.255, any Java applet with a source address containing 10.25 would be filtered.

Host Name/IP

This field appears if you chose **A Host Name or IP Address** as Type. If you enter a host name, ensure that there is a DNS server on the network that can resolve the host name to an IP address.

Cisco CP Warning: Inspection Rule

This window is displayed when Cisco CP finds two inspection rules that have been configured for a direction in a traffic flow. For example, you might have one inspection rule applied to traffic inbound on the From interface, and another applied to traffic outbound on the To interface. Two inspection rules may not harm the functioning of the router, but they may be unnecessary. Cisco CP allows you to keep the inspection rules the way they are, to remove the inspection rule on the From interface, or to remove the inspection rule on the To interface.

- **Do not make any change**—Cisco CP does not remove either inspection rule.
- **Keep inspection rule *name* on <**interface-name**> inbound, and dissociate inspection rule *name* on <**interface-name**> outbound**—Cisco CP keeps one inspection rule and dissociates the rule from the other interface.
- **Keep inspection rule *name* on <**interface-name**> outbound and dissociate inspection rule *name* on <**interface-name**> inbound**—Cisco CP keeps one inspection rule and dissociates the rule from the other interface.

Before you make a selection and click **OK**, first click **Cancel** to determine if you need to add entries to the inspection rule to retain. You can add entries by using the **Add** button in the Application area toolbar in the Edit Firewall Policy/ACL window.

Cisco CP Warning: Firewall

This window appears when you click **Apply Firewall** in the Edit Firewall Policy/ACL window. It lists the interfaces to which it will apply a rule, and describes the rule that it will apply.

Example:

```
Cisco CP will apply firewall configuration to the following
interfaces:
Inside (Trusted) Interface: FastEthernet 0/0
* Apply inbound default Cisco CP Inspection rule
* Apply inbound ACL. Anti-spoofing, broadcast, local loopback, etc.).

Outside (Untrusted) Interface: Serial 1/0
* Apply inbound access list to deny returning traffic.
```

Click **OK** to accept these changes, or click **Cancel** to stop the application of the firewall.

Edit Firewall Policy

The Edit Firewall Policy window provides a graphical view of the firewall policies on the router and enables you to add ACLs to policies without leaving the window. Read the procedures in the sections that follow to view the information in this window and add rules.

This help topic contains the following sections:

- Things You Must do Before Viewing Information in this Window
- Expanding and Collapsing the Display of a Policy
- Adding a New Rule to a Policy
- Adding a New Zone Policy
- Reordering Rules Within a Policy
- Copying and Pasting a Rule
- Displaying the Rule Flow Diagram
- Applying Your Changes
- Discarding Your Changes

Things You Must do Before Viewing Information in this Window

This window is empty if no zone, zone pairs, or policy maps have been configured. Create a basic configuration containing these elements by going to **Configure > Security > Firewall > Firewall > Create Firewall** and completing the Advanced Firewall wizard. After you have done this, you can create additional zones, zone pairs, and policies as needed by going to **Configure > Security > Firewall > Firewall Components > Zones** to configure zones, and to **Configure > Security > Firewall > Firewall Components > Zone Pairs** to configure additional zone pairs.

To create the policy maps that the zone pairs are to use, go to **Configure > Security > C3PL**. Click the **Policy Map** branch to display additional branches that enable you to create policy maps and the class maps that define traffic for the policy maps.

Expanding and Collapsing the Display of a Policy

When the display of a policy is collapsed, only the policy name and the source and destination zones are displayed. To expand the display of the policy to show the rules that make up the policy, click the **+** button to the left of the policy name. An expanded view of a firewall policy might look similar to the following:

		Traffic Classification			Action	Rule Options
	ID	**Source**	**Destination**	**Service**		
	clients-servers-policy (clients to servers)					
	1	any	any	tcp	Allow	
				udp	Inspect	
				icmp		
	2	Unmatched Traffic			Drop	

The policy named clients-servers-policy contains two ACLs. The rule with the ID 1 permits TCP, UDP, and ICMP traffic from any source to any destination. The rule with the ID 2 drops any unmatched traffic.

Adding a New Rule to a Policy

To add a new rule to a policy, complete the following steps:

Step 1 Click anywhere in the display for that policy, and click the **+ Add** button.

- To insert a rule for new traffic in the order required, select an existing rule, click the **+ Add** button, and choose **Insert** or **Insert After**. The Insert and Insert After options are also available from a context menu that you display by right-clicking on an existing rule.
- Choosing **Rule for New Traffic** automatically places the new rule at the top of the list.
- Choosing **Rule for Existing Traffic** allows you to select an existing class map and modify it. It automatically places the new rule at the top of the list.

Step 2 Complete the displayed dialog box. See Add a New Rule for more information.

Adding a New Zone Policy

To add a new zone policy, complete the following steps:

Step 1 Click **Add** and choose **New Zone Policy**.

Step 2 In the Add a Rule screen, specify the source zone by clicking the button to the right of the Source Zone field and selecting an existing zone or creating a new zone.

Step 3 Specify the destination zone by clicking the button to the right of the Destination Zone field and selecting an existing zone or creating a new zone.

Configure settings in the other fields of the Add a Rule window. See Add a New Rule for more information.

Reordering Rules Within a Policy

If a policy contains more than one rule that permits traffic, you can reorder them by selecting a rule and clicking the **Move Up** button or the **Move Down** button. The **Move Up** button is disabled if you selected a rule that is already at the top of the list, or if you selected the Unmatched Traffic rule. The **Move Down** button is disabled if you selected a rule that is already at the bottom of the list.

You can also use the **Cut** and the **Past**e buttons to reorder rules. To remove a rule from its current position, select it and click **Cut**. To place the rule in a new position, select an existing rule, click **Paste**, and choose **Paste** or **Paste After**.

The Move Up, Move Down, Cut, Paste, and Paste After operations are also available from the context menu displayed when you right-click on a rule.

Copying and Pasting a Rule

Copying and pasting a rule is very useful if one policy contains a rule that can be used with few or no modifications in another policy.

To copy a rule, select a rule and click the **Copy** button or right-click the rule and choose **Copy**. To paste the rule to a new location, click **Paste** and choose **Paste** or **Paste After**. The **Paste** and **Paste After** buttons are also available from the context menu. When you paste a rule to a new location, the Add a New Rule dialog box is displayed so you can make changes to the rule.

Displaying the Rule Flow Diagram

Click anywhere in a firewall policy and click **Rule Diagram** to display the Rule Flow Diagram for that policy. The Rule Flow Diagram displays the source zone on the right of the router icon and the destination zone on the left of the icon.

Applying Your Changes

To send your changes to the router, click **Apply Changes** at the bottom of the screen.

Discarding Your Changes

To discard changes that you have made but have not sent to the router, click **Discard Changes** at the bottom of the screen.

Add a New Rule

Define a traffic flow and specify protocols to inspect in the Add a Rule window. Complete the following steps to add a new rule:

Step 1 To create a zone policy, do the following:

a. To specify the source zone, click the button next to the Source Zone field. To choose an existing zone, click **Select a Zone** and choose the zone from the displayed dialog box. To create a zone, click **Create a Zone**, enter a zone name, and specify the interfaces to associate with the zone in the displayed dialog box.

b. To specify the destination zone, click the button next to the Destination Zone field. To choose an existing zone, click **Select a Zone** and choose the zone from the displayed dialog box. To create a zone, click **Create a Zone**, enter a zone name, and specify the interfaces to associate with the zone in the displayed dialog box.

Step 2 In the Source and Destination field, specify that the traffic is flowing between a network and another network by choosing **Network**, or that the traffic is flowing between entities that may be networks or may be individual hosts by choosing **Any**.

Step 3 Enter a name for the traffic flow in the Traffic Name field.

Step 4 Click **Add** next to the Source Network and Destination Network columns and add source and destination network addresses. You can add multiple entries for the source and destination networks, and you can edit an existing entry by selecting it and clicking **Edit**.

Step 5 Reorder an entry if necessary by selecting it and clicking **Move Up** or **Move Down**. The **Move Up** button is disabled when the selected entry is already at the top of the list. The **Move Down** button is disabled when the selected entry is already at the bottom of the list.

Step 6 Enter a name that describes the protocols or services that you are identifying for inspection in the Service Name field.

Step 7 To specify a service, click on a branch in the tree in the column on the left, choose the service, and click **Add>>**. Click the **+** icon next to a branch to display the available services of that type. To remove a service from the column on the right, select it and click **<<Remove**. The services or protocols in the tree can be viewed alphabetically or by category.

Step 8 To specify how the traffic should be handled, choose **Inspect, Allow,** or **Drop** in the Action field. If you choose **Allow**, you can click **Advanced** and choose a menu item to further define the action, such as inspecting the protocols that you chose in the service box. See the following help topics for more information:

- Application Inspection Dialog Box
- URL Filter
- Quality of Service
- Inspect Parameter

Step 9 If you chose **Drop** as the action, you can click **Log** to have the event logged.

Step 10 Click **OK** to close this dialog box and send the changes to the router.

Add Traffic

Use the **Add Traffic** dialog box to create a source and destination address entry for a rule.

Action

Use the Include or the Exclude option to specify whether the rule should be applied to the traffic exchanged between the source and destination addresses.

Choose **Permit** to include this traffic in the rule.

Choose **Deny** to have this traffic excluded from the rule.

Source Host/Network and Destination Host/Network

Specify the source and the destination of the traffic in these fields.

Type

Choose one of the following values:

- A Network—Choose to specify a network address as the source or destination, and specify the network address in the IP Address and Wildcard Mask fields.
- A Host Name or IP Address—Choose to specify the name or IP address of a host. Then, specify the host in the Host Name/IP field.
- Any IP Address—Choose to limit the source or destination traffic to any host or network.
- Network Object Group—If you selected **Network Object Group** in the Type field, click the **...** (more) button—located next to the Network Object Group field—to open the Select Network Object Groups dialog box. Select the network object group from the Available Groups pane, and then click **OK**. For details, see Select Network Object Groups Dialog Box, page 16-37.

IP Address

Enter the network address. This field is displayed when you choose **A Network** in the Type field.

Wildcard Mask

Enter the wildcard mask that specifies the bits that are used for the network address. For example, if the network address is 192.168.3.0, specify 0.0.0.255 as the mask. This field is displayed when you choose **A Network** in the Type field.

Host Name/IP

Enter the name or the IP address of a host in this field. If you enter a name, the router must be able to contact a DNS server to resolve the name to an IP address. This field is displayed when you choose **A Host Name** or **IP Address** in the Type field.

Application Inspection Dialog Box

Use the Application Inspection dialog box to configure deep packet inspection for the applications or protocols listed in the dialog box.

For example, to create a new policy map for Instant Messaging, check the box next to IM, click the button next to the IM field, and choose **Create**. Then, create the policy map in the Configure Deep Packet Inspection dialog box.

How to Get to This Page

Click **Configure > Security > Firewall > Firewall > Edit Firewall Policy > Select a rule > Edit > Advanced > Application Inspection**.

Related Topics

- Add Traffic, page 23-25
- Configure Deep Packet Inspection - SIP Dialog Box, page 23-30
- Manage H323 Messages Inspection Dialog Box, page 23-36
- URL Filter, page 23-37

Field Reference

Table 23-7 Application Inspection Dialog Box

Element	Description
HTTP	Select the checkbox. Click the button to the right of the field. Choose **Create**, **Select**, or **Edit**. Choose **Create** to configure a new policy map. The Configure Deep Packet Inspection dialog box is displayed. Choose **Select** to apply an existing policy map to the traffic. The policy map name appears in the field when you are done.
IM	Select the checkbox. Click the button to the right of the field. Choose **Create**, **Select**, or **Edit**. Choose **Create** to configure a new policy map. The Configure Deep Packet Inspection dialog box is displayed. Choose **Select** to apply an existing policy map to the traffic. The policy map name appears in the field when you are done.
P2P	Select the checkbox. Click the button to the right of the field. Choose **Create**, **Select**, or **Edit**. Choose **Create** to configure a new policy map. The Configure Deep Packet Inspection dialog box is displayed. Choose **Select** to apply an existing policy map to the traffic. The policy map name appears in the field when you are done.

Table 23-7 Application Inspection Dialog Box (continued)

Element	Description
SMTP	Select the checkbox. Click the button to the right of the field. Choose **Create**, **Select**, or **Edit**. Choose **Create** to configure a new policy map. The Configure Deep Packet Inspection dialog box is displayed. Choose **Select** to apply an existing policy map to the traffic. The policy map name appears in the field when you are done.
IMAP	Select the checkbox. Click the button to the right of the field. Choose **Create**, **Select**, or **Edit**. Choose **Create** to configure a new policy map. The Configure Deep Packet Inspection dialog box is displayed. Choose **Select** to apply an existing policy map to the traffic. The policy map name appears in the field when you are done.
POP3	Select the checkbox. Click the button to the right of the field. Choose **Create**, **Select**, or **Edit**. Choose **Create** to configure a new policy map. The Configure Deep Packet Inspection dialog box is displayed. Choose **Select** to apply an existing policy map to the traffic. The policy map name appears in the field when you are done.

Table 23-7 Application Inspection Dialog Box (continued)

Element	Description
Sun RPC	Select the checkbox. Click the button to the right of the field. Choose **Create**, **Select**, or **Edit**. Choose **Create** to configure a new policy map. The Configure Deep Packet Inspection dialog box is displayed. Choose **Select** to apply an existing policy map to the traffic. The policy map name appears in the field when you are done.
H323	Select the checkbox. Click the button to the right of the field. Click **Manage**. The Manage H323 Messages dialog box is displayed. **Note** The Cisco IOS image on the router has to be 12.4(20)T to enable H323 application inspection.
SIP	Select the checkbox. Click the button to the right of the field. Click **Manage**. The Enable Deep packet Inspection for SIP dialog box is displayed. **Note** The Cisco IOS image on the router has to be 12.4(20)T to enable SIP application inspection.

Configure Deep Packet Inspection - SIP Dialog Box

Use the Configure Deep Packet Inspection - SIP dialog box to configure SIP application inspection feature for deep packet inspection on SIP.

How to Get to This Page

Click **Configure > Security > Firewall > Firewall > Edit Firewall Policy > Select a rule > Edit > Application Inspection > Check SIP checkbox > button to right of field > Manage**.

Related Topics

- Application Inspection Dialog Box, page 23-27
- Configure SIP inspection based on header fields Dialog Box, page 23-32
- Configure SIP inspection based on status response patterns Dialog Box, page 23-34
- Manage H323 Messages Inspection Dialog Box, page 23-36

Field Reference

Table 23-8 Configure Deep Packet Inspection - SIP Dialog Box

Element	Description
Enter the maximum number of messages per second for invite request.	Enter the rate limit value in the range between 1 to 2147483647.
Enter the maximum number of messages per second for register request.	Enter the rate limit value in the range between 1 to 2147483647.
Permit or deny SIP traffic based on patterns in the header.	Click **Add**. The Configure SIP inspection based on header fields Dialog Box is displayed. Select a pattern and click **Edit**. The Enable SIP inspection based on status response Dialog Box is displayed. Select a pattern and click **Delete** if you want to delete a pattern.
Permit or deny SIP traffic based on status in the response.	Click **Add**. The Configure SIP inspection based on status response patterns Dialog Box is displayed. Select a pattern and click **Edit**. The Enable SIP inspection based on status response Dialog Box is displayed. Select a pattern and click **Delete** if you want to delete a pattern.
SIP traffic that does not conform to SIP protocol standards.	Check the checkbox to activate the options below it.

Table 23-8 Configure Deep Packet Inspection - SIP Dialog Box (continued)

Element	Description
Allow	Click the **Allow** radio button to allow entry of packets that do not conform to SIP protocol standards.
Drop	Click the **Drop** radio button to deny entry to packets that do not conform to SIP protocol standards.
Generate Logs	Check the **Generate Logs** checkbox to enable logging for either Allow or Drop operations.

Configure SIP inspection based on header fields Dialog Box

Use the **Configure SIP inspection based on header fields** dialog box to configure SIP inspection based on pattern in the header fields.

How to Get to This Page

Click **Configure > Security > Firewall > Firewall > Edit Firewall Policy > Select a rule > Edit > Application Inspection > Check SIP checkbox > button to right of field > Manage > Configure Deep Packet Inspection - SIP > Permit or deny SIP traffic based on patterns in the header > Add**.

Related Topics

- Enable SIP inspection based on status response Dialog Box, page 23-35
- Configure Deep Packet Inspection - SIP Dialog Box, page 23-30
- Configure SIP inspection based on status response patterns Dialog Box, page 23-34
- Enable SIP inspection based on status response Dialog Box, page 23-35

Field Reference

Table 23-9 Configure SIP inspection based on header fields Dialog Box

Element	Description
Select the message to inspect	Choose the kind of message to inspect from the drop-down list. You can choose request, response, or req-response.
Select the field of message to inspect	Choose the field in the header of the message that will be inspected. Each option can be chosen only once. For example, if you chose Accept-Language once, it is not displayed when you create the next pattern.
Pattern List	Click **Add**. The Add Pattern dialog box is displayed. Select a pattern and click **Edit**. The Edit Pattern dialog box is displayed. Select a pattern and click **Delete** to delete a pattern.
Take the following action	Choose Allow, Drop, or Rate-limit from the drop-down menu.
Enable Logging	Check the Enable Logging checkbox to generate logs of the inspection.

Enable SIP inspection based on header fields Dialog Box

Use the Enable SIP inspection based on header fields dialog box to edit the SIP inspection patterns configured through the Configure SIP inspection based on header fields Dialog Box.

How to Get to This Page

Click **Configure > Security > Firewall > Firewall > Edit Firewall Policy > Select a rule > Edit > Application Inspection > Check SIP checkbox > button to right of field > Manage > Configure Deep Packet Inspection - SIP > Edit**

Related Topics

- Configure SIP inspection based on header fields Dialog Box, page 23-32
- Configure Deep Packet Inspection - SIP Dialog Box, page 23-30
- Configure SIP inspection based on status response patterns Dialog Box, page 23-34
- Enable SIP inspection based on status response Dialog Box, page 23-35

Field Reference

Table 23-10 Enable SIP inspection based on header fields Dialog Box

Element	Description
Select the message to inspect	The message chosen while configuring the SIP inspection pattern is displayed.
Select the field of message to inspect	The field of message chosen while configuring the SIP inspection pattern is displayed.
Pattern List	Click **Add** to add a new pattern with the same parameters. The Add Pattern dialog box is displayed. Select a pattern and click **Edit** to edit a pattern. The Edit Pattern dialog box is displayed. Select a pattern and click **Delete** to delete a pattern.
Take the following action	The action associated with the pattern is displayed. You can change the action.
Enable Logging	The logging associated with the pattern is displayed. You can change it.

Configure SIP inspection based on status response patterns Dialog Box

Use the Configure SIP inspection based on status response patterns dialog box to configure SIP inspection based on pattern in the status response patterns.

How to Get to This Page

Click **Configure > Security > Firewall > Firewall > Edit Firewall Policy > Select a rule > Edit > Application Inspection > Check SIP checkbox > button to right of field > Manage > Configure Deep Packet Inspection - SIP > Permit or deny SIP traffic based on status in the response > Add**.

Related Topics

- Enable SIP inspection based on status response Dialog Box, page 23-35
- Configure Deep Packet Inspection - SIP Dialog Box, page 23-30
- Configure SIP inspection based on header fields Dialog Box, page 23-32
- Enable SIP inspection based on status response Dialog Box, page 23-35

Field Reference

Table 23-11 Configure SIP inspection based on status response patterns Dialog Box

Element	Description
Pattern List	Click **Add**. The Add Pattern dialog box is displayed. Select a pattern and click **Edit**. The Edit Pattern dialog box is displayed. Select a pattern and click **Delete** to delete a pattern.
Take the following action	Choose Allow, Drop, or Rate-limit from the drop-down menu.
Enable logging	Check the Enable Logging checkbox to generate logs of the inspection.

Enable SIP inspection based on status response Dialog Box

Use the Enable SIP inspection based on status response dialog box to edit the pattern list configured through the Configure SIP inspection based on status response patterns dialog box.

How to Get to This Page

Click **Configure > Security > Firewall > Firewall > Edit Firewall Policy > Select a rule > Edit > Application Inspection > Check SIP checkbox > button to right of field > Manage > Configure Deep Packet Inspection - SIP > Permit or deny SIP traffic based on status in the response > Edit**.

Related Topics

- Configure SIP inspection based on status response patterns Dialog Box, page 23-34
- Configure Deep Packet Inspection - SIP Dialog Box, page 23-30
- Configure SIP inspection based on header fields Dialog Box, page 23-32
- Enable SIP inspection based on status response Dialog Box, page 23-35

Field Reference

Table 23-12 Enable SIP inspection based on status response Dialog Box

Element	Description
Pattern List	Click **Add** to add a new pattern with the same parameters. The Add Pattern dialog box is displayed. Select a pattern and click **Edit** to edit a pattern. The Edit Pattern dialog box is displayed. Select a pattern and click **Delete** to delete a pattern.
Take the following action	The action associated with the pattern is displayed. You can change the action.
Enable Logging	The logging associated with the pattern is displayed. You can change it.

Manage H323 Messages Inspection Dialog Box

Use the Manage H323 Messages Inspection dialog box to define inspection parameters for H323 messages.

How to Get to This Page

Click **Application Inspection > Check H323 checkbox > button to right of field > Manage**.

Related Topics

- Application Inspection Dialog Box, page 23-27
- Configure Deep Packet Inspection - SIP Dialog Box, page 23-30

Field Reference

Table 23-13 Manage H323 Messages Inspection Dialog Box

Element	Description
Inspect Message	Check the checkbox against the parameter to apply. It is possible to select all the parameters.
Message Type	List of the type of messages.
Action on Message	Click **Allow**, **Drop**, or **Limit**. If you click **Limit**, enter a value in the field for the number of messages to be limited per second.
Log	Check the checkbox against the parameters to generate logs.

URL Filter

Add a URL filter by choosing an existing URL filter from the URL Filter Name list, or by clicking **Create New** and creating a new URL filter using the dialog boxes displayed. The settings for the URL filter that you chose or created are summarized in this dialog box.

Quality of Service

You can drop traffic that exceeds a specified rate per second, the police rate, and drop traffic that exceeds a specified burst value. The police rate can be a value between 8,000 and 2,000,000,000 bits per second. The burst rate can be a value between 1,000 and 512,000,000 bytes.

Inspect Parameter

Specify an existing parameter map in the Inspect Parameter window by choosing a parameter map in the Inspect Parameter Map list, or click **Create New** to create a new parameter map to apply to the rule for the policy you are modifying. The details of the parameter map that you specify are displayed in the Preview box.

To learn about parameter maps, see Timeouts and Thresholds for Inspect Parameter Maps and CBAC.

Select Traffic

Select a class map that specifies the traffic to add to the policy. To view more information about a particular class map, select the class map and click **View Details**.

When you click **OK**, the Add a New Rule dialog is displayed, with the information in the class map that you chose. You can make additional changes to the class map or leave it unchanged. If you do make changes, you can change the name of the class map if you do not want your changes to apply to other policies that use the original class map.

Delete Rule

This dialog box is displayed when you delete a rule that contains a class map or ACL that you might want to delete along with the rule or keep for use in other rules.

Automatically delete class maps and ACLs used by this rule

Click this option to remove the class maps and ACLs that are part of this rule. They are removed from the router configuration and not be available for use by other rules.

I will delete the unused class maps and ACLs later

Click this option to remove the rule but retain the class maps and ACLs. You can keep them for use in other parts of the firewall configuration.

View Details

Click **View Details** to display the names of the class maps and ACLs that are associated with the rule you are deleting. The dialog box expands to show the details. When you click View Details, the button name becomes Hide Details.

Hide Details

Click **Hide Details** to close the details portion of the dialog box. When you click Hide Details, the button name becomes View Details.

Manually Deleting Class Maps

To manually delete a class map, complete the following steps.

Step 1 Go to **Configure > Security > C3PL > Class Maps**.

Step 2 Click the node for the type of class map that you are deleting.

Step 3 Select the name of the class map that was displayed in the View Details window and click **Delete**.

Manually Deleting ACLs

To manually delete an ACL, complete the following steps.

Step 1 Go to **Configure > Router > ACL**.

Step 2 Click the node for the type of ACL that you are deleting.

Step 3 Select the name or number of the ACL that was displayed in the View Details window and click **Delete**.

CHAPTER 24

Zone-Based Policy Firewall

Zone-based policy firewall (also known as "Zone-Policy Firewall" or "ZPF") changes the firewall from the older interface-based model to a more flexible, more easily understood zone-based configuration model. Interfaces are assigned to zones, and an inspection policy is applied to traffic moving between the zones. Inter-zone policies offer considerable flexibility and granularity, so different inspection policies can be applied to multiple host groups connected to the same router interface.

A zone, or security zone, establishes a security border in your network. It defines a boundary where traffic is subjected to policy restrictions as it crosses to another region of your network. The interfaces in a zone should share common functions or features. For example, two interfaces that are connected to the local LAN might be placed in one security zone, and the interfaces connected to the Internet might be placed in another security zone.

For traffic entering one zone to be able to flow to another zone, for example *zone-inside* to *zone-outside*, the two zones must configured in a zone pair. Traffic can only flow in one direction between the zones in a zone pair. If you want traffic to flow in both directions between two zones, you must create a zone pair for each direction.

Configuration Task Order

The following tasks must be completed to configure a Zone-Based Policy Firewall:

- In the Zone window (see the Zone List help topic), define zones and assign interfaces.
- In the Zone Pairs window (see the Zone Pairs help topic), create the zone pairs that will govern traffic flow between zones.
- Define class-maps that describe traffic that must have policy applied as it crosses a zone pair. Refer to the Cisco Common Classification Policy Language section for more information.
- Define policy maps to apply action to your class-map's traffic. Policy maps are described in the Cisco Common Classification Policy Language section.
- Apply policy-maps to zone-pairs. See the Add or Edit a Zone Pair help topic for more information.

The sequence of tasks is not important, but some events must be completed in order. For instance, you must configure zones before you can configure zone pairs, and you must configure a class-map before you assign it to a policy-map. If you try to complete a task that relies on another portion of the configuration that you have not configured, Cisco CP does not allow you to do so.

For More Information

Zone-Based Policy General Rules in these help topics describes the rules governing interface behavior and the flow of traffic between zone-member interfaces.

For a good description of how Zone- Based Policy Firewall can be implemented, read *The Zone-Based Policy Firewall Design Guide* available on Cisco.com by going to **Support > Select a Product > Cisco IOS Software > Cisco IOS > Cisco IOS Software Release 12.4 Family > Software Releases 12.4 Mainline > Configure > Feature Guides** and clicking **Zone-Based Policy Firewall Design Guide**. This document may also be available at the following link:

http://www.cisco.com/en/US/products/sw/secursw/ps1018/products_tech_note09186a00808bc994.shtml

Zone List

This window displays the name of each security zone, the interfaces that it contains, and any associated zone pairs that the zone is a member of. A zone can be a member of multiple zone pairs.

Related Links

- Zone-Based Policy Firewall
- Configuration Task Order
- Zone-Based Policy General Rules
- Add a Zone
- Zone Pairs

Table 24-1 Zone List

Element	Description
Add	To create a new zone, click **Add**.
Edit	To choose different interfaces for an existing zone, choose the zone and click **Edit**
Delete	To delete a zone, choose the zone and click **Delete**. If you want to remove a zone that is a member of a zone pair, you must first delete the zone pair.
Name	The name of the zone.
Associated Interfaces	The router interfaces associated with the zone. You can change the interfaces associated with the zone by choosing the zone and clicking **Edit**. Each interface can be a member of only one zone.
Associated Zone Pairs	The zone pairs that the zone is a member of. A zone can be a member of multiple zone pairs.

Add or Edit a Zone

In this screen, create or edit a security zone.

Related Links

- Zone List
- Zone-Based Policy General Rules

Table 24-2 Add or Edit a Zone

Element	Description
Zone Name	In this field, enter a name for the zone. It is a good idea to use descriptive zone names, such as inside, outside, and DMZ. If you are editing a zone, this field is read-only.
Interface	This area lists the router interfaces. Check the box next to the interfaces that you want to associate with the zone. Because physical interfaces can be placed in only one zone, they do not appear in the list if they have already been placed in a zone. Virtual interfaces, such as Dialer interfaces or Virtual Template interfaces can be placed in multiple zones and will always appear in the list.

Note

- Traffic flowing to or from a chosen interface is governed by the policy map associated with the zone.
- An interface that you associate with this zone may be used for a site-to-site VPN, DMVPN, Easy VPN, SSL VPN or other type of connection whose traffic might be blocked by a firewall. When you associate an interface with a zone in this dialog, Cisco CP does not create any passthrough ACL to permit such traffic. You can configure the necessary passthrough for the policy map two ways.
  - Go to **Configure > Security > Firewall > Firewall > Edit Firewall Policy > Rule for New Traffic**. In the displayed dialog, provide the source and destination IP address information, and the type of traffic that must be allowed to pass through the firewall. In the Action field, select **Permit ACL**.
  - Go to **Configure > Security > C3PL > Policy Map > Protocol Inspection**. Provide a protocol inspection policy map that will allow the necessary traffic to pass through the firewall.

Zone-Based Policy General Rules

Router network interfaces' membership in zones is subject to several rules governing interface behavior, as is the traffic moving between zone member interfaces:

- A zone must be configured before interfaces can be assigned to the zone.
- An interface can be assigned to only one security zone.
- All traffic to/from a given interface is implicitly blocked when the interface is assigned to a zone, excepting traffic to/from other interfaces in the same zone, and traffic to any interface on the router.
- Traffic is implicitly allowed to flow by default among interfaces that are members of the same zone.
- To permit traffic to/from a zone member interface, a policy allowing or inspecting traffic must be configured between that zone and any other zone.

- The self zone is the only exception to the default deny-all policy. All traffic to any router interface is allowed until traffic is explicitly denied.
- Traffic cannot flow between a zone member interface and any interface that is not a zone member.
- Pass, inspect, and drop actions can only be applied between two zones.
- Interfaces that have not been assigned to a zone function as classical router ports and might still use classical stateful inspection/CBAC configuration.
- If it is required that an interface on the box not be part of the zoning/firewall policy, it might still be necessary to put that interface in a zone and configure a pass all policy (sort of a dummy policy) between that zone and any other zone to which traffic flow is desired.
- From the preceding it follows that, if traffic is to flow among all the interfaces in a router, all the interfaces must be part of the zoning model (each interface must be a member of one zone or another).
- The only exception to the preceding deny by default approach is the traffic to/from the router, which will be permitted by default. An explicit policy can be configured to restrict such traffic.

This set of rules was taken from *The Zone-Based Policy Firewall Design Guide* available at the following link:

http://www.cisco.com/en/US/products/ps6350/products_feature_guide09186a008072c6e3.html

Zone Pairs

A zone-pair allows you to specify a unidirectional firewall policy between two security zones. The direction of the traffic is specified by specifying a source and destination security zone.The same zone cannot be defined as both the source and the destination.

If you want traffic to flow in both directions between two zones, you must create a zone pair for each direction. If you want traffic to flow freely among all interfaces, each interface must be configured in a zone.

Related Links

- Zone-Based Policy Firewall
- Zone List
- Zone-Based Policy General Rules

Field Reference

Table 24-3 Zone Pairs

Element	Description
Buttons	To create a new zone pair, click **Add**. To edit an existing zone pair, choose the zone pair and click **Edit**. To remove a zone pair, choose the zone pair, and click **Delete**.
Zone Pair	The name of the zone pair.
Source	For the selected zone pair, the name of the zone from which traffic enters the router.
Destination	For the selected zone pair, the name of the zone to which traffic is sent.
Policy	The name of the policy applied to the zone pair.

Zone Pair Examples

The following table shows an example of four zone-pairs.

Zone Pair	Source	Destination	Policy
LAN-out	zone-VLAN1	zone-FE1	inspection-policymap-a
LAN-in	zone-FE1	zone-VLAN1	inspection-policymap-b
Bkup-out	self	zone-BRI0	inspection-policymap-c
Bkup-in	zone-BRI0	self	inspection-policymap-c

LAN-out and LAN-in are zone-pairs configured for traffic flowing between the LAN interface, VLAN1, and the FastEthernet 1 interface. Each zone-pair is controlled by a separate policy. Bkup-out and Bkup-in are configured for traffic generated by the router. The same policy controls traffic sent from zone-BRI0 as traffic sent by the router, represented by the self zone.

Add or Edit a Zone Pair

In this screen, create or edit a zone pair, and associate a policy map with the zone pair. If you are editing a zone pair, you can change the policy map, but you cannot change the name or the source or destination zones.

Related Links

- Zone List
- Zone Pairs
- Policy Map

Table 24-4 Add or Edit a Zone Pair

Element	Description
Zone Pair	In this field, enter a name for the zone pair. If you are editing a zone pair, this field is read-only.
Source zone	From this list, choose the source zone from which traffic is to originate. If you are editing a zone pair, this field is read-only. If the source zone is for traffic that originates from the router itself, such as SNMP, RIP, or EIGRP traffic, choose the zone self. This list only contains the zone self no user-created zones have been configured, and you must go to **Configure > Security > Firewall > Firewall Components > Zones** to create zones and then return to this screen to choose zones for the zone pair.
Destination zone	From this list, choose the source zone from which traffic is to originate. If you are editing a zone pair, this field is read-only. If the source zone is for traffic that is being sent to the router itself, choose the zone self. This list is empty if no zones have been configured.
Policy	From this list, choose the policy that you want to apply to the zone pair. The Policy list contains the name of each policy map configured on the router. If no policy maps are configured, this list is empty, and you must configure the policy map that you want to apply to this zone pair.

Add a Zone

In this screen, add and name a new security zone. This screen is displayed from the Association tab, and enables you to add a zone without leaving the interface edit dialogs.

Table 24-5 Add a Zone

Element	Description
Zone Name	Enter the name of the zone that you want to add. After you have created this zone, it will be available in the Select Zone screen in the, and you can associate the interface with it.

Associating an Interface With a Zone Created in the Add a Zone Screen

To associate an interface with a zone you created in this screen, do the following:

Step 1 In the Association tab, click the button to the right of the zone field.

Step 2 Choose **Select a Zone**.

Step 3 In the Select Zone screen, choose the zone that you created in this screen, and click **OK**. The interface is associated with the zone you created.

Note

- Traffic flowing to or from this interface is governed by the policy map associated with the zone.
- An interface that you associate with this zone may be used for a site-to-site VPN, DMVPN, Easy VPN, SSL VPN or other type of connection whose traffic might be blocked by a firewall. When you associate an interface with a zone in this dialog, Cisco CP does not create any passthrough ACL to permit such traffic. You can configure the necessary passthrough for the policy map two ways.
  - Go to **Configure > Security > Firewall > Firewall > Edit Firewall Policy > Rule for New Traffic**. In the displayed dialog, provide the source and destination IP address information, and the type of traffic that must be allowed to pass through the firewall. In the Action field, select **Permit ACL**.
  - Go to **Configure > C3PL > Policy Map > Protocol Inspection**. Provide a protocol inspection policy map that will allow the necessary traffic to pass through the firewall.

Select a Zone

If a security zone has been configured on the router, you can add the interface that you are configuring as a member of that zone.

Related Links

- Zone-Based Policy Firewall
- Association

Table 24-6 Select a Zone

Element	Description
Select a Zone for the Interface	To include the interface in a zone, select the zone that you want to include the interface in, and click **OK**.

CHAPTER 25

Site-to-Site VPN

The help topics in this section describe the Site-to-Site VPN configuration screens, and the VPN Design Guide screens.

VPN Design Guide

If you are an administrator setting up a VPN network, the VPN Design Guide helps you to determine which kind of VPN to configure. You provide information about what type of user you are, the type of equipment that the router establishes VPN connections with, the type of traffic that the VPN will carry, and other features that you need to configure. After you provide this information, the VPN Design Guide recommends a VPN type, and allows you to launch the wizard that will enable you to configure that type of VPN.

Create Site to Site VPN

A Virtual Private Network (VPN) lets you protect traffic that travels over lines that your organization may not own or control. VPNs can encrypt traffic sent over these lines and authenticate peers before any traffic is sent.

You can let Cisco Configuration Professional (Cisco CP) guide you through a simple VPN configuration by clicking the VPN icon. When you use the Wizard in the Create Site-to-Site VPN tab, Cisco CP provides default values for some configuration parameters in order to simplify the configuration process.

If you want to learn more about VPN technology, there is background information at the link More About VPN.

Create a Site-to-Site VPN

This option allows you to create a VPN network connecting two routers.

Create a Secure GRE Tunnel (GRE-over-IPSec)

This option allows you to configure a generic routing encapsulation protocol (GRE) tunnel between your router and a peer system.

What Do You Want to Do?

If you want to:	Do this:
Configure the router as part of a VPN network connecting two routers. When you configure a VPN network between two routers, you can control how the remote router is authenticated, how traffic is encrypted, and what traffic is encrypted.	Select **Create a site-to-site VPN** . Then click **Launch the selected task**.
Configure a GRE tunnel between your router and another router. You may want to configure a GRE tunnel if you need to connect networks that use different LAN protocols, or if you need to send routing protocols over the connection to the remote system.	Select Create a Secure GRE tunnel (GRE-over-IPSec). Then click **Launch the selected task**.

If you want to:	Do this:
Find out how to perform other VPN-related tasks that this wizard does not guide you through.	Select a topic from the following list: • How Do I View the IOS Commands I Am Sending to the Router? • How Do I Create a VPN to More Than One Site? • After Configuring a VPN, How Do I Configure the VPN on the Peer Router? • How Do I Edit an Existing VPN Tunnel? • How Do I Confirm That My VPN Is Working? • How Do I Configure a Backup Peer for My VPN? • How Do I Accommodate Multiple Devices with Different Levels of VPN Support? • How Do I Configure a VPN on an Unsupported Interface? • How Do I Configure a VPN After I Have Configured a Firewall? • How Do I Configure NAT Passthrough for a VPN? • How Do I Configure a DMVPN Manually?

If you want to:	Do this:
Configure an Easy VPN concentrator. Configuration instructions for Easy VPN servers and concentrators are available on www.cisco.com.	The document *Cisco Easy VPN Remote Phase II* provides guidelines to use when configuring a Cisco VPN 3000 series concentrator to operate with an Easy VPN Remote Phase II client. It is available at the following link: http://www.cisco.com/en/US/docs/ios/12_2/12_2y/12_2yj8/feature/guide/ftezvp2.html The following link connects you to Cisco VPN 3000 series documentation: http://www.cisco.com/en/US/products/hw/vpndevc/ps2284/products_getting_started_guide_book09186a00800bbe74.html

Site-to-Site VPN Wizard

You can have Cisco CP use default settings for most of the configuration values, or you can let Cisco CP guide you in configuring a VPN.

What do you want to do?

If you want to:	Do this:
Quickly configure a site-to-site VPN using Cisco CP-provided defaults.	Check **Quick setup**, and then click **Next**. Cisco CP will automatically provide a default IKE policy to govern authentication, a default transform set to control the encryption of data and a default IPSec rule that will encrypt all traffic between the router and the remote device. Quick setup is best used when both the local router and the remote system are Cisco routers using Cisco CP. Quick setup will configure 3DES encryption if it is supported by the IOS image. Otherwise, it will configure DES encryption. If you need AES or SEAL encryption, click **Step-by-step wizard**.
View the default IKE policy, transform set, and IPSec rule that will be used to configure a One-step VPN.	Click **View Defaults**.
Configure a site-to-site VPN using parameters that you specify.	Check **Step-by-Step wizard**, and then click **Next**. You can create a custom configuration for the VPN, and use any of the Cisco CP defaults that you need. Step-by-step wizard allows you to specify stronger encryption than the Quick setup wizard allows.

View Defaults

This window displays the default Internet Key Exchange (IKE) policy, transform set, and IPSec rule that Cisco CP will use to configure a Quick Setup site-to-site VPN. If you need a different configuration than this window shows, check **Step-by-Step wizard** so that you can define configuration values.

VPN Connection Information

Use this window to identify the IP address or host name of the remote site that will terminate the VPN tunnel that you are configuring, to specify the router interface to use, and to enter the pre-shared key that both routers will use to authenticate each other.

Select the interface for this VPN Connection

Select the interface on this router that connects to the remote site.The router you are configuring is represented as the Local router in the Use Case Scenario diagram.

Peer Identity

Enter the IP address of the remote IP Security (IPSec) peer that will terminate the VPN tunnel you are configuring. The remote IPSec peer might be another router, a VPN concentrator, or any other gateway device that supports IPSec.

Peer(s) with dynamic IP addresses

Select this option if the peers the router connects to use a dynamically-assigned IP addresses.

Peer with static IP address

Select this option if the peer the router connects to uses a fixed IP address.

Enter the IP Address of the remote peer

(Enabled when Peer with static IP address is selected). Enter the IP address of the remote peer.

Authentication

Click this button if the VPN peers use a pre-shared key to authenticate connections from each other. This key must be the same on each side of the VPN connection.

Enter the pre-shared key, and then reenter it for confirmation. Exchange the pre-shared key with the administrator of the remote site through some secure and convenient method, such as an encrypted e-mail message. Question marks (?) and spaces must not be used in the pre-shared key. The pre-shared key can contain a maximum of 128 characters.

Note

- The characters you enter for the pre-shared key are not displayed in the field as you enter them. You may find it helpful to write down the key before you enter it so that you can communicate it to the administrator of the remote system.
- Pre-shared keys must be exchanged between each pair of IPSec peers that need to establish secure tunnels. This authentication method is appropriate for a stable network with a limited number of IPSec peers. It may cause scalability problems in a network with a large or increasing number of IPSec peers.

Digital Certificate

Click this button if the VPN peers will use digital certificates for authentication.

Note The router must have a digital certificate issued by a Certificate Authority to authenticate itself. If you have not configured a digital certificate for the router, go to VPN components, and use the Digital Certificate wizard to enroll for a digital certificate.

Traffic to Encrypt

If you are configuring a Quick Setup site-to-site VPN connection, you need to specify the source and destination subnets in this window.

Source

Choose the interface on the router that will be the source of the traffic on this VPN connection. All traffic coming through this interface whose destination IP address is in the subnet specified in the Destination area will be encrypted.

Details

Click this button to obtain details about the interface you selected. The details window shows any access rules, IPSec policies, Network Address Translation (NAT) rules, or Inspection rules associated with the interface. To examine any of these rules in more detail, go to Additional Tasks/ACL Editor, and examine them in the Rules windows.

Destination

IP address and Subnet Mask. Enter the IP address and subnet mask of the destination for this traffic. For more information about how to enter values in these fields, see IP Addresses and Subnet Masks.

The destination is depicted as the Remote router in the Use Case Scenario diagram in the main VPN wizard window.

IKE Proposals

This window lists all the Internet Key Exchange (IKE) policies that have been configured on the router. If no user-defined policies have been configured, the windows lists the Cisco CP default IKE policy. IKE policies govern the way that devices in a VPN authenticate themselves.

The local router will use the IKE policies listed in this window to negotiate authentication with the remote router.

The local router and the peer device must both use the same policy. The router that initiates the VPN connection offers the policy with the lowest priority number first. If the remote system rejects that policy, the local router offers the policy with the next lowest number, and continues in this fashion until the remote system accepts. You must coordinate closely with the administrator of the peer system so that you can configure identical policies on both routers.

For Easy VPN connections, IKE policies are only configured on the Easy VPN server. The Easy VPN client sends proposals, and the server responds according to its configured IKE policies.

Priority

This is the order in which the policy will be offered during negotiation.

Encryption

Cisco CP supports a variety of encryption types, listed in order of security. The more secure an encryption type is, the more processing time it requires.

Note

- Not all routers support all encryption types. Unsupported types will not appear in the screen.
- Not all IOS images support all the encryption types that Cisco CP supports. Types unsupported by the IOS image will not appear in the screen.
- If hardware encryption is turned on, only those encryption types supported by hardware encryption will appear in the screen.

Cisco CP supports the following types of encryption:

- DES—Data Encryption Standard. This form of encryption supports 56-bit encryption.
- 3DES—Triple DES. This is a stronger form of encryption than DES, supporting 168-bit encryption.
- AES-128—Advanced Encryption Standard (AES) encryption with a 128-bit key. AES provides greater security than DES and is computationally more efficient than 3DES.
- AES-192—AES encryption with a 192-bit key.
- AES-256—AES encryption with a 256-bit key.

Hash

The authentication algorithm to be used for the negotiation. Cisco CP supports the following algorithms:

- SHA_1—Secure Hash Algorithm. A hash algorithm used to authenticate packet data.
- MD5—Message Digest 5. A hash algorithm used to authenticate packet data.

D-H Group

The Diffie-Hellman Group—Diffie-Hellman is a public-key cryptography protocol that allows two routers to establish a shared secret over an unsecure communications channel. Cisco CP supports the following groups:

- group1—D-H Group 1. 768-bit D-H Group.
- group2—D-H Group 2. 1024-bit D-H Group. This group provides more security than group 1, but requires more processing time.
- group5—D-H Group 5.1536-bit D-H Group. This group provides more security than group 2, but requires more processing time.

Authentication

The authentication method to be used. The following values are supported:

- PRE_SHARE—Authentication will be performed using pre-shared keys.
- RSA_SIG—Authentication will be performed using digital certificates.

Note You must choose the authentication type that you specified when you identified the interfaces that the VPN connection is using.

Type

Either Cisco CP Default or User Defined. If no User Defined policies have been created on the router, this window will show the default IKE policy.

To add or edit an IKE policy:

If you want to add an IKE policy that is not included in this list, click **Add** and create the policy in the window displayed. Edit an existing policy by selecting it and clicking **Edit**. Cisco CP Default policies are read only, and cannot be edited.

To accept the policy list:

To accept the IKE policy list and continue, click **Next**.

Transform Set

This window lists the Cisco CP-default transform sets and the additional transform sets that have been configured on this router. These transform sets will be available for use by the VPN or DMVPN. A transform set represents a certain combination of security protocols and algorithms. During the IPSec security association negotiation, the peers agree to use a particular transform set for protecting a particular data flow. A transform describes a particular security protocol with its corresponding algorithms.

You can select only one transform set in this window, but you can associate additional transform sets to the VPN or DMVPN connection using the VPN or DMVPN Edit tabs.

Select Transform Set

Select the transform set that you want to use from this list.

Details of the Selected Transform Set

This area supplies details about the selected transform set. Not all types of encryption, authentication, and compression have to be configured; therefore, some columns may not contain values.

To learn the possible values each column may contain, click **Add or Edit Transform Set**.

Name

The name given to this transform set.

ESP Encryption

The type of Encapsulating Security Protocol (ESP) encryption used. If ESP encryption is not configured for this transform set, this column will be empty.

ESP Authentication

The type of ESP authentication used. If ESP authentication is not configured for this transform set, this column will be empty.

AH Authentication

The type of Authentication Header (AH) authentication used. If AH authentication is not configured for this transform set, this column will be empty.

IP Compression

If IP compression is configured for this transform set, this field contains the value COMP-LZS.

Note IP compression is not supported on all routers.

Mode

This column contains one of the following:

- Transport—Encrypt data only. Transport mode is used when both endpoints support IPsec. Transport mode places the authentication header or encapsulated security payload after the original IP header; thus, only the IP payload is encrypted. This method allows users to apply network services such as quality-of-service (QoS) controls to encrypted packets.
- Tunnel—Encrypt data and IP header. Tunnel mode provides stronger protection than transport mode. Because the entire IP packet is encapsulated within AH or ESP, a new IP header is attached, and the entire datagram can be encrypted. Tunnel mode allows network devices such as routers to act as an IPsec proxy for multiple VPN users.

Type

Either User Defined, or Cisco CP Default.

What Do You Want to Do?

If you want to:	Do this:
Select a transform set for the VPN to use.	Select a transform set, and click **Next**.
Add a transform set to the router's configuration.	Click **Add**, and create the transform set in the Add Transform Set window. Then click **Next** to continue VPN configuration.

If you want to:	Do this:
Edit an existing transform set.	Select a transform set, and click **Edit**. Then, edit the transform set in the Edit Transform Set window. After editing the transform set, click **Next** to continue VPN configuration. Cisco CP Default transform sets are read only and cannot be edited.
Associate additional transform sets with this VPN.	Select one transform set in this window, and complete the VPN wizard. Then, associate other transform sets to the VPN in the Edit tab.

Traffic to Protect

This window lets you define the traffic that this VPN protects. The VPN can protect traffic between specified subnets, or protect the traffic specified in an IPSec rule that you select.

Protect All Traffic Between the Following Subnets

Use this option to specify a single source subnet (a subnet on the LAN) whose outgoing traffic you want to encrypt, and one destination subnet supported by the peer that you specified in the VPN Connection window.

All traffic flowing between other source and destination pairs will be sent unencrypted.

Source

Enter the address of the subnet whose outgoing traffic you want to protect, and specify the subnet mask. For more information, refer to Available Interface Configurations.

All traffic from this source subnet that has a destination IP address on the destination subnet will be protected.

Destination

Enter the address of the destination subnet, and specify the mask for that subnet. You can select a subnet mask from the list, or type in a custom mask. The subnet number and mask must be entered in dotted decimal format, as shown in the previous examples.

All traffic going to the hosts in this subnet will be protected.

Create/Select an access-list for IPSec traffic

Use this option if you need to specify multiple sources and destinations, and/or specific types of traffic to encrypt. An IPSec rule can consist of multiple entries, each specifying different traffic types and different sources and destinations.

Click the button next to the field, and specify an existing IPSec rule that defines the traffic you want to encrypt, or create an IPSec rule to use for this VPN. If you know the number of the IPSec rule, enter it in the box to the right. If you do not know the number of the rule, click the **...** button and browse for the rule. When you select the rule, the number will appear in the box.

Note Because they can specify traffic type, and both source and destination, IPSec rules are extended rules. If you enter the number or name of a standard rule, a Warning message is displayed indicating that you have entered the name or number of a standard rule.

Any packets that do not match the criteria in the IPSec rule are sent with no encryption.

Summary of the Configuration

This window shows you the VPN or DMVPN configuration that you created. You can review the configuration in this window and use the back button to make changes if you want.

Spoke Configuration

If you have configured a DMVPN hub, you can have Cisco CP generate a procedure that will assist you or other administrators in configuring DMVPN spokes. The procedure explains which options to select in the wizard, and what information to enter in spoke configuration windows. You can save this information to a text file that you or another administrator can use.

Test the connectivity after configuring

Click to test the VPN connection you have just configured.The results of the test will be shown in another window.

To save this configuration to the router's running configuration and leave this wizard:

Click **Finish.** Cisco CP saves the configuration changes to the router's running configuration. The changes will take effect immediately, but will be lost if the router is turned off.

If you checked **Preview commands before delivering to router** in the Cisco CP Preferences window, the Deliver window will appear. In this window, you can view the CLI commands you that are delivering to the router.

Spoke Configuration

This window contains information that you can use to give a spoke router a configuration that will be compatible with the DMVPN hub that you configured. It lists the windows you need to complete, giving you data that you need to enter in the window so that the spoke will be able to communicate with the hub.

It provides the following data that you need to input into the spoke configuration:

- The hub's public IP address. This is the IP address of the hub interface that supports the mGRE tunnel.
- The IP address of the hub's mGRE tunnel.
- The subnet mask that all tunnel interfaces in the DMVPN must use.
- The advanced tunnel configuration information.
- The routing protocol to use, and any information associated with the protocol, such as Autonomous System number (for EIGRP), and OSPF Process ID.
- The hash, encryption, DH group, and Authentication Type of the IKE policies that the hub uses, so that compatible IKE policies can be configured on the spoke.
- The ESP and Mode information of the transform sets that the hub uses. If similar transform sets have not been configured on the spoke, they can be configured using this information.

Secure GRE Tunnel (GRE-over-IPSec)

Generic routing encapsulation (GRE) is a tunneling protocol developed by Cisco that can encapsulate a wide variety of protocol packet types inside IP tunnels, creating a virtual point-to-point link to Cisco routers at remote points over an IP internetwork. By connecting multi-protocol subnetworks in a single-protocol backbone environment, IP tunneling using GRE allows network expansion across a single-protocol backbone environment.

This wizard enables you to create a GRE tunnel with IPSec encryption. When you create a GRE tunnel configuration, you also create an IPSec rule that describes the endpoints of the tunnel.

GRE Tunnel Information

General GRE tunnel information is provided in this screen.

Tunnel Source

Select the interface name or the IP address of the interface that the tunnel will use. The IP address of the interface must be reachable from the other end of the tunnel; therefore it must a a public, routable IP address. An error will be generated if you enter an IP address that is not associated with any configured interface.

Note Cisco CP lists interfaces with static IP addresses and interfaces configured as unnumbered in the Interface list. Loopback interfaces are not included in the list.

Details

Click to obtain details about the interface that you selected. The details window shows any access rules, IPSec policies, NAT rules, or Inspection rules associated with the interface. If a NAT rule has been applied to this interface that causes the address to be unroutable, the tunnel will not operate properly. To examine any of these rules in more detail, go to Additional Tasks/ACL Editor and examine the in the Rules window.

Tunnel Destination

Enter the IP address of the interface on the remote router at the other end of the tunnel. This is the source interface from the point of view of the other end of the tunnel.

Make sure that this address is reachable by using the **ping** command. The **ping** command is available from the Tools menu. If the destination address cannot be reached, the tunnel will not be created properly.

IP Address of the GRE tunnel

Enter the IP address of the tunnel. The IP addresses of both ends of the tunnel must be in the same subnet. The tunnel is given a separate IP address so that it can be a private address, if necessary.

IP Address

Enter the IP address of the tunnel in dotted decimal format. For more information, see IP Addresses and Subnet Masks.

Subnet Mask

Enter the subnet mask for the tunnel address in dotted decimal format.

VPN Authentication Information

VPN peers use a pre-shared key to authenticate connections from each other. This key must be the same on each side of the VPN connection.

Pre-Shared Key

Click this button if the VPN peers use a pre-shared key for authentication and then enter the pre-shared key, and then reenter it for confirmation. Exchange the pre-shared key with the administrator of the remote site through some secure and convenient method, such as an encrypted e-mail message. Question marks (?) and spaces must not be used in the pre-shared key.

Note

- The characters that you enter for the pre-shared key are not displayed in the field as you enter them. You may find it helpful to write down the key before you enter it so that you can communicate it to the administrator of the remote system.
- Pre-shared keys must be exchanged between each pair of IPSec peers that need to establish secure tunnels. This authentication method is appropriate for a stable network with a limited number of IPSec peers. It may cause scalability problems in a network with a large or increasing number of IPSec peers.

Digital Certificate

Click this button if the VPN peers will use digital certificates for authentication.

The router must have a digital certificate issued by a Certificate Authority to authenticate itself. If you have not configured a digital certificate for the router, go to VPN components, and use the Digital Certificate wizard to enroll for a digital certificate.

Note If you are authenticating using digital certificates, the VPN tunnel might not be created if the CA server contacted during IKE negotiation is not configured to respond to Certificate Revocation List (CRL) requests. To correct this problem, go to the Digital Certificates page, select the configured trustpoint, and select None for Revocation.

Backup GRE Tunnel Information

You can configure a backup GRE-over-IPSec tunnel that the router can use when the primary tunnel fails. This tunnel will use the same interface that you configured for the primary tunnel, but it must be configured with the backup VPN router as the peer. If routing is configured for the primary GRE-over-IPSec tunnel, the keepalive packets that the routing protocol sends are used to verify that the tunnel is still active. If the router stops receiving keepalive packets on the primary tunnel, then traffic is sent through the backup tunnel.

Create a backup secure GRE tunnel for resilience

Check this box if you want to create a backup tunnel.

IP address of the backup GRE tunnel's destination

Enter the IP address of the interface on the remote router at the other end of the tunnel. (This is the source interface from the point of view of the other end of the tunnel.)

Make sure that this address is reachable by using the **ping** command. The **ping** command is available from the Tools menu. If the destination address specified in the Ping dialog cannot be reached, the tunnel will not be created properly.

Tunnel IP address

Enter the IP address of the tunnel. The IP addresses of both ends of the tunnel must be in the same subnet. The tunnel is given a separate IP address so that it can be a private address, if necessary.

IP Address

Enter the IP address of the tunnel in dotted decimal format. For more information, see IP Addresses and Subnet Masks.

Subnet Mask

Enter the subnet mask for the tunnel address in dotted decimal format.

Routing Information

This window enables you to configure routing for the tunneled traffic. Information that you add in this window appears in the Routing window. Changes that you make in the Routing window may affect routing of VPN traffic. Configuring routing enables you to specify the networks that will participate in the GRE-over-IPSec VPN. Additionally, if you configure a backup GRE-over-IPSec tunnel, the keepalive packets sent by routing protocols allow the router to determine whether the primary tunnel has failed.

Select a dynamic routing protocol if this router is being used in a large VPN deployment with a large number of networks in the GRE over IPSec VPN. Select static routing if a small number of networks will participate in the VPN.

EIGRP

Check this box to use the Enhanced Interior Gateway Routing Protocol (EIGRP) protocol to route traffic. Then click **Next** to specify which networks will participate in the GRE-over-IPSec VPN in the Routing Information window.

OSPF

Check this box to use the Open Shortest Path First protocol (OSPF) to route traffic. Then click **Next** to specify which networks will participate in the GRE-over-IPSec VPN in the Routing Information window.

RIP

Check this box to use the Routing Information Protocol(RIP) to route traffic. Then click **Next** to specify which networks will participate in the GRE-over-IPSec VPN in the Routing Information window.

Note This option is not available when you configure a backup GRE-over-IPSec tunnel.

Static Routing

Static routing can be used in smaller VPN deployments in which only a few private networks participate in the GRE-over-IPSec VPN. You can configure a static route for each remote network so that traffic destined for the remote networks will pass through the appropriate tunnels.

Static Routing Information

You can configure a static route for each remote network so that traffic destined for the remote networks will pass through the appropriate tunnels. Configure the first static route in the Static Routing Information window. If you need to configure additional static routes, you can do so in the Routing window.

Check this box if you want to specify a static route for the tunnel, and select one of the following:

- **Tunnel all traffic**—All traffic will be routed through the tunnel interface and encrypted. Cisco CP creates a default static route entry with the tunnel interface as the next hop.

  If a default route already exists, Cisco CP modifies that route to use the tunnel interface as the next hop, replacing the interface that was originally there, and creates a new static entry to the tunnel destination network that specifies the interface in the original default route as the next hop.

  The following example assumes the network at the other end of the tunnel is 200.1.0.0, as specified in the destination network fields:

  ```
  ! Original entry
  ip route 0.0.0.0  0.0.0.0 FE0
  ! Entry changed by SDM
  ip route 0.0.0.0  0.0.0.0 Tunnel0
  ! Entry added by SDM
  ip route 200.1.0.0  255.255.0.0 FE0
  ```

  If no default route exists, Cisco CP simply creates one, using the tunnel interface as the next hop. For example:

  ```
  ip route 0.0.0.0  0.0.0.0 Tunnel0
  ```

- **Do split tunneling**—Split tunneling allows traffic that is destined for the network specified in the IP Address and Network Mask fields to be encrypted and routed through the tunnel interface. All other traffic will not be encrypted. When this option is selected, Cisco CP creates a static route to the network, using the IP address and network mask.

  The following example assumes that the network address 10.2.0.0/255.255.0.0 was entered in the destination address fields:

  ```
  ip route 10.2.0.0 255.255.0.0 Tunnel0
  ```

  When split tunneling is selected, the IP Address and Subnet Mask fields will appear, requiring you to enter the IP Address and Subnet Mask of the destination peer. You must ensure that the destination IP address entered in the Tunnel Destination field of the GRE Tunnel Information window is reachable. If it is not reachable, no tunnel will be established.

IP Address

Enabled with split tunneling. Enter the IP address of the network at the other end of the tunnel. Cisco CP will create a static route entry for the packets with a destination address in that network. This field is disabled when **Tunnel all traffic** is selected.

You must ensure that the IP address entered in this field is reachable before you configure this option. If it is not reachable, no tunnel will be established.

Network Mask

Enabled with split tunneling. Enter the network mask used on the network at the other end of the tunnel. This field is disabled when **Tunnel all traffic** is selected.

Select Routing Protocol

Use this window to specify how other networks behind your router are advertised to the other routers in the network. Select one of the following:

- EIGRP—Extended Interior Gateway Routing Protocol.
- OSPF—Open Shortest Path First.
- RIP—Routing Internet Protocol.
- Static Routing. This option is enabled when you are configuring a GRE over IPSec tunnel.

Note RIP is not supported for DMVPN Hub and spoke topology but is available for DMVPN Full Mesh topology.

Summary of Configuration

This screen summarizes the GRE configuration that you have completed. You can review the information in this screen and click the back button to return to any screen in which you want to make changes. If you want to save the configuration, click **Finish**.

GRE tunnel configuration creates an IPSec rule that specifies which hosts the GRE traffic will be allowed to flow between. This IPSec rule is displayed in the summary.

To save this configuration to the router's running configuration and leave this wizard:

Click **Finish**. Cisco CP saves the configuration changes to the router's running configuration. The changes will take effect immediately, but will be lost if the router is turned off.

If you checked **Preview commands before delivering to router** in the Cisco CP Preferences window, the Deliver window will appear. In this window, you can view the CLI commands you that are delivering to the router.

Edit Site-to-Site VPN

Virtual Private Networks (VPNs) let you protect data between your router and a remote system by encrypting traffic so that it cannot be read by others who are using the same public network. In effect, it gives you the protection of a private network over public lines that may be used by other organizations.

Use this window to create and manage VPN connections to remote systems. You can create, edit, and delete VPN connections, and reset existing connections. You can also use this window to configure your router as an Easy VPN client with connections to one or more Easy VPN servers or concentrators.

Click the link for the part of the window for which you want help:

Site-to-Site VPN Connections

VPN connections, sometimes referred to as *tunnels*, are created and managed from the VPN Connections box. A VPN connection links a router interface to one or more peers specified by a crypto map defined in an IP Security (IPSec) policy.You can view, add, edit, and delete the VPN connections in this list.

Status column

The status of the connection, which is indicated by the following icons:

 The connection is up.

The connection is down.

The connection is being established.

Interface

The router interface that is connected to the remote peers in this VPN connection. An interface can be associated with only one IPSec policy. The same interface will appear on multiple lines if there is more than one crypto map defined for the IPSec policy used in this connection.

Description

A short description of this connection.

IPSec Policy

The name of the IPSec policy used in this VPN connection. The IPSec policy specifies how data is encrypted, which data will be encrypted, and where data will be sent. For more information, click More about VPN Connections and IPSec Policies.

Sequence Number

The sequence number for this connection. Because an IPSec policy may be used in more than one connection, the combination of the sequence number and IPSec policy name uniquely identifies this VPN connection. The sequence number does not prioritize the VPN connection; the router will attempt to establish all configured VPN connections regardless of sequence number.

Peers

The IP addresses or host names of the devices at the other end of the VPN connection. When a connection contains multiple peers, their IP addresses or host names are separated by commas. Multiple peers might be configured to provide alternative routing paths for the VPN connection.

Transform Set

This shows the name of the transform set used by this VPN connection. Multiple transform set names are separated by commas. A transform set specifies the algorithms that will be used to encrypt data, ensure data integrity, and provide

data compression. Both peers must use the same transform set, and they negotiate to determine which set they will use. Multiple transform sets may be defined to ensure that the router can offer a transform set that the negotiating peer will agree to use. The transform sets is a component of the IPSec policy.

IPSec Rule

The rule that determines which traffic should be encrypted on this connection. The IPSec rule is a component of the IPSec Policy.

Type

One of the following:

- Static—This is a static site-to-site VPN tunnel. The VPN tunnel uses static crypto maps.
- Dynamic—This is a dynamic site-to-site VPN tunnel. The VPN tunnel uses dynamic crypto maps.

Add Button

Click to add a VPN connection

Delete Button

Click to delete a selected VPN connection

Test Tunnel.. Button

Click to test a selected VPN tunnel.The results of the test will be shown in another window.

Clear Connection Button

Click to reset an established connection to a remote peer. This button is disabled if you have selected a dynamic site-to-site VPN tunnel.

Generate Mirror..Button

Click to create a text file that captures the VPN configuration of the local router so that a remote router can be given a VPN configuration that enables it to establish a VPN connection to the local router. This button is disabled if you have selected a dynamic site-to-site VPN tunnel.

Note Any previously configured VPN connections detected by Cisco CP that do not use ISAKMP crypto maps will appear as read-only entries in the VPN connection table and cannot be edited.

Add new connection

Use this window to add a new VPN connection between the local router and a remote system, referred to as a *peer*. You create the VPN connection by associating an IPSec policy with an interface.

To create a VPN connection:

Step 1 Select the interface you want to use for the VPN from the Select Interface list. Only interfaces that are not used in other VPN connections are shown in this list.

Step 2 Select a policy from the Choose IPSec Policy list. Click **OK** to return to the VPN Connections window.

Add Additional Crypto Maps

Use this window to add a new crypto map to an existing IPSec policy. This window shows the interface associated with the VPN connection that you selected in the VPN Connections window, the IPSec policy associated with it, and the crypto maps that the policy already contains.

The crypto map specifies a sequence number, the peer device at the other end of the connection, the set of transforms that encrypt the traffic, and the IPSec rule that determines which traffic is encrypted.

Note Adding a crypto map to an existing IPSec policy is the only way to add a VPN tunnel to an interface that is already being used in an existing VPN connection.

Interface

This is the interface used in this VPN connection.

IPSec Policy

This is the name of the IPSec policy controlling the VPN connection. The crypto maps making up the IPSec policy are shown in the list below this field. For more information, click More about VPN Connections and IPSec Policies.

What Do You Want to Do?

If you want to:	Do this:
Configure the crypto map yourself.	Click **Add New Crypto Map** and use the Add Crypto Map window to create the new crypto map. Click **OK** when you are finished. Then click **OK** in this window.
Have Cisco Configuration Professional (Cisco CP) help you add a new crypto map to this connection.	Check the **Use Add Wizard** box, and click **OK**. Cisco CP will guide you in creating a new crypto map, and will associate it with the IPSec policy.

Crypto Map Wizard: Welcome

This wizard will guide you through the creation of a crypto map. A crypto map specifies the peer devices at the other end of the VPN connection, defines how traffic will be encrypted, and identifies which traffic will be encrypted.

Click **Next** to begin creating a crypto map.

Crypto Map Wizard: Summary of the configuration

The Cryptomap wizard summary page displays the data you entered in the wizard windows. You can review it, click Back to return to a screen to make changes, and then return to the Summary window and click **Finish** to deliver the cryptomap configuration to the router.

Delete Connection

Use this window to delete a VPN tunnel, or simply to disassociate it from an interface but preserve the definition for future use.

Delete the crypto map with sequence number *n* from IPSec policy *policy name*

Click this button, and then click **OK** to remove the VPN tunnel definition. The associations created between the interface, IPSec policy, and peer devices will be lost when you do this. If more than one interface has been associated with this tunnel definition, those associations are deleted as well.

Delete the dynamic crypto map with sequence number *n* from the dynamic crypto map set *set name*

This button is shown if you selected a dynamic site-to-site VPN tunnel. Click this button, and then click **OK** to remove the VPN tunnel definition. The associations created between the interface, IPSec policy, and peer devices will be lost when you do this. If more than one interface has been associated with this tunnel definition, those associations are deleted as well.

Disassociate the IPSec policy *policy name* from the interface *interface name,* and keep the IPSec policy for possible future reuse

Click this button, and then click **OK** to retain the tunnel definition but remove its association with the interface. You will be able to associate this definition with another router interface if you wish.

Generate Mirror...

This window shows you the IPSec policy used for the VPN tunnel to the selected peer, and allows you to save the policy in a text file that you can use when configuring the VPN connection on the peer device.

Peer Device

Select the IP address or host name of the peer device to see the IPSec policy configured for the tunnel to that device. The policy appears in the box under the peer IP address.

To create a text file of the IPSec policy:

Click **Save**, and specify a name and location for the text file. You can give this text file to the administrator of the peer device so that he or she can create a policy that mirrors the one you created on the router. Click **After Configuring a VPN, How Do I Configure the VPN on the Peer Router?** to learn how to use the text file to create a mirror policy.

Caution The text file that you generate must not be copied into the configuration file of the remote system, but must be used only to show what has been configured on the local router so that the remote device can be configured in a way that is compatible. Identical names for IPSec policies, IKE policies, and transform sets may be used on the remote router, but the policies and transform sets may be different. If the text file is simply copied into the remote configuration file, configuration errors are likely to result.

Cisco CP Warning: NAT Rules with ACL

This window appears when you are configuring a VPN using interfaces with associated NAT rules that use Access rules. This type of NAT rule can change IP addresses in packets before the packets leave or enter the LAN, and a NAT rule will prevent VPN connections from functioning properly if it changes source IP addresses so that they don't match the IPSec rule configured for the VPN. To prevent this from happening, Cisco CP can convert these to NAT rules that use route maps. Route maps specify subnets that should not be translated.

The window shows the NAT rules that have to be changed to ensure the VPN connection functions properly.

Original Address

The IP address that NAT will translate.

Translated Address

The IP address that NAT will substitute for the original address.

Rule Type

The type of NAT rule, either Static or Dynamic.

To make the listed NAT rules use route maps:

Click **OK**.

How Do I...

This section contains procedures for tasks that the wizard does not help you complete.

How Do I Create a VPN to More Than One Site?

You can use Cisco CP to create multiple VPN tunnels on one interface on your router. Each VPN tunnel will connect the selected interface on your router to a different subnet at the destination router. You can configure multiple VPN tunnels to connect to the same interface but to different subnets on the destination router, or you can configure multiple VPN tunnels that will connect to different interfaces on the destination router.

First, you must create the initial VPN tunnel. The steps below describe how to create the initial VPN tunnel. If you have already created your first VPN tunnel and need to add an additional tunnel to the same interface, skip the first procedure and perform the steps in the next procedure in this help topic.

Create the initial VPN tunnel:

Step 1 From the Feature bar, choose **Configure > Security > VPN > Site-to-Site VPN**.

Step 2 Choose **Create a Site-to-Site VPN**.

Step 3 Click **Launch the Selected Task**.

The VPN Wizard starts.

Step 4 Click **Quick Setup**.

Step 5 Click **Next>**.

Step 6 From the Select the Router Interface for this VPN Connection field, choose the interface on the source router on which to create the VPN tunnel. This is the interface connected to the Internet on the Local system in the Use Case Scenario diagram.

Step 7 In the Peer Identity field, enter the IP address of the destination router interface.

Step 8 In the Authentication fields, enter and reenter the pre-shared key that the two VPN peers will use.

Step 9 In the Source field, select the interface that connects to the subnet whose IP traffic you want to protect. This is the Local router in the Use Case Scenario diagram, and is usually an interface connected to the LAN.

Step 10 In the Destination fields, enter the IP address and subnet mask of the destination router.

Step 11 Click **Next>**.

Step 12 Click **Finish**.

Create an Additional Tunnel from the Same Source Interface

After you have created the initial VPN tunnel, follow these steps to create an additional tunnel from the same source interface to a different destination interface or destination subnet:

Step 1 From the Feature bar, choose **Configure > Security > VPN > Site-to-Site VPN**.

Step 2 Choose **Create a Site-to-Site VPN**.

Step 3 Click **Launch the Selected Task**.

The VPN Wizard starts.

Step 4 Click **Quick Setup**.

Step 5 Click **Next>**.

Step 6 From the Select the Router Interface for this VPN Connection field, choose the same interface that you used to create the initial VPN connection.

Step 7 In the Peer Identity field, enter the IP address of the destination router interface. You can enter the same IP address that you entered when you created the initial VPN connection. This indicates that this second VPN connection should use the same interface on the destination router as the initial VPN connection. If you do not want both VPN connections to connect to the same destination interface, enter the IP address of a different interface on the destination router.

Step 8 In the Authentication fields, enter and reenter the pre-shared key that the two VPN peers will use.

Step 9 In the Source field, select the same interface used to create the initial VPN connection.

Step 10 In the Destination fields, you have the following options:

- If, in the Peer Identity field, you entered the IP address of a different interface on the destination router and want to protect the IP traffic coming from a specific subnet, enter the IP address and subnet mask of that subnet in the appropriate fields.
- If you entered the same IP address in the Peer Identity field as you used for the initial VPN connection, indicating that this VPN tunnel will use the same router interface as the initial VPN tunnel, then enter the IP address and subnet mask of the new subnet that you want to protect in the appropriate fields.

Step 11 Click **Next>**.

Step 12 Click **Finish**.

After Configuring a VPN, How Do I Configure the VPN on the Peer Router?

Cisco CP generates VPN configurations on your router. Cisco CP includes a function that will generate a text file of the configuration that can be used as a template to create a VPN configuration for the peer router to which your VPN tunnel connects. This text file can only be used as a template that shows you which commands need to be configured. It cannot be used without editing because it contains information that is only correct for the local router you configured.

To generate a template configuration for the peer VPN router:

Step 1 From the Feature bar, choose **Configure > Security > VPN > Site-to-Site VPN**.

Step 2 Click **Edit Site-to-Site VPN**.

Step 3 Select the VPN connection that you want to use as a template, and click **Generate Mirror**.

Cisco CP displays the Generate Mirror screen.

Step 4 From the Peer Device field, select the IP address of the peer device for which you want to generate a suggested configuration.

The suggested configuration for the peer device appears on the Generate Mirror screen.

Step 5 Click **Save** to display the Windows Save File dialog box, and save the file.

Caution Do not apply the mirror configuration to the peer device without editing! This configuration is a template that requires additional manual configuration. Use it only as a starting point to build the configuration for the VPN peer.

Step 6 After saving the file, use a text editor to make any needed changes to the template configuration. These are some commands that may need editing:

- The peer IP address command(s)
- The transform policy command(s)
- The crypto map IP address command(s)
- The ACL command(s)

- The interface ip address command(s)

Step 7 After you have finished editing the peer configuration file, deliver it to the peer router using a TFTP server.

How Do I Edit an Existing VPN Tunnel?

To edit an existing VPN tunnel:

Step 1 From the Feature bar, choose **Configure > Security > VPN > Site-to-Site VPN**.

Step 2 Click **Edit Site-to-Site VPN**.

Step 3 Click the connection that you want to edit.

Step 4 Click **Add.**

Step 5 Select **Static crypto maps to <policy name>**

Step 6 In the Add static crypto maps window, you can add more crypto maps to the VPN connection.

Step 7 If you need to modify any of the components of the connection, such as the IPSec policy or the existing crypto map, note the names of those components in the VPN window, and go to the appropriate windows under VPN Components to make changes.

How Do I Confirm That My VPN Is Working?

You can verify that your VPN connection is working by using the Monitor mode in Cisco CP. If your VPN connection is working, Monitor mode will display the VPN connection by identifying the source and destination peer IP addresses. Depending on whether your VPN connection is an IPSec tunnel or an Internet Key Exchange (IKE) security association (SA), Monitor mode will display the number of packets transferred across the connection, or show the current state of the connection. To display the current information about a VPN connection:

Step 1 From the Feature bar, choose **Monitor > Security**.

Step 2 Choose **VPN Status**.

Step 3 Choose **IPSec tunnels** or **IKE SAs**.

Each configured VPN connection will appear as a row on the screen.

If you are viewing IPSec tunnel information, you can verify the following information to determine that your VPN connection is working:

- The local and remote peer IP addresses are correct, indicating that the VPN connection is between the correct sites and router interfaces.
- The tunnel status is "up." If the tunnel status is "down" or "administratively down," then the VPN connection is not active.
- The number of encapsulation and decapsulation packets is not zero, indicating that data has been transferred over the connection and that the sent and received errors are not too high.

If you are viewing IKE SA information, you can verify that your VPN connection is working by verifying that the source and destination IP addresses are correct, and that the state is "QM_IDLE," indicating that the connection has been authenticated and that data transfer can take place.

How Do I Configure a Backup Peer for My VPN?

To configure multiple VPN peers inside a single crypto map:

Step 1 From the Feature bar, choose **Configure > Security > VPN > VPN Components > IPSec**.

Step 2 Choose **IPSec Policies**.

Step 3 In the IPSec Policies table, click the IPSec policy to which you want to add another VPN peer.

Step 4 Click **Edit**.

The Edit IPSec Policy dialog box appears.

Step 5 Click **Add**.

Step 6 The Add Crypto Map dialog box appears, letting you set the values for the new crypto map. Set the values for the new crypto map, using all four tabs in the dialog box. The Peer Information tab contains the Specify Peers field, which lets you enter the IP address of the peer you want to add.

Step 7 When you have finished, click **OK**.

The crypto map with the new peer IP address appears in the "Crypto Maps in this IPSec Policy" table.

Step 8 To add additional peers, repeat Step 4 through Step 8.

How Do I Accommodate Multiple Devices with Different Levels of VPN Support?

To add multiple transform sets to a single crypto map:

Step 1 From the Feature bar, choose **Configure > Security > VPN > VPN Components**.

Step 2 Choose **IPSec Policies**.

Step 3 In the IPSec Policies table, click the IPSec policy that contains the crypto map to which you want to add another transform set.

Step 4 Click **Edit**. The Edit IPSec Policy dialog box appears.

Step 5 In the "Crypto Maps in this IPSec Policy" table, click the crypto map to which you want to add another transform set.

Step 6 Click **Edit**. The Edit Crypto Map dialog box appears.

Step 7 Click the **Transform Sets** tab.

Step 8 In the Available Transform Sets field, click a transform set that you want to add to the crypto map.

Step 9 Click **>>** to add the selected transform set to the crypto map.

Step 10 If you want to add additional transform sets to this crypto map, repeat Step 9 and Step 10 until you have added all the transform sets you want.

Step 11 Click **OK**.

How Do I Configure a VPN on an Unsupported Interface?

Cisco CP can configure a VPN over an interface type unsupported by Cisco CP. Before you can configure the VPN connection, you must first use the router CLI to configure the interface. The interface must have, at a minimum, an IP address configured, and it must be working. To verify that the connection is working, verify that the interface status is "Up."

After you have configured the unsupported interface using the CLI, you can use Cisco CP to configure your VPN connection. The unsupported interface will appear in the fields that require you to choose an interface for the VPN connection.

How Do I Configure a VPN After I Have Configured a Firewall?

In order for a VPN to function with a firewall in place, the firewall must be configured to permit traffic between the local and remote peer IP addresses. Cisco CP creates this configuration by default when you configure a VPN configuration after you have already configured a firewall.

How Do I Configure NAT Passthrough for a VPN?

If you are using NAT to translate addresses from networks outside your own and if you are also connecting to a specific site outside your network via a VPN, you must configure NAT passthrough for your VPN connection, so that network address translation does not take place on the VPN traffic. If you have already configured NAT on your router and are now configuring a new VPN connection using Cisco CP, you will receive a warning message informing you that Cisco CP will configure NAT so that it does not translate VPN traffic. You must accept the message so that Cisco CP will create the necessary ACLs to protect your VPN traffic from translation.

If you are configuring NAT using Cisco CP and you have already configured a VPN connection, perform the following procedure to create ACLs.

Step 1 From the Feature bar, choose **Configure > Router > ACL**.

Step 2 In the Rules tree, choose **ACL Editor**.

Step 3 Click **Add**.

The Add a Rule dialog box appears.

Step 4 In the Name/Number field, enter a unique name or number for the new rule.

Step 5 From the Type field, choose **Extended Rule**.

Step 6 In the Description field, enter a short description of the new rule.

Step 7 Click **Add**.

The Add an Extended Rule Entry dialog box appears.

Step 8 In the Action field, choose **Permit**.

Step 9 In the Source Host/Network group, from the Type field, select **A Network**.

Step 10 In the IP Address and Wildcard Mask fields, enter the IP address and subnet mask of the VPN source peer.

Step 11 In the Destination Host/Network group, from the Type field, select **A Network**.

Step 12 In the IP Address and Wildcard Mask fields, enter the IP address and subnet mask of the VPN destination peer.

Step 13 In the Description field, enter a short description of the network or host.

Step 14 Click **OK**.

The new rule now appears in the Access Rules table.

CHAPTER 26

Easy VPN Remote

Cable modems, xDSL routers, and other forms of broadband access provide high-performance connections to the Internet, but many applications also require the security of VPN connections that perform a high level of authentication and that encrypt the data between two particular endpoints. However, establishing a VPN connection between two routers can be complicated and typically requires tedious coordination between network administrators to configure the VPN parameters of the two routers.

The Cisco Easy VPN Remote feature eliminates much of this tedious work by implementing Cisco Unity Client Protocol, which allows most VPN parameters to be defined at a Cisco IOS Easy VPN server. This server can be a dedicated VPN device, such as a Cisco VPN 3000 concentrator or a Cisco PIX Firewall or a Cisco IOS router that supports the Cisco Unity Client Protocol.

After the Cisco Easy VPN server has been configured, a VPN connection can be created with minimal configuration on an Easy VPN remote, such as a Cisco 800 series router or a Cisco 2800 series router. When the Easy VPN remote initiates the VPN tunnel connection, the Cisco Easy VPN server pushes the IPsec policies to the Easy VPN remote and creates the corresponding VPN tunnel connection.

The Cisco Easy VPN Remote feature provides for automatic management of the following details:

- Negotiating tunnel parameters, such as addresses, algorithms, and lifetime.
- Establishing tunnels according to the parameters that were set.
- Automatically creating the NAT or Port Address Translation (PAT) and associated access lists that are needed, if any.

- Authenticating users, that is, ensuring that users are who they say they are by way of usernames, group names, and passwords.
- Enabling VPN access through a firewall. You can use Cisco Configuration Professional (CP) to configure your router to use Cisco Tunneling Control Protocol (CTCP) to enable encrypted traffic to go through a firewall.

Note The Enable Easy VPN Access Through Firewall feature is supported on Cisco routers that are running Cisco IOS Release 12.4(20)T and later.

- Managing security keys for encryption and decryption.

Cisco CP provides a wizard that guides you through Easy VPN Remote configuration. You can also edit an existing configuration using Easy VPN Remote edit screens.

This chapter contains the following sections:

- Creating an Easy VPN Remote Connection
- Administering Easy VPN Remote Connections
- Other Procedures

Creating an Easy VPN Remote Connection

Create an Easy VPN Remote connection by using the Easy VPN Remote wizard. Complete these steps:

Step 1 On the Cisco CP toolbar, click **Configure**.

Step 2 On the Cisco CP category bar, click **VPN**.

Step 3 In the VPN tree, choose **Easy VPN Remote**.

Step 4 In the Create Easy VPN Remote tab, complete any recommended tasks that are displayed by clicking the link for the task. Cisco CP either completes the task for you, or displays the necessary configuration screens for you to make settings in.

Step 5 Click **Launch Easy VPN Remote Wizard** to begin configuring the connection.

Step 6 Make configuration settings in the wizard screens. Click **Next** to go from the current screen to the next screen. Click **Back** to return to a screen you have previously visited.

Step 7 Cisco CP displays the Summary screen when you have completed the configuration. Review the configuration. If you need to make changes, click **Back** to return to the screen in which you need to make changes, then return to the Summary screen.

Step 8 If you want to test the connection after sending the configuration to the router, check **Test the connectivity after configuring**. After you click **Finish**, Cisco CP tests the connection and displays the test results in another screen.

Step 9 To send the configuration to the router, click **Finish**.

The section Create Easy VPN Remote Reference contains detailed information about the screens you use.

Create Easy VPN Remote Reference

The following topics describe the Create Easy VPN Remote screens:

- Create Easy VPN Remote
- Configure an Easy VPN Remote Client
- Easy VPN Remote Wizard: Network Information
- Easy VPN Remote Wizard: Identical Address Configuration
- Easy VPN Remote Wizard: Interfaces and Connection Settings
- Easy VPN Remote Wizard: Server Information
- Easy VPN Remote Wizard: Authentication
- Easy VPN Remote Wizard: Automatic Firewall Bypass
- Easy VPN Remote Wizard: Summary of Configuration

Create Easy VPN Remote

Cisco CP allows you to configure your router as a client to an Easy VPN server or concentrator. Your router must be running a Cisco IOS software image that supports Easy VPN Phase II. The Create Easy VPN Remote tab enables you to launch the Easy VPN Remote wizard.

To be able to complete the configuration, you must have the following information ready.

- Easy VPN server's IP address or hostname
- IPSec group name
- Key
- Whether or not there are devices on the local network with IP addresses that conflict with addresses used in networks that the Easy VPN Remote client will connect to.

Field Reference

Table 26-1 Create Easy VPN Remote Tab Felds

Element	Description
Use Case Scenario	This area displays a network diagram that depicts the type of connection that the wizard enables you to configure.
Recommended Tasks	This area describes recommended tasks to complete before beginning the Easy VPN Remote configuration. Click the link for a particular task to complete it. If the Cisco IOS image on the router is version 12.4(9)T or later, Cisco CP displays the recommended task Enable DNS if DNS is not enabled on the router so that a Split DNS configuration, if pushed by the server, will work.
Launch Easy VPN Remote Wizard	Click **Launch Easy VPN Remote Wizard** to start the wizard.

Configure an Easy VPN Remote Client

This wizard guides you through the configuration of an Easy VPN Remote Phase II Client.

Note If the router is not running a Cisco IOS image that supports Easy VPN Remote Phase II or later, you will not be able to configure an Easy VPN client.

Easy VPN Remote Wizard: Network Information

Indicate whether or not there are IP addresses in the local network that overlap with IP addresses in networks that the router connects to through the Easy VPN server in this screen. Also, indicate if there are devices on the local network that must be reached from those networks.

Note This screen is displayed when the Cisco IOS image on the router is version 12.4(11)T or later.

Field Reference

Table 26-2 Network Information Fields

Element	Description
Client IP Addressing	
Does your client location have an addressing scheme that might overlap with other client locations?	Yes—Click **Yes** if devices on your local network use IP addresses that are also used by devices in other networks that the router will connect to through the Easy VPN Server. For example, printers on the local network may use IP addresses that are used by devices in the peer network. If you click Yes, Cisco CP displays the Device Reachability fields. No—Click **No** if devices on the local network do not use IP addresses that are also used in networks that the router connects to through the Easy VPN server.

Table 26-2 Network Information Fields (continued)

Element	Description
Device Reachability	
Do you have devices at your client location that must be reached from the server-side networks or other client locations?	Yes—Click **Yes** if there are devices on the local network, such as printers, that must be reached from networks that the router connects to through the Easy VPN server. No—Click **No** if there are no devices that must be reached from networks that the router connects to through the Easy VPN server.

Easy VPN Remote Wizard: Identical Address Configuration

Enter the local and global IP addresses of the devices that must be reached from networks that the router connects to through the Easy VPN server in this screen.

Field Reference

Table 26-3 Identical Address Configuration Fields

Element	Description
Accessible Devices	
Device Local IP	The local IP address of a device that is identified as a device that must be reached by other networks.
Device Global IP	The global IP address given to a device that is identified as a device that must be reached by other networks. Because the global IP address for each device must be routable from the Easy VPN server, you must obtain these addresses from the Easy VPN server administrator. Each IP address must be on the same subnet, and one address must be reserved for use by non accessible devices on the local network.
Add	To add the local IP address and global IP address of a device, click **Add**.
Edit	To change the IP address information for a device, choose an entry and click **Edit**.
Delete	To remove an entry for an accessible device, choose the entry and click **Delete**.
Non Accessible Devices	

Table 26-3 Identical Address Configuration Fields (continued)

Element	Description
IP Address	Enter the IP address that you reserved for non accessible devices in this field. This IP address must be in the same subnet as the device global IP addresses. Cisco CP creates a NAT rule to translate IP addresses of devices that do not need to be reached from other networks to this IP address, and assigns this IP address to a new loopback interface.
Subnet Mask	Enter the subnet mask in decimal format; for example, 255.255.255.0. Or, choose the number of subnet bits; for example, 24. Entering values in one field updates the other. For example, if you enter 255.255.255.0, the subnet bits field is automatically updated to display 24.

Warning Messages

Cisco CP displays a warning message when you click **Next** if it detects any of the following problems:

- There are no devices added.
- If you enter an IP address for the non accessible devices that is already used by a router interface.
- If you enter an IP address for the non accessible devices that is already used as a global IP address for an accessible device.
- If you enter local IP address for a device that falls outside the subnet for the LAN interface it connects to.

Easy VPN Remote Wizard: Interfaces and Connection Settings

In this window, you specify the interfaces that will be used in the Easy VPN configuration.

Field Reference

Table 26-4 Interfaces and Connection Settings Fields

Element	Description
Interfaces	
Choose the inside and outside interfaces in this box.	

Table 26-4 Interfaces and Connection Settings Fields

Element	Description
Check boxes	Check the inside (LAN) interfaces that serve the local networks that you want to include in this Easy VPN configuration. You can choose multiple inside interfaces, with the following restrictions: • If you choose an interface that is already used in another Easy VPN configuration, you are told that an interface cannot be part of two Easy VPN configurations. • If you choose interfaces that are already used in a VPN configuration, you are informed that the Easy VPN configuration you are creating cannot coexist with the existing VPN configuration. You will be asked if you want to remove the existing VPN tunnels from those interfaces and apply the Easy VPN configuration to them. • An existing interface does not appear in the list of interfaces if it cannot be used in an Easy VPN configuration. For example, loopback interfaces configured on the router do not appear in this list. • An interface cannot be designated as both an inside and an outside interface. Up to three inside interfaces are supported on Cisco 800 and Cisco 1700 series routers. You can remove interfaces from an Easy VPN configuration in the Edit Easy VPN Remote window.
Interface List	In the Interfaces list, choose the outside interface that connects to the Easy VPN server or concentrator. **Note** Cisco 800 routers do not support the use of interface E 0 as the outside interface.
Connection Settings	

Table 26-4 Interfaces and Connection Settings Fields

Element	Description
Automatically	With the automatic setting, the VPN tunnel is established automatically when the Easy VPN configuration is delivered to the router configuration file. However, you will not be able to control the tunnel manually in the VPN Connections window. The Connect or Disconnect button is disabled when this Easy VPN connection is chosen.
Manually	With the manual setting, you must click the **Connect** or **Disconnect** button in the Edit Easy VPN Remote window to establish or take down the tunnel, but you will have full manual control over the tunnel in the Edit Easy VPN Remote window. Additionally, if a security association (SA) timeout is set for the router, you will have to manually reestablish the VPN tunnel whenever a timeout occurs. You can change SA timeout settings in the VPN Components VPN Options window.
When there is traffic from local networks (interesting traffic)	With the traffic-based setting, the VPN tunnel is established whenever outbound local (LAN side) traffic is detected.  **Note** The option for traffic-based activation appears only if supported by the Cisco IOS image on your router.

Easy VPN Remote Wizard: Server Information

The information entered in this window identifies the Easy VPN tunnel, the Easy VPN server or concentrator that the router will connect to, and the way you want traffic to be routed in the VPN.

Field Reference

Table 26-5 Server Information Fields

Element	Description
Easy VPN Servers	
Easy VPN Server 1	Enter the IP address or the hostname of the primary Easy VPN server or concentrator to which the router will connect. If you enter a hostname, there must be a Domain Name System (DNS) server on the network that can resolve the hostname to the correct IP address for the peer device.
Easy VPN Server 2	The Easy VPN Server 2 field appears when the Cisco IOS image on the router supports Easy VPN Remote Phase III. This field does not appear when the Cisco IOS image does not support Easy VPN Remote Phase III. Enter the IP address or the hostname of the secondary Easy VPN server or concentrator to which the router will connect. If you enter a hostname, there must be a DNS server on the network that can resolve the hostname to the correct IP address for the peer device.
Mode of operation with no identical addressing	
Client	Choose **Client** if you want the PCs and other devices on the router's inside networks to form a private network with private IP addresses. Network Address Translation (NAT) and Port Address Translation (PAT) will be used. Devices outside the LAN will not be able to ping devices on the LAN, or reach them directly.
Network Extension	Choose **Network Extension** if you want the devices connected to the inside interfaces to have IP addresses that are routable and reachable by the destination network. The devices at both ends of the connection will form one logical network. PAT will be automatically disabled, allowing the PCs and hosts at both ends of the connection to have direct access to one another.
	Consult with the administrator of the Easy VPN server or concentrator before choosing this setting.

Table 26-5 Server Information Fields (continued)

Element	Description
	If you choose Network Extension, you can enable remote management of the router by checking the box to request a server-assigned IP address for your router. This IP address can be used for connecting to your router for remote management and troubleshooting (ping, Telnet, and Secure Shell). This mode is known as **Network Extension Plus** **Note** If the router is not running a Cisco IOS image that supports Easy VPN Remote Phase IV or later, you will not be able to set Network Extension Plus.
Mode of operation with overlapping address space and local devices needing to be reached	
If you clicked **Yes** in the Client IP Addressing section of the Network Information screen, and also clicked **Yes** in the Device Reachability section, the router is automatically configured for Network Extension mode.	
Have the server assign an IP address to manage my router remotely	Check this box if you want the Easy VPN server to assign an IP address to the router so that it can manage the router Easy VPN operation remotely.
Mode of operation with overlapping address space but no devices needing to be reached	
If you clicked **Yes** in the Client IP Addressing section of the Network Information screen, but clicked **No** in the Device Reachability section, the router is automatically configured for Client mode. The Easy VPN server automatically assigns the router an IP address so that it can manage the router Easy VPN operation remotely. All devices on the local network will share this IP address when communicating with other devices on the corporate network.	

Easy VPN Remote Wizard: Authentication

Use this window to specify security for the Easy VPN Remote tunnel.

Field Reference

Table 26-6 Authentication Screen Fields

Element	Description
Device Authentication	
Authentication	Choose **Digital Certificate** or **Preshared Key**.
Digital Certificate	If you choose digital certificate, a digital certificate must be configured on the router to use. **Note** The Digital Certificates option is available only if supported by the Cisco IOS image on your router.
Preshared Key	If you choose **Preshared Key** in the authentication field, you must supply a user group name as well as the preshared key.
User Group	Enter the IPSec group name. The group name must match the group name defined on the VPN concentrator or server. Obtain this information from your network administrator.
Key	Enter the IPSec group key. The group key must match the group key defined on the VPN concentrator or server. Obtain this information from your network administrator.
Reenter key	Reenter the key to confirm its accuracy.
User Authentication	
User authentication (XAuth) appears in this window if the Cisco IOS image on the router supports Easy VPN Remote Phase III. If user authentication does not appear, it must be configured from the router command-line interface.	
From PC browser when browsing	User authentication will be performed in the web browser. This option appears only if supported by the Cisco IOS image on your router.
From router console or Cisco CP	User authentication will be performed from the router console, or from Cisco CP.

Table 26-6 Authentication Screen Fields

Element	Description
Save XAuth Credentials to this router	The Easy VPN server may use XAuth to authenticate the router. If the server allows the save password option, you can eliminate the need to enter the username and password each time the Easy VPN tunnel is established by this option. Enter the username and password provided by the Easy VPN server administrator, and then reenter the password to confirm its accuracy. The information is saved in the router configuration file and used each time the tunnel is established. **Caution** Storing the XAuth username and password in router memory creates a security risk, because anyone who has access to the router configuration can obtain this information. If you do not want this information stored on the router, do not enter it here. The Easy VPN server will simply challenge the router for the username and password each time the connection is established. Additionally, Cisco CP cannot itself determine whether the Easy VPN server allows the save password option. You must determine whether the server allows this option. If the server does not allow this option, you should not create a security risk by entering the information here.
Username	Enter the username required for authentication.
Password	Enter the password required for authentication.
Reenter password	Reenter the password to confirm accuracy.

Easy VPN Remote Wizard: Automatic Firewall Bypass

Use the Automatic Firewall Bypass page to enable Easy VPN access through a firewall.

An Easy VPN tunnel network might not work if there is a firewall between the router and the VPN server that blocks VPN protocols such as Internet Key Exchange (IKE) and Extended Services Protocol (ESP). You can use Cisco CP to configure your router to use Cisco Tunneling Control Protocol (CTCP) to enable encrypted traffic to go through the firewall.

Note The Enable Easy VPN Access Through Firewall feature is supported on Cisco routers that are running Cisco IOS Release 12.4(20)T and later.

How to Get to This Page

1. Go to **Configure > Security > VPN > Easy VPN Remote**. The **Create Easy VPN Remote** tab is selected by default.
2. Click **Launch Easy VPN Remote Wizard** to start the Easy VPN Remote wizard pages.
3. Click **Next** until you reach the Automatic Firewall Bypass page.

Related Topics

- Create Easy VPN Remote, page 26-4
- Add or Edit Easy VPN Remote: Firewall Bypass, page 26-40

Field Reference

Table 26-7 Automatic Firewall Summary Bypass Page

Element	Description
Enable Easy VPN Access Through Firewall check box	Check this check box to configure the router to use Cisco Tunneling Control Protocol (CTCP) so that encrypted traffic can go through the firewall. Cisco CP configures the default port number as 10000 and the default keepalive value as 5 seconds. To change the default values, see Add or Edit Easy VPN Remote: Firewall Bypass, page 26-40.

Easy VPN Remote Wizard: Summary of Configuration

This window shows you the Easy VPN configuration that you have created, and it allows you to save the configuration. A summary similar to the following appears:

```
Easy VPN tunnel name:test1
Easy VPN server: 222.28.54.7
Group: myCompany
Key: 1234
Control: Auto
Mode: Client
Outside Interface: BVI222
Inside Interfaces: Dialer0
```

You can review the configuration in this window and click the **Back** button to change any items.

Clicking the **Finish** button writes the information to the router's running configuration, and, if the tunnel has been configured to operate in automatic mode, the router attempts to contact the VPN concentrator or server.

If you want to change the Easy VPN configuration at a later time, you can make the changes in the Edit Easy VPN Remote window.

Note In many cases, your router establishes communication with the Easy VPN server or concentrator after you click **Finish**, or after you click **Connect** in the Edit Easy VPN Remote window or VPN Connections windows. However, if the device has been configured to use XAuth, it challenges the router for a username and password. When this happens, you must first supply a Secure Shell (SSH) login ID and password to log on to the router and then provide the XAuth login and password for the Easy VPN server or concentrator. You must follow this process when you click **Finish** and the configuration is delivered to the router, and when you disconnect and then reconnect the tunnel in the Edit Easy VPN Remote window. Find out whether XAuth is used, and determine the required username and password.

Test VPN Connectivity

If you choose to test the VPN connection you have just configured, the results of the test are shown in another window.

Administering Easy VPN Remote Connections

Use Cisco CP to edit Easy VPN Remote connection settings, reset connections, and delete connections. You can use the Easy VPN Remote Edit screens to create an Easy VPN Remote connection, but it is recommended that you use the wizard to do so.

This section contains the following topics:

- Editing an Existing Easy VPN Remote Connection
- Creating a New Easy VPN Remote Connection
- Deleting an Easy VPN Remote Connection
- Resetting an Established Easy VPN Remote Connection
- Connecting to an Easy VPN Server
- Connecting other Subnets to the VPN Tunnel
- Editing CTCP Port Number and Keepalive Values
- Administering Easy VPN Remote Reference

Editing an Existing Easy VPN Remote Connection

Follow these steps to edit an existing Easy VPN Remote connection:

Step 1 On the Cisco CP Feature bar, click **Configure > Security > VPN**.

Step 2 In the VPN tree, choose **Easy VPN Remote**.

Step 3 Click the **Edit Easy VPN Remote** tab.

Step 4 Select the Easy VPN Remote connection that you want to edit.

Step 5 Click **Edit**.

Step 6 Modify settings in the **Edit Easy VPN Remote** dialog tabs.

Step 7 Click **OK** to send the changes to the router and close the dialog.

Creating a New Easy VPN Remote Connection

You can create a new Easy VPN Remote connection using the Easy VPN Remote Edit screens.

Follow these steps to create a new Easy VPN Remote connection:

Step 1 On the Cisco CP Feature bar, click **Configure > Security > VPN**.

Step 2 In the VPN tree, choose **Easy VPN Remote**.

Step 3 Click the **Edit Easy VPN Remote** tab.

Step 4 Click **Add**.

Step 5 Make settings in the **Add Easy VPN Remote** dialog tabs.

Step 6 Click **OK** to send the changes to the router and close the dialog.

Deleting an Easy VPN Remote Connection

Follow these steps to delete an Easy VPN Remote connection:

Step 1 On the Cisco CP Feature bar, click **Configure > Security > VPN**.

Step 2 In the VPN tree, choose **Easy VPN Remote**.

Step 3 Click the **Edit Easy VPN Remote** tab.

Step 4 Select the Easy VPN Remote connection that you want to delete.

Step 5 Click **Delete**.

Step 6 Confirm the deletion by clicking **OK** in the displayed message screen.

Resetting an Established Easy VPN Remote Connection

Follow these steps to reset an established Easy VPN Remote connection:

Step 1 On the Cisco CP Feature bar, click **Configure > Security > VPN**.

Step 2 In the VPN tree, choose **Easy VPN Remote**.

Step 3 Click the **Edit Easy VPN Remote** tab.

Step 4 Select the Easy VPN Remote connection that you want to reset.

Step 5 Click **Reset Connection**. The status window that is displayed reports the success or failure of the reset.

Connecting to an Easy VPN Server

Follow these steps to connect to an Easy VPN Remote server:

Step 1 On the Cisco CP Feature bar, click **Configure > Security > VPN**.

Step 2 In the VPN tree, choose **Easy VPN Remote**.

Step 3 Click the **Edit Easy VPN Remote** tab.

Step 4 Select an Easy VPN Remote connection.

Step 5 Click **Connect** to complete the connection to the configured Easy VPN Server.

Connecting other Subnets to the VPN Tunnel

To allow subnets not directly connected to your router to use the tunnel, follow these steps:

Step 1 In the Network Extensions Options window, check **Configure Multiple Subnets**.

Step 2 Choose **Enter the subnets** and add the subnets and network masks to the list, or choose **Select an ACL**.

Step 3 To enter the subnets manually, click the **Add** button and enter the subnet address and mask. Cisco CP will generate an ACL automatically.

Note The subnets you enter must *not* be directly connected to the router.

Step 4 To add an existing ACL, enter its name or choose it from the drop-down list.

Step 5 Click **OK** to close the dialog.

Editing CTCP Port Number and Keepalive Values

Use this procedure to edit existing CTCP port number and keepalive values.

Before You Begin

Make sure that the router is configured with a WAN interface on which Easy VPN Remote is configured.

Procedure

Step 1 Go to **Configure > Security > VPN > Easy VPN Remote**.

Step 2 Click the **Edit Easy VPN Remote** tab.

Step 3 Select the Easy VPN Remote connection that you want to edit.

Step 4 Click **Edit**. The Edit Easy VPN Remote page opens, which contains several tabs.

Step 5 Click the **Firewall Bypass** tab. The Automatic Firewall Bypass page opens. See Add or Edit Easy VPN Remote: Firewall Bypass, page 26-40.

Step 6 In the Port Number field, change the port number on which you want to configure CTCP. Valid port numbers are 1 to 65535.

Step 7 In the Keepalive field, change the keepalive value (in seconds) by which you want to end keepalives, so that NAT or firewall sessions do not time out. Valid keepalive values are 5 to 3600 seconds.

Step 8 Click **OK** to send the changes to the router and close the dialog.

Related Topics

- Creating an Easy VPN Remote Connection, page 26-2
- Easy VPN Remote Wizard: Automatic Firewall Bypass, page 26-14
- Add or Edit Easy VPN Remote: Firewall Bypass, page 26-40

Administering Easy VPN Remote Reference

The following topics describe the Edit Easy VPN Remote screens:

- Edit Easy VPN Remote
- Add or Edit Easy VPN Remote
- Add or Edit Easy VPN Remote: General Settings
- Network Extension Options
- Add or Edit Easy VPN Remote: Easy VPN Settings
- Add or Edit Easy VPN Remote: Authentication Information
- Add or Edit Easy VPN Remote: Easy VPN Client Phase III Authentication
- Add or Edit Easy VPN Remote: Interfaces and Connections
- Add or Edit Easy VPN Remote: Firewall Bypass
- Add or Edit Easy VPN Remote: Identical Addressing
- Easy VPN Remote: Add a Device
- Enter SSH Credentials
- XAuth Login Window

Edit Easy VPN Remote

Easy VPN connections are managed from this window. An Easy VPN connection is a connection configured between an Easy VPN client and an Easy VPN server or concentrator to provide for secure communications with other networks that the server or concentrator supports.

The list of connections displays information about the configured Easy VPN Remote connections.

Field Reference

Table 26-8 Edit Easy VPN Remote Fields

Element	Description
Add	Click **Add** to create a new Easy VPN Remote connection.
Edit	Choose an Easy VPN Remote connection, and click **Edit** to modify connection settings.
Delete	Choose an Easy VPN Remote connection, and click **Delete** to delete the connection.
Reset Connection	Choose an Easy VPN Remote connection, and click **Reset Connection** to clear the current security association (SA) and create a new one to reset the connection.
Test Tunnel	Choose an Easy VPN Remote connection, and click **Test Tunnel** to send data through the VPN tunnel. Cisco CP displays a message indicating the results of the test.
Connect or Disconnect or Login	The name of this button changes based on the status of the chosen Easy VPN Remote connection.
	This button is labeled Connect if all of the following are true: • The connection uses manual tunnel control. • The tunnel is down. • The XAuth response is *not* set to be requested from a PC browser session. Click **Connect** to establish the connection. This button is labeled Disconnect if all of the following are true: • The connection uses manual tunnel control. • The tunnel is up. • The XAuth response is *not* set to be requested from a PC browser session. Click **Disconnect** to terminate the connection.

Table 26-8 Edit Easy VPN Remote Fields

Element	Description
	This button is labeled Login if all of the following are true: • The Easy VPN server or concentrator being connected to uses XAuth. • The XAuth response is set to be requested from Cisco CP or the router console. • The tunnel is waiting for XAuth credentials (the connection has been initiated). Click **Login** to login to the Easy VPN server and establish the connection. If the connection is set to automatic or traffic-based tunnel control, this button is disabled.
Status	
	The connection is up. When an Easy VPN connection is up, the Disconnect button enables you to deactivate the connection if manual tunnel control is used.
	The connection is down. When an Easy VPN connection is down, the Connect button enables you to activate the connection if manual tunnel control is used.
	The connection is being established. Xauth Required—The Easy VPN server or concentrator requires an XAuth login and password. Use the Login button to enter the login ID and password and establish the connection. Configuration Changed—The configuration for this connection has been changed, and needs to be delivered to the router. If the connection uses manual tunnel control, use the Connect button to establish the connection.
Name	The name given to this Easy VPN connection.

Table 26-8 Edit Easy VPN Remote Fields

Element	Description
Mode	Either **client** or **network extension**. In client mode, the VPN concentrator or server assigns a single IP address to all traffic coming from the router; devices outside the LAN have no direct access to devices on the LAN. In network extension mode, the VPN concentrator or server does not substitute IP addresses, and it presents a full routable network to the peers on the other end of the VPN connection.
Details Choose an Easy VPN Remote connection from the list to see the values of the following settings for that connection.	
Authentication	Digital certificates or preshared key. The preshared key option shows the user group sharing the key.
Outside Interface	This is the interface that connects to the Easy VPN server or concentrator.
Inside Interfaces	These are the inside interfaces included in this Easy VPN connection. All hosts connected to these interfaces are part of the VPN.
Easy VPN Server	The names or IP addresses of the Easy VPN servers or concentrators. If the Cisco IOS image on your router supports Easy VPN Remote Phase III, you can identify two Easy VPN servers or concentrators during configuration using Cisco CP.
Multiple Subnet Support	The addresses of subnets which are not directly connected to the router but which are allowed to use the tunnel. An ACL defines the subnets allowed to use the tunnel.

Table 26-8 Edit Easy VPN Remote Fields

Element	Description
Tunnel Activation	The value is Auto, Manual, or traffic-based. If the connection is configured with the Manual setting, you must click **Connect** to establish the tunnel, but you can start or stop the tunnel at any time by clicking **Connect** or **Disconnect**. If the connection is configured with the Auto setting, the VPN tunnel is established automatically when the Easy VPN configuration is delivered to the router configuration file. However, the Connect or Disconnect button is not enabled for this connection. If the connection is configured with the traffic-based setting, the VPN tunnel is established automatically when inside traffic qualifies for outside routing. However, the Connect or Disconnect button is not enabled for this connection.
Backup Connection	A backup Easy VPN remote connection that has been set up. Backup connections are configured in the Cisco CP Interfaces and Connections task.
XAuth Response Method	If XAuth is enabled, the Item Value column shows one of the following about how the XAuth credentials are sent: • They must be entered from Cisco CP or the router console. • They must be entered from a PC browser when browsing. • The credentials are automatically sent because they have been saved on the router.
Identical Addressing	If identical addressing is configured, the Item Value column displays the word Configured," and the name, IP address, and number of subnet bits for the interface, for example, Loopback1 (20.20.20.1/24).
Split DNS	If split DNS is configured, the Item Value column displays the word Enabled, and the following information: • Domain names sent to corporate DNS servers • Corporate DNS servers pushed from Server • Internet DNS servers Multiple values are separated by commas.

Add or Edit Easy VPN Remote

Use this window to configure your router as an Easy VPN client. Your router must have a connection to an Easy VPN concentrator or server on the network.

Note This window appears if the Cisco IOS image on your router supports Easy VPN Client Phase II.

The Cisco Easy VPN Remote feature implements the Cisco Unity Client protocol, which allows most VPN parameters to be defined at a VPN remote access server. This server can be a dedicated VPN device, such as a VPN 3000 concentrator or a Cisco PIX Firewall, or it can be a Cisco IOS router that supports the Cisco Unity Client protocol.

Note

- If the Easy VPN server or concentrator has been configured to use XAuth, it requires a username and password whenever the router establishes the connection, including when you deliver the configuration to the router, and when you disconnect and then reconnect the tunnel. Find out whether XAuth is used and the required username and password.
- If the router uses Secure Shell (SSH) you must enter the SSH login and password the first time you establish the connection.

Field Reference

Table 26-9 Add or Edit Easy VPN Remote Fields

Element	Description
Name	Enter a name for the Easy VPN remote configuration.
Mode	
Client	Choose **Client** if you want the PCs and other devices on the router's inside networks to form a private network with private IP addresses. Network Address Translation (NAT) and Port Address Translation (PAT) will be used. Devices outside the LAN will not be able to ping devices on the LAN or to reach them directly.

Table 26-9 Add or Edit Easy VPN Remote Fields

Element	Description
Network Extension	Choose **Network Extension** if you want the devices connected to the inside interfaces to have IP addresses that are routable and reachable by the destination network. The devices at both ends of the connection will form one logical network. PAT will be automatically disabled, allowing the PCs and hosts at both ends of the connection to have direct access to one another.
Tunnel Control	
Auto	Choose **Auto** if you want the VPN tunnel to be established automatically when the Easy VPN configuration is delivered to the router configuration file. However, you will not be able to control the tunnel manually in the VPN Connections window. The Connect and Disconnect buttons are disabled when this Easy VPN connection is chosen.
Manual	Choose **Manual** if you want to control when the VPN tunnel is established and terminated. You must click the **Connect** button in the Edit Easy VPN Remote window to establish the tunnel. The Connect and Disconnect buttons are enabled whenever you choose a VPN connection with the Manual tunnel control setting.
Easy VPN Concentrator or Server	Specify the name or the IP address of the VPN concentrator or server that the router connects to. Choose **IP address** if you are going to provide an IP address or choose **Hostname** if you are going to provide the hostname of the concentrator or server. Then specify the appropriate value in the field underneath. If you specify a hostname, there must be a DNS server on the network that can resolve the hostname to the proper IP address. If you enter an IP address, use standard dotted decimal format, for example, 172.16.44.1.
Group	
Group Name]	Enter the IPSec group name. The group name must match the group name defined on the VPN concentrator or server. Obtain this information from your network administrator.
Group Key	Enter the IPSec group password. The group password must match the group password defined on the VPN concentrator or server. Obtain this information from your network administrator.

Table 26-9 Add or Edit Easy VPN Remote Fields

Element	Description
Confirm Key	Reenter the group password to confirm.
Interfaces	
Outside Interface Toward Server or Concentrator	Choose the interface that has the connection to the Easy VPN server or concentrator. **Note** Cisco 800 routers do not support the use of interface E 0 as the outside interface.
Inside Interfaces	Specify the inside interfaces to include in this Easy VPN configuration. All hosts connected to these interfaces will be part of the VPN. As many as three inside interfaces are supported on Cisco 800 series and Cisco 1700 series routers. **Note** An interface cannot be designated as both an inside interface and an outside interface.

Add or Edit Easy VPN Remote: General Settings

Use this Window to configure your router as an Easy VPN client. Your router must have a connection to an Easy VPN concentrator or server on the network.

Note This window appears if the Cisco IOS image on your router supports Easy VPN Client Phase IV.

The Cisco Easy VPN Remote feature implements the Cisco Unity Client protocol, which allows most VPN parameters to be defined on a VPN remote access server. This server can be a dedicated VPN device, such as a VPN 3000 concentrator or a Cisco PIX Firewall, or it can be a Cisco IOS router that supports the Cisco Unity Client protocol.

Field Reference

Table 26-10 Easy VPN Remote General Settings Fields

Element	Description
Name	Enter a name for the Easy VPN remote configuration.
Servers	You can specify up to ten Easy VPN servers by IP address or hostname, and you can order the list to specify which servers the router will attempt to connect to first. Click **Add** to specify the name or the IP address of a VPN concentrator or server for the router to connect to, and then enter the address or hostname in the window displayed. Click **Delete** to delete the specified IP address or hostname. Click **Move Up** to move the specified server IP address or hostname up in the list. The router attempts to contact routers in the order in which they appear in this list. Click **Move Down** to move the specified IP address or hostname down the list.
Mode	
Client	Choose **Client** mode if you want the PCs and other devices on the router's inside networks to form a private network with private IP addresses. Network Address Translation (NAT) and Port Address Translation (PAT) will be used. Devices outside the LAN will not be able to ping devices on the LAN or to reach them directly.
Network Extension	Choose **Network Extension** if you want the devices connected to the inside interfaces to have IP addresses that are routable and reachable by the destination network. The devices at both ends of the connection will form one logical network. PAT will be automatically disabled, allowing the PCs and hosts at both ends of the connection to have direct access to one another. • Enable remote management and troubleshooting of your router. You can enable remote management of the router by checking the box to request a server-assigned IP address for you router. This IP address can be used for connecting to your router for remote management and troubleshooting (ping, Telnet, and Secure Shell). This mode is called **Network Extension Plus**.

Table 26-10 Easy VPN Remote General Settings Fields

Element	Description
	Consult the administrator of the Easy VPN server or concentrator before you choose this setting. If you choose Network Extension, you also have the capability to: • Allow subnets not directly connected to the router to use the tunnel. To allow subnets not directly connected to your router to use the tunnel, click the **Options** button and configure the network extension options. • Enable remote management and troubleshooting of your router. You can enable remote management of the router by checking the box to request a server-assigned IP address for you router. This IP address can be used for connecting to your router for remote management and troubleshooting (ping, Telnet, and Secure Shell). This mode is called **Network Extension Plus**.
Have the server assign an IP address to manage my router remotely.	Check this box to request a server-assigned IP address for you router. This IP address can be used for connecting to your router for remote management and troubleshooting (ping, Telnet, and Secure Shell). This mode is called **Network Extension Plus**.

Network Extension Options

To allow subnets not directly connected to your router to use the tunnel, enter the subnets in this screen, or enter an ACL that defines the subnets you want to allow.

Field Reference

Table 26-11 Network Extension Options Fields

Element	Description
Configure Multiple Subnets	Check **Configure Multiple Subnets** to enable the other fields in this screen.
Enter the subnets. Cisco CP will create the necessary ACL.	Check this option to enter each subnet and subnet mask manually. Click **Add** to add an entry to the list. Click **Delete** to remove the selected entry.
Select an ACL	Check **Select an ACL** to use an ACL to define the subnets. If you know the name or number of the ACL enter it in the field. Or, click the button to the right of the field, and select an existing ACL or create a new ACL. To remove an ACL association in this screen, click the button and choose **None** (**clear rule association**).

Add or Edit Easy VPN Remote: Easy VPN Settings

Use this window to configure your router as an Easy VPN client. Your router must have a connection to an Easy VPN concentrator or server on the network.

Note This window appears if the Cisco IOS image on your router supports Easy VPN Client Phase III.

The Cisco Easy VPN Remote feature implements The Cisco Unity Client protocol, which allows most VPN parameters to be defined on a VPN remote access server. This server can be a dedicated VPN device, such as a VPN 3000 concentrator or a Cisco PIX Firewall, or it can be a Cisco IOS router that supports the Cisco Unity Client protocol.

Field Reference

Table 26-12 Easy VPN Settings Fields

Element	Description
Name	Enter a name for the Easy VPN remote configuration.
Mode	

Table 26-12 Easy VPN Settings Fields

Element	Description
Client	Choose **Client** mode if you want the PCs and other devices on the router's inside networks to form a private network with private IP addresses. Network Address Translation (NAT) and Port Address Translation (PAT) will be used. Devices outside the LAN will not be able to ping devices on the LAN or to reach them directly.
Network Extension	Choose **Network Extension** if you want the devices connected to the inside interfaces to have IP addresses that are routable and reachable by the destination network. The devices at both ends of the connection will form one logical network. PAT will be automatically disabled, allowing the PCs and hosts at both ends of the connection to have direct access to one another. Consult the administrator of the Easy VPN server or concentrator before you choose this setting.
Tunnel Control	
Auto	Choose **Auto** if you want the VPN tunnel to be established automatically when the Easy VPN configuration is delivered to the router configuration file. However, you will not be able to control the tunnel manually in the VPN Connections window. The Connect and Disconnect buttons are disabled when this Easy VPN connection is chosen.
Manual	Choose **Manual** if you want to control when the VPN tunnel is established and terminated. You must click the **Connect** button in the Edit Easy VPN Remote window to establish the tunnel. The Connect and Disconnect buttons are enabled whenever you choose a VPN connection with the Manual tunnel control setting.
Servers You can specify up to ten Easy VPN servers by IP address or hostname, and you can order the list to specify which servers the router will attempt to connect to first.	
Add	Click **Add** to specify the name or the IP address of a VPN concentrator or server for the router to connect to; then enter the address or hostname in the window displayed.
Delete	Click **Delete** to delete the chosen server IP address or hostname.

Table 26-12 Easy VPN Settings Fields

Element	Description
Move Up	Click **Move Up** to move the specified server IP address or hostname up in the list. The router attempts to contact routers in the order in which they appear in this list.
Move Down	Click **Move Down** to move the specified IP address or hostname down the list.
Outside Interface Toward Server or Concentrator	Choose the interface that has the connection to the Easy VPN server or concentrator. **Note** Cisco 800 routers do not support the use of interface E 0 as the outside interface.
Inside Interfaces	Specify the inside interfaces to include in this Easy VPN configuration. All hosts connected to these interfaces will be part of the VPN. As many as three inside interfaces are supported on Cisco 800 series and Cisco 1700 series routers. **Note** An interface cannot be designated as both an inside and an outside interface.

Add or Edit Easy VPN Remote: Authentication Information

Use this window to enter the information required for the router to be authenticated by the Easy VPN server or concentrator.

Field Reference

Table 26-13 Authentication Information Fields

Element	Description
Device Authentication	
Digital Certificate	If you choose digital certificate, a digital certificate must be configured on the router to use. **Note** The Digital Certificates option is available only if supported by the Cisco IOS image on your router.
Preshared Key	Choose Preshared Key to use the IKE key value given to you by your network administrator. Obtain the IPSec group name and IKE key value from your network administrator. The group name must match the group name defined on the VPN concentrator or server.
Group Name	Enter the IPSec groupname given to you by your network administrator. The group name must match the group name defined on the VPN concentrator or server. This field only appears if Preshared Key is chosen.
Current Key	The Current Key field displays asterisks (*) if there is a current IKE key value. This field contains the value <None> if no key has been configured. This field only appears if Preshared Key is chosen.
New Key	Enter the new IKE key value given to you by your network administrator. This field only appears if Preshared Key is chosen.
Reenter Key	Reenter the new key to confirm accuracy. If the values in the New Key and Reenter Key fields are not the same, Cisco CP prompts you to reenter the key values. This field only appears if Preshared Key is chosen
User Authentication	
If the Easy VPN server or concentrator has been configured to use XAuth, it requires a username and password whenever the router establishes the connection, including when you deliver the configuration to the router, and when you disconnect and reconnect the tunnel. Find out whether XAuth is used, and obtain the required username and password.	

Table 26-13 Authentication Information Fields

Element	Description
From PC	Choose **From PC** if you will enter the credentials in a web browser window. **Note** This option appears only if supported by the Cisco IOS image on your router.
From this router	Choose **From this router** if you will enter the credentials from the router command line interface or from Cisco CP.
Save Credentials	If the server allows passwords to be saved, you can eliminate the need to enter the username and password each time the Easy VPN tunnel is established. The information is saved in the router configuration file and used each time the tunnel is established. Choose **Save Credentials** to save the username and password to the router configuration file. **Caution** Storing the XAuth username and password in router memory creates a security risk because anyone who has access to the router configuration can obtain this information. If you do not want this information stored on the router, do not enter it here. The Easy VPN server will simply challenge the router for the username and password each time the connection is established. Also, Cisco CP cannot itself determine whether the server allows passwords to be saved. You must determine whether the server allows this option. If the server does not allow passwords to be saved, you should not create a security risk by entering the information here.
Username	Enter the username you have been given by the server administrator.
Current Password	The Current Password field displays asterisks (*) if there is a configured password. This field contains the value <None> if no password has been configured.

Table 26-13 Authentication Information Fields

Element	Description
New Password	Enter the new password given to you by the server administrator.
Reenter Password	Reenter the new password to confirm accuracy. If the values in the New Password and Reenter Password fields are not the same, Cisco CP prompts you to reenter the password values.

Add or Edit Easy VPN Remote: Easy VPN Client Phase III Authentication

This window appears if the Cisco IOS image on your router supports Easy VPN Client Phase III. If the image supports Easy VPN Client Phase II, a different window appears.

Use this window to enter the information required for the router to be authenticated by the Easy VPN server or concentrator.

Field Reference

Table 26-14 Authentication Information Fields

Element	Description
Device Authentication	
Group Name	Enter the IPSec groupname given to you by your network administrator. The group name must match the group name defined on the VPN concentrator or server.
Current Key	The Current Key field displays asterisks (*) if there is a current IKE key value. This field contains the value <None> if no key has been configured.
New Key	Enter the new IKE key value given to you by your network administrator.
Reenter Key	Reenter the new key to confirm accuracy. If the values in the New Key and Reenter Key fields are not the same, Cisco CP prompts you to reenter the key values.
User Authentication	

Table 26-14 Authentication Information Fields

Element	Description
If the Easy VPN server or concentrator has been configured to use XAuth, it requires a username and password whenever the router establishes the connection, including when you deliver the configuration to the router, and when you disconnect and reconnect the tunnel. Find out whether XAuth is used, and obtain the required username and password.	
From PC	Choose **From PC** if you will enter the credentials in a web browser window. **Note** This option appears only if supported by the Cisco IOS image on your router.
From this router	Choose **From this router** if you will enter the credentials from the router command line interface or from Cisco CP.
Save Credentials	If the server allows passwords to be saved, you can eliminate the need to enter the username and password each time the Easy VPN tunnel is established. The information is saved in the router configuration file and used each time the tunnel is established. Choose **Save Credentials** to save the username and password to the router configuration file. **Caution** Storing the XAuth username and password in router memory creates a security risk because anyone who has access to the router configuration can obtain this information. If you do not want this information stored on the router, do not enter it here. The Easy VPN server will simply challenge the router for the username and password each time the connection is established. Also, Cisco CP cannot itself determine whether the server allows passwords to be saved. You must determine whether the server allows this option. If the server does not allow passwords to be saved, you should not create a security risk by entering the information here.
Username	Enter the username you have been given by the server administrator.

Table 26-14 Authentication Information Fields

Element	Description
Current Password	The Current Password field displays asterisks (*) if there is a configured password. This field contains the value <None> if no password has been configured.
New Password	Enter the new password given to you by the server administrator.
Reenter Password	Reenter the new password to confirm accuracy. If the values in the New Password and Reenter Password fields are not the same, Cisco CP prompts you to reenter the password values.

Add or Edit Easy VPN Remote: Interfaces and Connections

Identify the inside and outside interfaces, and specify how the VPN tunnel is brought up in this screen.

Field Reference

Table 26-15 Interfaces and Connection Settings Fields

Element	Description
Interfaces	
Check boxes	Check the inside (LAN) interfaces that serve the local networks that you want to include in this Easy VPN configuration. You can choose multiple inside interfaces, with the following restrictions: • If you choose an interface that is already used in another Easy VPN configuration, you are told that an interface cannot be part of two Easy VPN configurations. • If you choose interfaces that are already used in a VPN configuration, you are informed that the Easy VPN configuration you are creating cannot coexist with the existing VPN configuration. You will be asked if you want to remove the existing VPN tunnels from those interfaces and apply the Easy VPN configuration to them.

Table 26-15 Interfaces and Connection Settings Fields

Element	Description
	• An existing interface does not appear in the list of interfaces if it cannot be used in an Easy VPN configuration. For example, loopback interfaces configured on the router do not appear in this list. • An interface cannot be designated as both an inside and an outside interface. Up to three inside interfaces are supported on Cisco 800 and Cisco 1700 series routers. You can remove interfaces from an Easy VPN configuration in the Edit Easy VPN Remote window.
Interface list	In the Interfaces list, choose the outside interface that connects to the Easy VPN server or concentrator.  **Note** Cisco 800 routers do not support the use of interface E 0 as the outside interface
Virtual Tunnel Interface	Check this option if you want to use a Virtual Tunnel Interface (VTI) for this connection. If the VTIs in the list are used by other VPN connections, click **Add** to create a new one.
Connection Settings	
Auto	Choose **Auto** to have the router establish the VPN tunnel automatically when the Easy VPN configuration is delivered to the router configuration file. You will not be able to control the tunnel manually using the Connect or Disconnect button. These buttons are disabled when this setting is chosen.

Table 26-15 Interfaces and Connection Settings Fields

Element	Description
Manual	Choose **Manual** if you want to bring up and shut down the VPN tunnel manually. With the manual setting, you must click the **Connect** or **Disconnect** button in the Edit Easy VPN Remote screen to establish or take down the tunnel. Additionally, if a security association (SA) timeout is set for the router, you will have to manually reestablish the VPN tunnel whenever a timeout occurs. You can change SA timeout settings in the VPN Components VPN Options window.
Interesting Traffic	Choose **Interesting Traffic** to establish the VPN tunnel whenever outbound local (LAN side) traffic is detected. The Connect or Disconnect button is disabled when you choose this Easy VPN connection setting. **Note** The Interesting Traffic option appears only if supported by the Cisco IOS image on your router.

Add or Edit Easy VPN Remote: Firewall Bypass

Use the Firewall Bypass page to enable VPN access through a firewall or to edit the existing port number and keepalive values.

An Easy VPN tunnel network might not work if there is a firewall between the router and the VPN server that blocks VPN protocols such as IKE and ESP. You can use Cisco CP to configure your router to use Cisco Tunneling Control Protocol (CTCP) to enable encrypted traffic to go through the firewall.

Note The Enable Easy VPN Access Through Firewall feature is supported on Cisco routers that are running Cisco IOS Release 12.4(20)T and later.

How to Get to This Page

1. Go to **Configure > Security > VPN > Easy VPN Remote**.
2. Click the **Edit Easy VPN Remote** tab.
3. Select the Easy VPN Remote connection that you want to edit.

4. Click **Edit**. The Edit Easy VPN Remote page opens, which contains several tabs.
5. Click the **Firewall Bypass** tab.

Related Topics

- Easy VPN Remote Wizard: Automatic Firewall Bypass, page 26-14
- Editing CTCP Port Number and Keepalive Values, page 26-20

Field Reference

Table 26-16 Firewall Bypass Page

Element	Description
Enable Easy VPN Access Through Firewall check box	When this check box is checked, Cisco CP configures the router to use Cisco Tunneling Control Protocol (CTCP) so that encrypted traffic can go through the firewall. To disable Easy VPN access through the firewall, uncheck this check box.
Port Number	The port number on which to configure the CTCP. The default port number is 10000, which you can change. Valid port numbers are 1 to 65535. If you enter a port number within the range of 1 to 1023, you will see the following warning message: `Port number <port_number> is a well-known port. Adding this port number will block all the applications bound to this port. Do you still want to configure this port number for CTCP?`
Keepalive	The keepalive value (in seconds) to send keepalives, so that NAT or firewall sessions do not timeout. The default keepalive value is 5 seconds, which you can change. Valid keepalive values are 5 to 3600 seconds.

Add or Edit Easy VPN Remote: Identical Addressing

In this screen, enter the information needed to configure identical addressing. Identical addressing enables remote networks to reach local devices that have IP addresses that might overlap with addresses in remote networks.

Field Reference

Table 26-17 Identical Addressing Tab Fields

Element	Description
Configure identical addressing	Check **Configure identical addressing** if there are devices on the local network with IP addresses that might overlap with addresses in remote networks in your organization. You must check this box to enable the other controls in this screen.
Loopback Interface	
Loopback Interface	Click the down arrow to select an existing loopback interface. If no loopback interfaces are configured, click **Add**.
Add	Clicking **Add** displays the dialog that enables you to configure a loopback interface.
Enable split tunneling	Split tunneling enables the router to only use the VPN tunnel to send traffic to network addresses given to it by the Easy VPN server and to send other traffic through the Internet. To enable the router to use this feature, click **Enable split tunneling**.
Accessible Devices	
Device Local IP	The local IP address of a device that is identified as a device that must be reached by other networks.
Device Global IP	The global IP address given to a device that is identified as a device that must be reached by other networks. Because the global IP address for each device must be routable from the Easy VPN server, you must obtain these addresses from the Easy VPN server administrator. Each IP address must be on the same subnet, and one address must be reserved for use by non accessible devices on the local network.
Add	To add the local IP address and global IP address of a device, click **Add**.
Edit	To change the IP address information for a device, choose an entry and click **Edit**.
Delete	To remove an entry for an accessible device, choose the entry and click **Delete**.

Warning Messages

Cisco CP displays a warning message when you click **OK** if it detects any of the following problems:

- There are no devices added.
- If you enter an IP address for the non accessible devices that is already used by a router interface.
- If you enter an IP address for the non accessible devices that is already used as a global IP address for an accessible device.
- If you enter local IP address for a device that falls outside the subnet for the LAN interface it connects to.
- If you chose client mode in the General tab. Identical addressing only works with network extension mode.
- If you did not choose a virtual tunnel interface in the Interfaces and Connections tab.

Easy VPN Remote: Add a Device

Enter the local IP address and global IP address information for a device in this screen. The global IP address is an IP address that can be used to identify the device to other networks.

Field Reference

Table 26-18 Add a Device Fields

Element	Description
Local IP Address	Enter the local IP address of the device that must be reached.
Global IP Address	Enter the global IP address that you want to use for this device. The address you use must be routable from the Easy VPN server.

Enter SSH Credentials

If the router uses Secure Shell (SSH), you must to enter the SSH login and password the first time you establish the connection. Use this window to enter SSH or Telnet login information.

Field Reference

Table 26-19 Enter SSH Credentials Fields

Element	Description
Username	Enter the SSH or Telnet account username that you will use to log in to this router.
Password	Enter the password associated with the SSH or Telnet account username that you will use to log in to this router.

XAuth Login Window

This window appears when the Easy VPN server requests extended authentication. Respond to the challenges by entering the information requested, such as the account username, password, or any other information, to successfully establish the Easy VPN tunnel. If you are unsure about the information that should be provided, contact your VPN administrator.

Other Procedures

This section contains procedures for tasks that the wizard does not help you complete.

How Do I Edit an Existing Easy VPN Connection?

To edit an existing Easy VPN remote connection, follow these steps:

Step 1 On the Cisco CP Feature bar, click **Configure > Security > VPN**.

Step 2 In the VPN tree, choose **Easy VPN Remote**.

Step 3 Click the **Edit Easy VPN Remote** tab and choose the connection that you want to edit.

Step 4 Click **Edit.**

The Edit Easy VPN Remote window appears.

Step 5 In the Edit Easy VPN Remote window, click the tabs to display the values that you want to change.

Step 6 When you have finished making changes, click **OK**.

How Do I Configure a Backup for an Easy VPN Connection?

To configure a backup for an Easy VPN Remote connection, your router must have an ISDN, async, or analog modem interface available for the backup.

If the ISDN, async, or analog modem interface has not been configured, follow these steps:

Step 1 From the Feature bar, click **Basic Router > Interfaces and Connections**.

Step 2 Click the **Create Connection** tab.

Step 3 Choose an ISDN, async, or analog modem interface from the list.

Step 4 Click the **Create New Connection** button and use the wizard to configure the new interface.

Step 5 In the appropriate wizard window, set the new interface as a backup for an Easy VPN Remote connection.

If the ISDN, async, or analog modem interface has been configured, follow these steps:

Step 1 From the Feature bar, click **Basic Router > Interfaces and Connections**.

Step 2 Click the **Edit Interface/Connection** tab.

Step 3 Choose an ISDN, async, or analog modem interface from the list of configured interfaces.

Step 4 Click the **Edit** button.

Step 5 Click the **Backup** tab and configure the backup for an Easy VPN Remote connection.

Step 6 When you have finished configuring the backup, click **OK**.

CHAPTER 27

Easy VPN Server

The Easy VPN Server feature introduces server support for the Cisco VPN Client Release 3.x and later software clients and Cisco VPN hardware clients. The feature allows a remote end user to communicate using IP Security (IPSec) with anyCisco IOS Virtual Private Network (VPN) gateway. Centrally managed IPSec policies are “pushed” to the client by the server, minimizing configuration by the end user.

The following link provides general information on the Cisco Easy VPN solution, and other links for more specific information:

http://www.cisco.com/en/US/products/sw/secursw/ps5299/index.html

This chapter contains the following sections:

- Creating an Easy VPN Server Connection
- Editing Easy VPN Server Connections

Creating an Easy VPN Server Connection

Use theCisco CP Easy VPN Server wizard to create an Easy VPN Server connection on the router.

Complete these steps to configure an Easy VPN Server connection using the Easy VPN Server wizard:

Step 1 In the Cisco CP Feature bar, click **Configure > Security > VPN**.

Step 2 In the VPN tree, click **Easy VPN Server**.

Step 3 In the Create Easy VPN Server tab, complete any recommended tasks that are displayed by clicking the link for the task. Cisco CP either completes the task for you, or displays the necessary configuration screens for you to make settings in.

Step 4 Click **Launch Easy VPN Server Wizard** to begin configuring the connection.

Step 5 Make configuration settings in the wizard screens. Click **Next** to go from the current screen to the next screen. Click **Back** to return to a screen you have previously visited.

Step 6 Cisco CP displays the Summary screen when you have completed the configuration. Review the configuration. If you need to make changes, click **Back** to return to the screen in which you need to make changes, then return to the Summary screen.

Step 7 If you want to test the connection after sending the configuration to the router, check **Test the connectivity after configuring**. After you click **Finish**, Cisco CP tests the connection and displays the test results in another screen.

Step 8 To send the configuration to the router, click **Finish**.

Create an Easy VPN Server Reference describes the configuration screens you use to create an Easy VPN server connection.

Create an Easy VPN Server Reference

The topics in this section describe the configuration screens:

- Create an Easy VPN Server
- Welcome to the Easy VPN Server Wizard
- Interface and Authentication
- Group Authorization and Group Policy Lookup
- User Authentication (XAuth)
- User Accounts for XAuth
- Add RADIUS Server
- Group Authorization: User Group Policies
- General Group Information

- DNS and WINS Configuration
- Split Tunneling
- Client Settings
- Choose Browser Proxy Settings
- Add or Edit Browser Proxy Settings
- User Authentication (XAuth)
- Client Update
- Add or Edit Client Update Entry
- Cisco Tunneling Control Protocol
- Summary
- Browser Proxy Settings

Create an Easy VPN Server

This wizard will guide you through the necessary steps to configure an Easy VPN Server on this router.

Field Reference

Table 27-1 Create an Easy VPN Server Fields

Element	Description
Launch the Easy VPN Server Wizard	Click this button to start the wizard.

Welcome to the Easy VPN Server Wizard

This wizard will guide you in performing the following tasks to successfully configure an Easy VPN Server on this router.

- Choosing the interface on which the client connections will terminate, and the authentication method used for the server and Easy VPN clients
- Configuring IKE policies
- Configuring an IPSec transform set
- Configuring group authorization and the group policy lookup method

- Configuring user authentication
- Configuring external RADIUS servers
- Configuring policies for remote users connecting to Easy VPN clients

Interface and Authentication

This window lets you choose the interface on which you want to configure the Easy VPN Server.

If you choose an interface that is already configured with a site-to-site IPSec policy, Cisco CP displays a message that an IPSec policy already exists on the interface. Cisco CP uses the existing IPSec policy to configure the Easy VPN Server.

If the chosen interface is part of an Easy VPN Remote, GREoIPSec, or DMVPN interface, Cisco CP displays a message to choose another interface.

Field Reference

Table 27-2 Interface and Authentication Fields

Element	Description
Details	Click this button to obtain details about the interface you choose. The details window shows any access rules, IPSec policies, NAT rules, or inspection rules associated with the interface. This button is dimmed when no interface is chosen.
Authentication	Choose one of the following: Pre-shared Keys—If you click **Pre-shared Keys**, you must enter a key value when you configure the Add Group Policy general setup window. Digital Certificates—If you click **Digital Certificates**, the preshared keys fields does not appear in the Add Group Policy general setup window. Both—If you **Both**, entering a key value in the Add Group Policy general setup window is optional.

Group Authorization and Group Policy Lookup

This window allows you to define a new AAA authorization network method list for group policy lookup or to choose an existing network method list.

Field Reference

Table 27-3 Group Authorization and Policy Lookup Fields

Element	Description
Local Only	This option allows you to create a method list for the local database only. When you define an AAA method list for the local database, the router looks at the local database for group authentication.
RADIUS Only	This option allows you to create a method list for a RADIUS database.
RADIUS and Local	This option allows you to create a method list for both RADIUS and local database. When you define method lists for both a RADIUS and local database, the router first looks at the RADIUS server and then the local database for group authentication.
Select an existing AAA method list	This option lets you choose an existing AAA method list on the router to use for group authentication.

User Authentication (XAuth)

You can configure user authentication on Easy VPN Server. You can store user authentication details on an external server such as a RADIUS server or a local database or on both. An AAA login authentication method list is used to decide the order in which user authentication details should be searched.

Field Reference

Table 27-4 User Authentication Fields

Element	Description
Local	Click **Local** to add user authentication details to the local database.
RADIUS	Click **RADIUS** if you want to add user authentication details to the database on the RADIUS server.
RADIUS and Local	Click **RADIUS and Local** to add user authentication details for both a RADIUS and local database.
Select an existing AAA Method List	Click **Select an existing AAA Method List** to choose a method list from a list of all method lists configured on the router. The chosen method list is used for extended authentication.
Add User Credentials	Click **Add User Credentials** to add a user account.
Summary	If you choose RADIUS, the Summary box is displayed. It explains how the RADIUS and local databases are used, and that the Easy VPN remote user can be notified when their password has expired. • Notify remote user of password expiration—This option is checked by default. When enabled, the Easy VPN Server notifies the user when their password has expired and prompts them to enter a new password.

User Accounts for XAuth

Add an account for a user you want to authenticate after IKE has authenticated the device.

Field Reference

Table 27-5 User Accounts for XAuth Fields

Element	Description
User Accounts	The user accounts that XAuth will authenticate are listed in this box. The account name and privilege level are visible.

Table 27-5 User Accounts for XAuth Fields (continued)

Element	Description
Add Edit	Use these buttons to add and edit user accounts. User accounts can be deleted in the **Additional Tasks > Router Access > User Accounts/View** window. **Note** Existing CLI view user accounts cannot be edited from this window. If you need to edit user accounts, go to **Additional Tasks > Router Access >User Accounts/CLI View**.

Add RADIUS Server

This window lets you add a new RADIUS server or edit or ping an already existing RADIUS server.

Field Reference

Table 27-6 Add a RADIUS Server Fields

Element	Description
Add	Add a new RADIUS server.
Edit	Edit an already exiting RADIUS server configuration.
Ping	Ping an already existing RADIUS server or newly configured RADIUS server.

Group Authorization: User Group Policies

This window allows you to add, edit, clone or delete user group policies on the local database.

Field Reference

Table 27-7 User Group Policies Fields

Element	Description
Group Policy List area	
Select	Check the box in this column next to the groups that you want this Easy VPN server connection to serve.
Group Name	Name given to the user group.
Pool	Name of the IP address pool from which an IP address is assigned to a user connecting from this group.
DNS	Domain Name System (DNS) address of the group. This DNS address is "pushed" to the users connecting to this group.
WINS	Windows Internet Naming Service (WINS) address of the group. This WINS address is "pushed" to the users connecting to this group.
Domain Name	Domain name of the group. This domain name is "pushed" to the users connecting to this group.
Split ACL	The access control list (ACL) that represents protected subnets for split tunneling purposes.
Configure Idle Timer	
Idle Timer	Click the **Configure Idle Timer** check box and enter a value for the maximum time that a VPN tunnel can remain idle before being disconnected. Enter hours in the left field, minutes in the middle field, and seconds in the right field. The minimum time allowed is 1 minute. Disconnecting idle VPN tunnels can help the Easy VPN Server run more efficiently by reclaiming unused resources.

General Group Information

This window allows you to configure, edit and clone group polices.

Field Reference

Table 27-8 General Group Information Fields

Element	Description
Please Enter a Name for This Group	Enter the group name in the field provided. If this group policy is being edited, this field is disabled. If you are cloning a group policy, you must enter a new value in this field.
Preshared Key	Enter the preshared key in the fields provided. The **Current key** field cannot be changed. **Note** You do not have to enter a preshared key if you are using digital certificates for group authentication. Digital certificates are also used for user authentication.
Pool Information	Specifies a local pool of IP addresses that are used to allocate IP addresses to clients. Create a New Pool—Enter the range of IP addresses for the local IP address pool in the IP Address Range field. Select from an Existing Pool—Choose the range of IP addresses from the existing pool of IP addresses. **Note** This field cannot be edited if there are no predefined IP address pools.
Subnet Mask (Optional)	Enter a subnet mask to send with the IP addresses allocated to clients in this group.
Maximum Connections Allowed	Specify the maximum number of client connections to the Easy VPN Server from this group. Cisco CP supports a maximum of 5000 connections per group.

DNS and WINS Configuration

This window allows you to specify the Domain Name Service (DNS) and Windows Internet Naming Service (WINS) information.

Field Reference

Table 27-9 DNS and WINS Fields

Element	Description
DNS	Enter the primary and secondary DNS server IP address in the fields provided. Entering a secondary DNS server address is optional.
WINS	Enter the primary and secondary WINS server IP address in the fields provided. Entering a secondary WINS server address is optional.
Domain Name	Specify the domain name that should be pushed to the Easy VPN client.

Split Tunneling

This window allows you to enable split tunneling for the user group you are adding.

Split tunneling is the ability to have a secure tunnel to the central site and simultaneous clear text tunnels to the Internet. For example, all traffic sourced from the client is sent to the destination subnet through the VPN tunnel.

You can also specify which groups of ACLs represent protected subnets for split tunneling.

Field Reference

Table 27-10 Split Tunneling Fields

Element	Description
Enable Split Tunneling	This box allows you to add protected subnets and ACLs for split tunneling. • Enter the Protected Subnets—Add or remove the subnets for which the packets are tunneled from the VPN clients. • Choose the Split Tunneling ACL—Choose the ACL to use for split tunneling.

Table 27-10 Split Tunneling Fields (continued)

Element	Description
Split DNS	Enter the Internet domain names that should be resolved by your network's DNS server. The following restrictions apply: • A maximum of 10 entries is allowed. • Entries must be separated with a comma. • Do not use spaces anywhere in the list of entries. • Duplicate entries or entries with invalid formats are not accepted. **Note** This feature appears only if supported by your Cisco server's IOS release.

Client Settings

This window allows you to configure additional attributes for security policy such as adding or removing a backup server, Firewall Are-U-There, and Include-Local-LAN.

Note Some of the features described below appear only if supported by your Cisco server's IOS release.

Field Reference

Table 27-11 Client Setting Fields

Element	Description
Backup Servers	You can specify up to ten servers by IP address or hostname as backup for the Easy VPN server, and order the list to control which servers the router will attempt to connect to first if the primary connection to the Easy VPN server fails. • **Add—**Click **Add** to specify the name or the IP address of an Easy VPN server for the router to connect to when the primary connection fails, and then enter the address or hostname in the window displayed. • **Delete—**Click **Delete** to remove a specified IP address or hostname.
Configuration Push	You can specify an Easy VPN client configuration file using a URL and version number. The Easy VPN Server sends the URL and version number to Easy VPN hardware clients requesting that information. Only Easy VPN hardware clients belonging to the group policy you are configuring can request the URL and version number you enter in this window. Enter the URL of the configuration file in the URL field. The URL should begin with an appropriate protocol, and can include usernames and passwords. The following are URL examples for downloading an upgrade file called sdm.exe: • http://*username*:*password*@www.cisco.com/go/vpn/sdm.exe • https://*username*:*password*@www.cisco.com/go/vpn/sdm.exe • ftp://*username*:*password*@www.cisco.com/go/vpn/sdm.exe • tftp://*username*:*password*@www.cisco.com/go/vpn/sdm.exe • scp://*username*:*password*@www.cisco.com/go/vpn/sdm.exe • rcp://*username*:*password*@www.cisco.com/go/vpn/sdm.exe

Table 27-11 Client Setting Fields (continued)

Element	Description
Configuration Push	• cns: • xmodem: • ymodem: • null: • flash:sdm.exe • nvram:sdm.exe • usbtoken[0-9]:sdm.exe The USB token port number range is 0-9. For example, for a USB token attached to USB port 0, the URL is usbtoken0:sdm.exe. • usbflash[0-9]:sdm.exe The USB flash port number range is 0-9. For example, for a USB flash attached to USB port 0, the URL is usbflash0:sdm.exe. • disk[0-1]:sdm.exe The disk number is 0 or 1. For example, for disk number 0, the URL is disk0:sdm.exe. • archive:sdm.exe • tar:sdm.exe • system:sdm.exe In these examples, *username* is the site username and *password* is the site password. Enter the version number of the file in the Version field. The version number must be in the range 1 to 32767.

Table 27-11 Client Setting Fields (continued)

Element	Description
Browser Proxy	You can specify browser proxy settings for Easy VPN software clients. The Easy VPN Server sends the browser proxy settings to Easy VPN software clients requesting that information. Only Easy VPN software clients belonging to the group policy you are configuring can request the browser proxy settings you enter in this window. Enter the name under which the browser proxy settings were saved, or choose one of the following from the drop-down menu: • Choose an existing setting... Opens a window with a list of existing browser proxy settings. • Create a new setting and choose... Opens a window where you can create new browser proxy settings. • None Clears any browser proxy settings assigned to the group.
Firewall Are-U-There	You can restrict VPN connections to clients running Black Ice or Zone Alarm personal firewalls.
Include Local LAN	You can allow a non–split tunneling connection to access the local subnetwork at the same time as the client.
Perfect Forward Secrecy (PFS)	Enable PFS if it is required by the IPSec security association you are using.

Choose Browser Proxy Settings

From the drop-down list, choose the browser proxy settings you want to associate with the group.

Field Reference

Table 27-12 Choose Browser Proxy Settings

Element	Description
Proxy Settings	Choose the settings that you want to associate with the group.

Add or Edit Browser Proxy Settings

This window allows you to add or edit browser proxy settings.

Field Reference

Table 27-13 Browser Proxy Settings Fields

Element	Description
Browser Proxy Settings Name	If you are adding browser proxy settings, enter a name that will appear in drop-down menus listing browser proxy settings. If you are editing browser proxy settings, the name field is read-only.
Proxy Settings	Choose one of the following: • No Proxy Server You do *not* want clients in this group to use a proxy server when they use the VPN tunnel. • Automatically Detect Settings You want clients in this group to automatically detect a proxy server when they use the VPN tunnel. • Manual Proxy Configuration You want to manually configure a proxy server for clients in this group. If you choose this option, complete the procedure for manually configuring a proxy server in this help topic.

Manually Configuring a Proxy Server

If you choose Manual Proxy Configuration, follow these steps to manually configure a proxy server:

Step 1 Enter the proxy server IP address in the Server IP Address field.

Step 2 Enter the port number that proxy server uses for receiving proxy requests in the Port field.

Step 3 Enter a list of IP addresses for which you do *not* want clients to use the proxy server.

Separate the addresses with commas, and do not enter any spaces.

Step 4 If you want to prevent clients from using the proxy server for local (LAN) addresses, check the **Bypass proxy server for local address** check box.

Step 5 Click **OK** to save the browser proxy settings.

User Authentication (XAuth)

This allows you to configure additional attributes for user authentication, such as Group Lock and save Password Attributes.

Field Reference

Table 27-14 User Authentication (XAuth) Fields

Element	Description
XAuth Banner	Enter the text for a banner that is shown to users during XAuth requests. **Note** This feature appears only if supported by your Cisco server's IOS release.
Maximum Logins Allowed Per User	Specify the maximum number of connections a user can establish at a time. Cisco CP supports a maximum of ten logins per user.
Group Lock	You can restrict a client to connect to the Easy VPN Server only from the specified user group.
Save Password	You can save extended authentication user name and password locally on the Easy VPN Client.

Client Update

This window allows you to set up client software or firmware update notifications, and displays existing client update entries. Existing client update entries can be selected for editing or deletion.

Notifications are sent automatically to clients which connect to the server after a new or edited client update configuration is saved. Clients already connected require manual notification. To send a manual IKE notification of update availability, choose a group policy in the group policies window and click the **Send Update** button. Group clients meeting the client update criteria are sent the notification.

Note The client update window is available only if supported by your Cisco server's IOS release.

Field Reference

Table 27-15 Client Update Fields

Element	Description
Client Type	Displays the type of client for which the revision is intended.
Versions	Displays which revisions are available.
URL Column	Displays the location of the revisions.
Add Button	Click to configure a new client update entry.
Edit Button	Click to edit the specified client update entry.
Delete Button	Click to delete the specified client update entry.

Add or Edit Client Update Entry

This window allows you to configure a new client update entry.

Field Reference

Table 27-16 Client Update Entry Fields

Element	Description
Client Type	Enter a client type or choose one from the drop-down menu. Client type names are case sensitive. For software clients, the client type is usually the operating system, for example, *Windows*. For hardware clients, the client type is usually the model number, for example, *vpn3002*. If you are editing the client update entry, the client type is read-only.
URL	Enter the URL that leads to the latest software or firmware revision. The URL should begin with an appropriate protocol, and can include usernames and passwords. The following are URL examples for downloading an upgrade file called vpnclient-4-6.exe: • http://*username*:*password*@www.cisco.com/go/vpn/vpnclient-4.6.exe • https://*username*:*password*@www.cisco.com/go/vpn/vpnclient-4.6.exe • ftp://*username*:*password*@www.cisco.com/go/vpn/vpnclient-4.6.exe • tftp://*username*:*password*@www.cisco.com/go/vpn/vpnclient-4.6.exe • scp://*username*:*password*@www.cisco.com/go/vpn/vpnclient-4.6.exe • rcp://*username*:*password*@www.cisco.com/go/vpn/vpnclient-4.6.exe • cns: • xmodem: • ymodem: • null: • flash:vpnclient-4.6.exe • nvram:vpnclient-4.6.exe • usbtoken[0-9]:vpnclient-4.6.exe The USB token port number range is 0-9. For example, for a USB token attached to USB port 0, the URL is usbtoken0:vpnclient-4.6.exe.

Table 27-16 Client Update Entry Fields (continued)

Element	Description
	• usbflash[0-9]:vpnclient-4.6.exe The USB flash port number range is 0-9. For example, for a USB flash attached to USB port 0, the URL is usbflash0:vpnclient-4.6.exe. • disk[0-1]:vpnclient-4.6.exe The disk number is 0 or 1. For example, for disk number 0, the URL is disk0:vpnclient-4.6.exe. • archive:vpnclient-4.6.exe • tar:vpnclient-4.6.exe • system:vpnclient-4.6.exe In these examples, *username* is the site username and *password* is the site password.
Revisions	Enter the revision number of the latest update. You can enter multiple revision numbers by separating them with commas, for example, *4.3,4.4,4.5*. Do not use any spaces.

Cisco Tunneling Control Protocol

Cisco Tunneling Control Protocol (cTCP) enables VPN clients to operate in environments where standard ESP protocol (port 50) or IKE protocol (UDP port 500) are not permitted. For a variety of reasons, firewalls may not permit ESP or IKE traffic, thus blocking VPN communication. cTCP solves this problem by encapsulating ESP and IKE traffic in the TCP header so that firewalls do not see it.

Field Reference

Table 27-17 Cisco Tunneling Control Protocol

Element	Description
Enable cTCP	Check Enable cTCP to enable this protocol on the Easy VPN server.

Table 27-17 (continued)Cisco Tunneling Control Protocol (continued)

Element	Description
Specify the port numbers	Specify the port numbers on which the Easy VPN server must listen for cTCP requests from clients, You can add a maximum of 10 port numbers. Use a comma to separate entries. Here is an example of 3 port entries: 1000,3000,4000.

Summary

This window shows you the Easy VPN Server configuration that you have created, and it allows you to save the configuration. You can review the configuration in this window and click the **Back** button to change any items.

Clicking the **Finish** button writes the information to the router running configuration. If the tunnel has been configured to operate in Auto mode, the router also attempts to contact the VPN concentrator or server.

If you want to change the Easy VPN Server configuration at a later time, you can make the changes in the Edit Easy VPN Server panel.

To save this configuration to the router running configuration and leave this wizard, click **Finish**. Changes will take effect immediately.

Table 27-18 Summary Buttons

Element	Description
Test VPN Connectivity After Configuring	Click to test the VPN connection you have just configured. The results of the test appear in a separate window.

Browser Proxy Settings

This window lists browser proxy settings, showing how they are configured. You can add, edit, or delete browser proxy settings. Use the group policies configuration to associate browser proxy settings with client groups.

Field Reference

Table 27-19 Add a RADIUS Server Fields

Element	Description
Name	The name of the browser proxy settings.
Settings	Displays one of the following: • No Proxy Server No proxy server can be used by clients when they connect through the VPN tunnel. • Automatically Detect Settings Clients attempt to automatically detect a proxy server. • Manual Proxy Configuration Settings are manually configured.
Server Details	Displays the proxy server IP address and port number used.
Bypass Local Addresses	If set, prevents clients from using the proxy server for local (LAN) addresses.
Exceptions List	A list of IP addresses for which you do *not* want clients to use the proxy server.
Add Button	Configure new browser proxy settings.
Edit Button	Edit the specified browser proxy settings.
Delete Button	Delete the specified browser proxy settings. Browser proxy settings associated with one or more group policies can *not* be deleted before those associations are removed.

Editing Easy VPN Server Connections

To edit an Easy VPN Server connection, complete these steps:

Step 1 In the Cisco CP Feature bar, click **Configure > Security > VPN**.

Step 2 In the VPN tree, click Easy VPN Server.

Step 3 Click **Edit Easy VPN Server**.

Step 4 Choose the VPN server connection that you want to edit.

Step 5 Click **Edit**. Then, make changes to the settings in the displayed dialogs.

Step 6 Click OK to close the dialog and send the changes to the router.

Step 7 If you checked **Preview commands before delivering to router** in the Edit Preferences screen, the Cisco IOS CLI commands that you are sending are displayed. Click **Deliver** to send the configuration to the router, or click **Cancel** to discard it.

Edit Easy VPN Server Reference describes the configuration screens.

Edit Easy VPN Server Reference

The topics in this section describe the Edit Easy VPN Server screens:

- Edit Easy VPN Server
- Add or Edit Easy VPN Server Connection
- Restrict Access
- Group Policies Configuration
- IP Pools
- Add or Edit IP Local Pool
- Add IP Address Range

Edit Easy VPN Server

This window lets you view and manage Easy VPN server connections.

Field Reference

Table 27-20 Edit Easy VPN Server Fields

Element	Description
Add	Click **Add** to add a new Easy VPN Server.
Edit	Click **Edit** to edit an existing Easy VPN Server configuration.

Table 27-20 Edit Easy VPN Server Fields (continued)

Element	Description
Delete	Click **Delete** to delete a specified configuration.
Name	The name of the IPSec policy associated with this connection.
Interface	The name of the interface used for this connection.
Group Authorization	The name of the method list used for group policy lookup.
User Authentication Column	The name of the method list used for user authentication lookup.
Mode Configuration	Displays one of the following: • Initiate The router is configured to initiate connections with Easy VPN Remote clients. • Respond The router is configured to wait for requests from Easy VPN Remote clients before establishing connections.
Test VPN Server Button	Click to test the chosen VPN tunnel. The results of the test appear in a separate window.
Restrict Access Button	Click this button to restrict group access to the specified Easy VPN Server connection. This button is enabled only if both of the following conditions are met: • There is more than one Easy VPN Server connection using the local database for user authentication. • There is at least one local group policy configured.

Add or Edit Easy VPN Server Connection

This window lets you add or edit an Easy VPN Server connection.

Field Reference

Table 27-21 Easy VPN Server Connection Fields

Element	Description
Choose an Interface	If you are adding a connection, choose the interface to use from this list. If you are editing the connection, this list is disabled.
Choose an IPSec Policy	If you are adding a connection, choose the IPSec policy to use from this list. If you are editing the connection, this list is disabled.
Method List for Group Policy Lookup	Choose the method list to use for group policy lookup from this list. Method lists are configured by clicking **Additional Tasks** on the Cisco CP taskbar, and then clicking the AAA node.
Enable User Authentication	Check this check box if you want to require users to authenticate themselves.
Method List for User Authentication	Choose the method list to use for user authentication from this list. Method lists are configured by clicking Additional tasks on the Cisco CP taskbar, and then clicking the AAA node.
Mode Configuration	Check **Initiate** if you want the router to initiate connections with Easy VPN Remote clients. Check **Respond** if you want the router to wait for requests from Easy VPN Remote clients before establishing connections.

Restrict Access

This window allows you to specify which group policies are allowed to use the Easy VPN connection.

Field Reference

Table 27-22 Add a RADIUS Server Fields

Element	Description
Restrict Access	Click **Restrict Access** to enable restrictive access for this Easy VPN connection.

Table 27-22 Add a RADIUS Server Fields (continued)

Element	Description
Check Boxes	Allow a group access to the Easy VPN Server connection by checking its check box. Deny a group access to the Easy VPN Server connection by unchecking its check box.

Group Policies Configuration

This window lets you view, add, clone, and choose group policies for editing or deletion. Group policies are used to identify resources for Easy VPN Remote clients.

Field Reference

Table 27-23 Group Policies Configuration Fields

Element	Description
Common Pool	Click **Common Pool** to designate an existing pool as a common pool for all group policies to use. If no local pools have been configured, this button is disabled. Pools can be configured by clicking **Additional Tasks > Local Pools**, or when you configure Easy VPN Server connections.
Add Edit Clone Delete	Use these buttons to manage group policies on the router. Clicking **Clone** displays the Group Policy edit tabs.
Send Update	Click to send an IKE notification of software or firmware updates to active clients of the chosen group. If this button is disabled, the chosen group does not have client update configured. To set up client update notifications for the chosen group, click the **Edit** button and then click the **Client Update** tab.
Group Name	The name of the group policy.
Pool	The IP address pool used by the clients in this group.
DNS	The DNS servers used by the clients in this group.

Table 27-23 Group Policies Configuration Fields (continued)

Element	Description
WINS	The WINS servers used by the clients in this group.
Domain Name	The domain name used by the clients in this group.
ACL	If split tunneling is specified for this group, this column may contain the name of an ACL that defines which traffic is to be encrypted.
Details Window	The Details window is a list of feature settings and their values for the chosen group policy. Feature settings are displayed only if they are supported by your Cisco router's IOS release, and apply only to the chosen group. The following feature settings may appear in the list: • Authentication—Values indicate a preshared key if one was configured, or a digital certificate if a preshared key was not configured. • Maximum Connections Allowed—Shows the maximum number of simultaneous connections allowed. Cisco CP supports a maximum of 5000 simultaneous connections per group. • Access Restrict—Shows the outside interface to which the specified group is restricted. • Backup Servers—Shows the IP address of backup servers that have been configured. • Firewall Are-U-There—Restricts connections to devices running Black Ice or Zone Alarm firewalls. • Include Local LAN—Allows a connection *not* using split tunneling to access the local stub network at the same time as the client. • PFS (perfect forward secrecy)—PFS is required for IPSec. • Configuration Push, URL, and Version—The server sends a configuration file from the specified URL and with the specified version number to a client. • Group Lock—Clients are restricted to the group. • Save Password—XAuth credentials can be saved on the client.

Table 27-23 Group Policies Configuration Fields (continued)

Element	Description
	• Maximum Logins—The maximum number of connections a user can establish simultaneously. Cisco CP supports a maximum of 10 simultaneous logins per user. • XAuth Banner—The text message shown to clients during XAuth requests.

IP Pools

This window lists the IP address pools available to group policies configured on the router. Depending upon the area of Cisco CP you are working in, **Add**, **Edit**, and **Delete** buttons may be available, and the name of the window varies depending on the area of Cisco CP you are working in. You can use these to manage local IP pools on the router.

Field Reference

Table 27-24 IP Pools Fields

Element	Description
Pool Name Column	The name of the IP address pool.
IP Address Range	The IP address range for the selected pool. A range of 2.2.2.0 to 2.2.2.254 provides 255 addresses.
Cache Size	The size of the cache for this pool.
Group Name	If a local pool is configured with the group option using the CLI, the name of the group is displayed in the group name column. This column is not displayed in all Cisco CP areas. **Note** You cannot configure local pools with the group option using Cisco CP.

Add or Edit IP Local Pool

This window lets you create or edit a local pool of IP addresses.

Field Reference

Table 27-25 Add or Edit IP Local Pool Fields

Element	Description
Pool Name	If you are creating a pool, enter the pool name. If you are editing a pool, this field is disabled.
IP Address Range	Enter or edit the IP address ranges for the pool in this area. A pool can contain more than one IP address range. Use the Add, Edit, and Delete buttons to create additional ranges, edit ranges, and delete IP address ranges.
Cache Size	Enter or edit the cache size for this pool in this field.

Add IP Address Range

This window lets you add an IP address range to an existing pool.

Field Reference

Table 27-26 Add IP Address Range Fields

Element	Description
Start IP Address	Enter the lowest IP address in the range. For example, if you are defining a range between 10.10.10.1 to 10.10.10.254, enter 10.10.10.1.
End IP Address	Enter the highest IP address in the range. For example, if you are defining a range between 10.10.10.1 to 10.10.10.254, enter 10.10.10.254.

CHAPTER 28

Enhanced Easy VPN

The following sections describe the Cisco Configuration Professional configuration screens for Enhanced Easy VPN.

Interface and Authentication

Specify the router interface to which the virtual template interface is to be unnumbered, and specify the method to use for authentication in this window.

Field Reference

Table 28-1 Interface and Authentication

Element	Description
Interface	A virtual template interface must be unnumbered to a router interface to obtain an IP address. Cisco recommends that you unnumber the virtual template interface to a loopback address for greatest flexibility. To do this, click **Unnumbered to new loopback interface** and enter an IP address and subnet mask for the loopback interface. A sample loopback IP address and subnet mask is 127.0.0.1, 255.255.255.0. To unnumber the virtual template interface to another interface, click **Unnumbered to** and choose the interface. You should choose the interface that terminates the tunnel on the router. Click **Details** to view IP address, authentication, policy, and other information about the interface that you are choosing.

Table 28-1 Interface and Authentication (continued)

Element	Description
Authentication	Select the method that Easy VPN clients are to use to authenticate themselves to the Easy VPN Server configured on the router. Pre-shared keys require that you communicate the key to administrators of Easy VPN clients. Digital certificates do not require this, but each client must enroll for and receive a digital certificate.

RADIUS Servers

Identify the RADIUS servers that the router will use for authorization and group policy lookup and the VPN groups configured on the RADIUS servers in the RADIUS Servers window.

Field Reference

Table 28-2 RADIUS Servers Fields

Element	Description
RADIUS Client Source	Configuring the RADIUS source allows you to specify the source IP address to be sent in packets bound for the RADIUS server. To view the IP address and other information about an interface, select the interface and click the **Details** button. This option can have the following values:
	• Router chooses source—Choose **Router chooses source** if you want the source IP address in the RADIUS packets to be the address of the interface through which the RADIUS packets exit the router. • Interface name—If you choose a specific router interface, the source IP address in the RADIUS packets will be the address of that interface. The source IP address in the RADIUS packets sent from the router must be configured as the NAD IP address in the Cisco Access Control Server (ACS) version 3.3 or later.

Table 28-2 RADIUS Servers Fields (continued)

Element	Description
	Note Cisco IOS software allows a single RADIUS source interface to be configured on the router. If the router already has a configured RADIUS source and you choose a different source, the source IP address placed in the packets sent to the RADIUS server changes to the IP address of the new source, and may not match the NAD IP address configured on the Cisco ACS.
RADIUS Server List	
Server IP	The Server IP column lists the IP addresses of each configured server, for example, 192.168.108.14
Parameters	The Parameters column lists the authorization and accounting ports for each server. For example, the column might contain the following entry for a RADIUS server: `Authorization Port 1645; Accounting Port 1646`
Select	The Select column contains a check box for each configured server. Check the box next to each server that you want to be used. The router does not contact a RADIUS server if the box next to it is not checked.
Add	Click **Add** to create an entry for a RADIUS server.
Edit	Select a server entry and click **Edit** to change the information the router has for that server.
Ping	Select a server entry and click **Ping** to test the connection between the router and the RADIUS server.

Table 28-2 RADIUS Servers Fields (continued)

Element	Description
VPN Groups in RADIUS Server	Enter the VPN groups configured on the RADIUS server that you want this connection to give access to. Use a comma to separate entries. A sample set of entries follows: `WGP-1, WGP-2, ACCTG, CSVC` These names must match the group names configured on the RADIUS server. For easy administration, they should also match the group names you configure for the easy VPN clients.
PKI-based Per-user Policy DownLoad	Check **PKI-based Per-user Policy Download** if you want the Easy VPN server to download user-specific attributes from the RADIUS server and push them to the client during mode configuration. The Easy VPN server obtains the username from the client's digital certificate. This option is displayed under the following conditions: • The router runs a Cisco IOS 12.4(4)T or later image. • You choose digital certificate authentication in the IKE policy configuration. • You choose RADIUS or RADIUS and Local group authorization.

Group Authorization and Group User Policies

You can create user groups that each have their own IP address pool, client update configuration, split tunneling configuration, and other custom settings, These group attributes are downloaded to the client in that group when they connect to the Easy VPN server. The same group name must be configured on the clients who are members of the group to ensure that the correct group attributes are downloaded.

Field Reference

Table 28-3 Group Authorization and Group User Policies

Element	Description
Group Policies	If group polices have already been configured, they appear in the list in this window, and you can select them for this connection by checking the Select box to the left of the group name. The group name, IP address pool name, DNS and WINS server names, and domain name of each configured group is shown in the list. When you click **Add** to configure settings for a new group or click **Edit** to change settings, the changes appear in this list. To use settings for an existing group as a basis for a new group configuration, select the existing group and click **Clone**. The Add, Edit, and Clone buttons display dialogs that enable you to configure group settings.
Configure Idle Timer	Check **Configure Idle Timer** if you want to specify how long a connection is to be maintained for idle clients in the Idle Timer fields. Enter time values in HH:MM:SS format. For example, to enter 3 hours, 20 minutes, and 32 seconds, enter the following values in the fields: `03:20:32` The timeout value will apply to all groups configured for this connection.

Add or Edit Easy VPN Server: General Tab

Enter general information for the Easy VPN Server connection in this dialog.

Field Reference

Table 28-4 Add or Edit Easy VPN Server: General Tab

Element	Description
Name for this connection	Enter a name to identify this connection the name that you enter is displayed in the Edit Easy VPN Server window.
IP Address of Virtual Tunnel Interface	Click Interface and Authentication for a description of the IP Address of Virtual Tunnel fields.
Tunnel Mode	Choose **IPSec-IPV4** in the Tunnel Mode field. The IPSec-IPV4 option enables the creation of a IP version 4 IPSec tunnel.
Description	You can enter a description that administrators in you network will find useful when changing configurations or troubleshooting the network.

Add or Edit Easy VPN Server: IKE Tab

The IKE dialog in the Add Easy VPN Server dialogs enables you to create an IKE profile for this connection.

Field Reference

Table 28-5 Add or Edit Easy VPN Server Connection: IKE Tab

Element	Description
Match Identity Type	The IKE profile includes match criteria that allow the router to identify the incoming and outgoing connections to which the IKE connection parameters are to apply. Match criteria can currently be applied to VPN groups. Group is automatically chosen in the Match Identity Type field.

Table 28-5 Add or Edit Easy VPN Server Connection: IKE Tab (continued)

Element	Description
Add VPN groups to be associated with this IKE profile.	Build a list of groups that you want to be included in the match criteria. The groups you add are listed. • Add—Click **Add** to display a menu with the following options: – Add External Group Name—Choose **Add External Group Name** to add the name of a group that is not configured on the router, and enter the name in the dialog displayed. – Select From Local Groups—Choose **Select From Local Groups** to add the name of a group that is configured on the router. In the displayed dialog, check the box next to the group that you want to add. If all the local groups are used in other IKE profiles, Cisco CP informs you that all groups have been selected. • Delete—Choose a group and click **Delete** to remove it from the list.
Mode Configuration	Choose one of the following options to specify how the Easy VPN server is to handle mode configuration requests: • Respond—Choose **Respond** in the Mode Configuration field if the Easy VPN server is to respond to mode configuration requests. • Initiate—Choose **Initiate** if the Easy VPN server is to initiate mode configuration requests. • Both—Choose **Both** if the Easy VPN server is to both initiate and respond to mode configuration requests.
Group Policy Lookup Authorization Policy	Specify an authorization policy that controls access to group policy information on the AAA server. • default—Choose **default** if you want to grant access to group policy lookup information. • Policyname—To specify a policy, choose an existing policy in the list. • Add—Click **Add** to create a policy in the displayed dialog.

Table 28-5 Add or Edit Easy VPN Server Connection: IKE Tab (continued)

Element	Description
User Authentication Policy	Check **User Authentication Policy** if you want to allow XAuth logins, or if you want to specify a user authentication policy to use for XAuth logins. Choose one of the following options: • default—Choose **default** if you want to allow XAuth logins. • Policyname—If policies have been configured on the router, they are displayed in this list and you can select a policy to use. Click **Add** to create a policy in the displayed dialog and use it in this IKE policy.
Dead Peer Discovery	Click **Dead Peer Discovery** to enable the router to send dead peer detection (DPD) messages to Easy VPN Remote clients. If a client does not respond to DPD messages, the connection with it is dropped. • Keepalive Interval—Specify the number of seconds between DPD messages in the Keepalive Interval field. The range is from 10 to 3600 seconds. • Retry Interval—Specify the number of seconds between retries if DPD messages fail in the Retry Interval field. The range is from 2 to 60 seconds. Dead peer discovery helps manage connections without administrator intervention, but it generates additional packets that both peers must process in order to maintain the connection.
Download user attributes from RADIUS server based on PKI certificate fields.	Check this option if you want the Easy VPN server to download user-specific attributes from the RADIUS server and push them to the client during mode configuration. The Easy VPN server obtains the username from the client's digital certificate. This option is displayed under the following conditions: • The router runs a Cisco IOS 12.4(4)T or later image. • You choose digital certificate authentication in the IKE policy configuration. • You choose RADIUS or RADIUS and Local group authorization.

Add or Edit Easy VPN Server: IPSec Tab

Enter the information to create an IPSec profile in this dialog. An IPSec profile specifies the transform sets to be used, how the Security Association (SA) lifetime is to be determined, and other information.

Field Reference

Table 28-6 Add or Edit Easy VPN Server: IPSec Tab

Element	Description
Transform Set Columns	Use the two columns at the top of the dialog to specify the transform sets that you want to include in the profile. The left-hand column contains the transform sets configured on the router. To add a configured transform set to the profile, select it and click the **>>** button. If there are no transform sets in the left-hand column, or if you need a transform set that has not been created, click **Add** and create the transform set in the displayed dialog.
Time Based IPSec SA Lifetime	Click **Time Based IPSec SA Lifetime** if you want a new SA to be established after a set period of time has elapsed. Enter the time period in the HH:MM:SS fields to the right. The range is from 0:2:0 (2 minutes) to 24:0:0 (24 hours).
Traffic Volume Based IPSec SA Lifetime	Click **Traffic Volume Based IPSec SA Lifetime** if you want a new SA to be established after a specified amount of traffic has passed through the IPSec tunnel. Enter the number of kilobytes that should pass through the tunnel before an existing SA is taken down and a new one is established. The range is from 2560 KB to 536870912 KB.
IPSec SA Idle Time	Click IPSec SA Idle Time if you want a new SA to be established after the peer has been idle for a specified amount of time. Enter the idle time period in the HH:MM:SS fields to the right. The range is from 0:1:0 (one minute) to 24:0:0 (24 hours)

Table 28-6 Add or Edit Easy VPN Server: IPSec Tab (continued)

Element	Description
Perfect Forwarding Secrecy	Click **Perfect Forwarding Secrecy** if IPSec should ask for perfect forward secrecy (PFS) when requesting new security associations for this virtual template interface, or should require PFS in requests received from the peer. You can specify the following values: • group1—The 768-bit Diffie-Hellman prime modulus group is used to encrypt the PFS request. • group2—The 1024-bit Diffie-Hellman prime modulus group is used to encrypt the PFS request. • group5—The 1536-bit Diffie-Hellman prime modulus group is used to encrypt the PFS request.

Create Virtual Tunnel Interface

Enter the information for a virtual tunnel interface in this dialog.

Field Reference

Table 28-7 Create Virtual Tunnel Interface

Element	Description
Interface Type	Choose **default**, or **tunnel** as the interface type. If you are editing a virtual tunnel interface, the configured value is displayed and the field is read only
Configure the interface IP address	The IP address of the virtual tunnel interface can be unnumbered to another interface, or it can have no IP address. Choose **IP Unnumbered** and choose an interface name in the Unnumbered to field, or choose **No IP address**.
Tunnel Mode	Cisco CP currently supports the IPSec-IPv4 tunnel mode and it is selected.

Table 28-7 Create Virtual Tunnel Interface (continued)

Element	Description
Select Zone	This field appears when the router runs a Cisco IOS image that supports Zone-Policy Based Firewall (ZPF), and a zone has been configured on the router. If you want this virtual tunnel interface to be a zone member, click the button to the right of this field. Click **Select a Zone** and select the zone that you want the interface to be a member of, or click **Create a Zone** to create a new zone for this interface. **Note** It is not required that the virtual tunnel interface be a member of a zone. However, the router does not forward traffic between zone-member interfaces and non zone-member interfaces.

CHAPTER 29

Dynamic Multipoint VPN

The help topics that follow provide information about configuring Dynamic Multipoint Virtual Private Network (DMVPN).

The following topics provide more information:

- Dynamic Multipoint VPN, page 29-1
- Edit Dynamic Multipoint VPN (DMVPN), page 29-28
- How Do I Configure a DMVPN Manually?, page 29-36

Dynamic Multipoint VPN

A typical Virtual Private Network (VPN) connection is a point-to-point IPSec tunnel connecting two routers. DMVPN enables you to create a network with a central hub that connects other remote routers, referred to as spokes using a GRE over IPSec tunnel. IPSec traffic is routed through the hub to the spokes in the network. Cisco CP allows you to configure your router as a primary or a secondary DMVPN hub, or as a spoke router in a DMVPN network.

See *Dynamic Multipoint IPsec VPNs (Using Multipoint GRE/NHRP to Scale IPsec VPNs)* for more information about DMVPN (requires a CCO login ID):

http://www.cisco.com/en/US/tech/tk583/tk372/technologies_white_paper09186a008018983e.shtml

Cisco CP supports the configuration of a hub-and-spoke DMVPN that uses IPSec profiles to define encryption. You can configure a fully-meshed DMVPN, and use crypto-maps to define encryption in the DMVPN using the CLI. Fully meshed DMVPNs and DMVPNs using crypto maps are managed and modified using the CLI. Cisco CP supports the configuration of a DMVPN starting from IOS version 12.2(13)T.

Cisco CP supports the configuration of a single DMVPN on a router.

The wizards in the Dynamic Multipoint VPN page helps you to configure your router as a DMVPN hub or as a DMVPN spoke.

Related Topics

- Configuring a DMVPN Hub, page 29-3
- Dynamic Multipoint VPN Hub Wizard, page 29-2
- Configuring a DMVPN Spoke, page 29-20
- Dynamic Multipoint VPN Spoke Wizard, page 29-19

Dynamic Multipoint VPN Hub Wizard

This wizard helps you configure your router as a DMVPN hub. The hub should be configured before the spokes so that you can provide the spoke administrators with the information they need to configure their spoke routers.

The application window explains what to configure. After you have finished, you must provide spoke administrators with the following information about the hub:

- IP address of the physical interface of the hub router.
- IP address of the mGRE tunnel interface of the hub.
- Dynamic routing protocol to use to send routing updates to the DMVPN, and the autonomous system (AS) number (for EIGRP), or process ID (for OSPF) that should be used.

Cisco CP's Configure Spoke feature enables you to create a text file that contains the information that spoke administrators need about how the hub is configured. This feature is available from the Summary window of this wizard.

You also need to tell the spoke administrators which subnet mask to use, and assign each spoke an IP address from the same subnet as the hub so that address conflicts do not occur.

Related Topics

- Dynamic Multipoint VPN, page 29-1
- Configuring a DMVPN Hub, page 29-3
- Dynamic Multipoint VPN Spoke Wizard, page 29-19

Configuring a DMVPN Hub

Procedure

To configure your router as a DMVPN hub, complete the following steps.

Step 1 Click **Configure > Security > VPN > Dynamic Multipoint VPN**.

The Dynamic Multipoint VPN page opens with the Create Dynamic Multipoint VPN (DMVPN) tab and the Edit Dynamic Multipoint VPN (DMVPN) tab.

Step 2 Click the Create a hub (server or head-end) in a DMVPN radio button under the Create Dynamic Multipoint VPN (DMVPN) tab.

The hub has to be configured first because spokes are configured using information about the hub.

The DMVPN Hub Wizard is launched.

The Configure a DMVPN hub wizard page informs you about the tasks the wizard helps you accomplish.

Step 3 Click **Next.**

The DMVPN Network Topology wizard page is displayed.

Step 4 Click the Hub and Spoke network radio button or the Fully meshed network radio button.

Step 5 Click **Next**.

The Type of Hub wizard page is displayed.

Step 6 Click the Primary Hub radio button or the Backup Hub radio button. The Backup Hub radio button is dimmed if the network is Hub and Spoke.

Step 7 Click **Next**.

The Multipoint GRE Tunnel Interface Configuration page is displayed.

Step 8 Select the interface that connects to the internet from the drop-down box.

Step 9 Enter the IP address in the IP Address field and the subnet mask in the field below it.

Step 10 Click the **Advanced** button.

Step 11 Click **OK**.

Step 12 Click **Next**.

A Cisco CP Warning message is displayed—Do you use the same router for EasyVPN server?

Step 13 Click **Yes**. The wildcard preshared key is configured only for this DMVPN hub

Click **No**. A global wildcard preshared key is configured.

The Authentication wizard page is displayed.

Step 14 Click the Digital Certificates radio button or the Pre-shared key**s** radio button.

Step 15 Enter the pre-shared key and confirm it in the Reenter key field, if you clicked the Pre-shared keys radio button.

Step 16 Click **Next**.

The IKE Proposals wizard page is displayed.

Step 17 Click the **Add** button to add more policies.

Click the **Edit** button to edit an existing policy.

Step 18 Click **Next**.

The Transform Set wizard page is displayed.

Step 19 Select the transform set from the drop-down box.

The details of the specified transform set are displayed.

Step 20 Click the **Add** button to add more transform sets.

Click the **Edit** button to edit an existing transform set.

Step 21 Click **Next**.

The Select Routing Protocol wizard page is displayed.

Step 22 Click the EIGRP radio button or the OSPF radio button.

Step 23 Click **Next**.

The Routing Information wizard page is displayed.

Step 24 Enter the EIGRP or OSPF information.

Step 25 Click the **Add** button to add a private network to advertise to other routers in this DMVPN.

Select an advertised private network and click the **Edit** button to edit that private network.

Select an advertised private network and click the **Delete** button to delete that private network.

Step 26 Click **Next**.

The Summary of the Configuration page is displayed.

Step 27 Click Spoke Configuration to view information about how to configure a spoke router.

Step 28 Click **Back** to go back and modify any settings.

Click **Cancel** to cancel all the changes you have made without sending them to the router.

Click **Finish** to send your configuration to the router.

DMVPN Hub Reference

This section describes the pages and dialog boxes you can use when working with DMVPN hub and includes the following topics:

- Dynamic Multipoint VPN Page, page 29-6
- DMVPN Hub Wizard—Configure a DMVPN Hub Page, page 29-7

Dynamic Multipoint VPN Page

Use this page to launch the DMVPN Spoke wizard or the DMVPN Hub wizard. You need to identify your router as a hub or as a spoke in the DMVPN network.

It is important to configure the hub first because spokes must be configured using information about the hub. If you are configuring a hub, you can use the Spoke Configuration feature available in the Summary window to generate a procedure that you can send to spoke administrators so that they can configure the spokes with the correct hub information. If you are configuring a spoke, you must obtain the correct information about the hub before you begin.

How to get to this page

Configure > Security > VPN > Dynamic Multipoint VPN

Related Topics

- DMVPN Hub Reference, page 29-5
- DMVPN Hub Wizard—Configure a DMVPN Hub Page, page 29-7

Field Reference

Table 29-1 lists the elements on the Dynamic Multipoint VPN page:

Table 29-1 Dynamic Multipoint VPN Page

Element	Description
Create Dynamic Multipoint VPN (DMVPN) tab	
Create a spoke (client) in Dynamic Multipoint VPN radio button	Click this radio button if your router is a spoke in the DMVPN network. Spokes are the logical endpoints in the network. Before starting configuration, you should ping the hub to be sure you have connectivity to it, and have all the necessary information about the hub configuration that you need. This information is listed in the section Dynamic Multipoint VPN Spoke Wizard, page 29-19.
Create a hub (server or head-end) in Dynamic Multipoint VPN radio button	Click this radio button if your router is a hub in the DMVPN network. The hub is the logical center point in a DMVPN network, and is connected to each spoke router via a point-to-point IPSec connection. The hub can route IPSec traffic between the spoke routers in the network.

Table 29-1 Dynamic Multipoint VPN Page (continued)

Element	Description
Create Dynamic Multipoint VPN (DMVPN) tab	
Edit Dynamic Multipoint VPN (DMVPN) tab	Click the Edit DMVPN tab to edit the DMVPN tunnel configurations.

DMVPN Hub Wizard—Configure a DMVPN Hub Page

Use this page to see a list of the tasks the wizard follows.

You need to:

- Specify the DMVPN network topology
- Specify the hub type
- Configure a multipoint GRE tunnel
- Configure a pre-shared key

How to get to this page

Configure > Security > VPN > Dynamic Multipoint VPN > Create a hub (server or head-end) in a DMVPN.

Related Topics

- DMVPN Hub Wizard—DMVPN Network Topology Page, page 29-7
- Dynamic Multipoint VPN Page, page 29-6

DMVPN Hub Wizard—DMVPN Network Topology Page

Use this page to choose the network topology for the DMVPN traffic.

How to get to this page

Configure > Security > VPN > Dynamic Multipoint VPN > Create a hub (server or head-end) in a DMVPN.

Related Topics

- DMVPN Hub Wizard—Type of Hub Page, page 29-8
- DMVPN Hub Wizard—Configure a DMVPN Hub Page, page 29-7

Field Reference

Table 29-2 lists the elements on the DMVPN Network Topology page:

Table 29-2 DMVPN Network Topology Page

Element	Description
Hub and Spoke network radio button	Click the Hub and Spoke network radio button to choose the hub and spoke network topology. In this topology, all DMVPN traffic is routed through the hub.
Fully meshed network radio button	Click the fully meshed network radio button to choose the fully meshed network topology. In this topology, the spoke dynamically establishes a direct tunnel to another spoke device and sends DMVPN traffic directly to it.

DMVPN Hub Wizard—Type of Hub Page

Use this page to identify the type of hub you are configuring your router to be.

DMVPN networks can be configured with a single hub, or with a primary and a backup hub.

How to get to this page

Configure > Security > VPN > Dynamic Multipoint VPN > Create a hub (server or head-end) in a DMVPN.

Related Topics

- DMVPN Hub Wizard—Multipoint GRE Tunnel Interface Configuration Page, page 29-9
- DMVPN Hub Wizard—DMVPN Network Topology Page, page 29-7

Field Reference

Table 29-3 lists the elements on the Type of Hub page:

Table 29-3 Type of Hub

Element	Description
Primary Hub radio button	Click the Primary Hub radio button if the router is the primary hub in the DMVPN network.
Backup Hub radio button	Click the Backup Hub radio button if the router is a backup hub in a full-mesh DMVPN network. If the router is using a Hub and Spoke network, the Backup Hub radio button is dimmed with the message that Cisco CP does not support backup hub configuration on this router.

DMVPN Hub Wizard—Multipoint GRE Tunnel Interface Configuration Page

Use this page to configure Multipoint Generic Routing Encapsulation (mGRE).

mGRE is used in a DMVPN network to allow a single GRE interface on a hub to support an IPSec tunnel to each spoke router. This greatly simplifies DMVPN configuration. GRE allows routing updates to be sent over IPSec connections.

How to get to this page

Configure > Security > VPN > Dynamic Multipoint VPN > Create a hub (server or head-end) in a DMVPN.

Related Topics

- Advanced Configuration for the Tunnel Interface Button, page 29-11
- DMVPN Hub Wizard—Type of Hub Page, page 29-8

Field Reference

Table 29-4 lists the elements on the Multipoint GRE Tunnel Interface Configuration page:

Table 29-4 Multipoint GRE Tunnel Interface Configuration Page

Element	Description
Select the interface that connects to the Internet drop-down box	Select the router interface that connects to the Internet. The GRE tunnel originates from this interface. Selecting an interface that uses a dialup connection may cause the connection to be always up. You can examine supported interfaces in the Interfaces and Connections tab to determine if an interface uses a dialup connection. Typically, interfaces such as ISDN or Asynchronous Serial are configured for a dialup connection.
IP Address field	Enter the IP address for the mGRE interface. This must be a private address and be in the same subnet as the GRE interfaces of the other routers in the network. For example, the GRE interfaces might share the subnet 10.10.6.0, and be given IP addresses in the range 10.10.6.1 through 10.10.6.254.
Subnet Mask field	Enter the mask for the subnet that the GRE interfaces are in. For example, the mask for the subnet 10.10.6.0 could be 255.255.255.0. For more information, see "IP Addresses and Subnet Masks" section on page 97-1.
Advanced button	Click the Advanced button to configure GRE tunnel parameters. Cisco CP provides default values for advanced tunnel settings. However, the hub administrator must decide on the tunnel settings and give them to the personnel administering spoke routers so that they can make matching settings.

Advanced Configuration for the Tunnel Interface Button

Use this window to configure GRE tunnel parameters.

Cisco CP provides default values, but you must obtain the correct values from the hub administrator and enter them here.

The default values are provided in this help topic. If you change from the default, and need to restore it, consult this help topic.

How to get to this page

Configure > Security > VPN > Dynamic Multipoint VPN > Create a hub (server or head-end) in a DMVPN.

Related Topics

- Cisco CP Warning Message Dialog Box, page 29-12
- DMVPN Hub Wizard—Multipoint GRE Tunnel Interface Configuration Page, page 29-9

Field Reference

Table 29-5 lists the elements on the Advanced Configuration for the Tunnel Interface Button:

Table 29-5 Advanced Configuration for the Tunnel Interface Button

Element	Description
NHRP Authentication String field	Enter the string that DMVPN hubs and spokes must use to authenticate themselves for NHRP transactions. The string can be up to eight characters long. Special characters, such as spaces and question marks (?), are not allowed. All devices in the DMVPN must be configured with the same authentication string. Cisco CP Default: DMVPN_NW
NHRP Network ID field	Enter the NHRP Network ID. The network ID is a globally unique, 32-bit network identifier for a nonbroadcast, multiaccess (NBMA) network. The range is from 1 to 4294967295. Cisco CP Default: 100000

Table 29-5 Advanced Configuration for the Tunnel Interface Button (continued)

Element	Description
NHRP Hold Time field	Enter the number of seconds that NHRP network IDs should be advertised as valid. Cisco CP Default: 360
Tunnel Key field	Enter the key to use for this tunnel. This key should be the same for all mGRE tunnels in the network. Cisco CP Default: 100000
Bandwidth field	Enter the intended bandwidth, in kilobytes per second (kbps). Default bandwidth values are set during startup; the bandwidth values can be displayed using the show interfaces EXEC command. A typical bandwidth setting in DMVPN configurations is 1000. Cisco CP Default: 1000
MTU field	Enter the largest amount of data, in bytes, that should be allowed in a packet travelling through the tunnel. Cisco CP Default: 1400
Tunnel Throughput Delay field	Set a delay value for an interface, in tens of microseconds. Cisco CP Default: 1000

Cisco CP Warning Message Dialog Box

Use this dialog box to configure the wildcard preshared key for the DMVPN hub only or to configure a global wildcard preshared key.

The Cisco CP Warning Message asks if you use the same router for EasyVPN server.

Related Topics

- DMVPN Hub Wizard—Authentication Page, page 29-13
- Advanced Configuration for the Tunnel Interface Button, page 29-11

Field Reference

Table 29-6 lists the elements on the Cisco CP Warning Message Dialog Box:

Table 29-6 Cisco CP Warning Message Dialog Box

Element	Description
Yes button	Click **Yes**. The wildcard preshared key is configured only for this DMVPN hub.
No button	Click **No**. The global wildcard preshared key is configured.

DMVPN Hub Wizard—Authentication Page

Use this page to configure a pre-shared key or a digital certificate.

DMVPN peers can use a pre-shared key or digital certificates to authenticate connections from each other. If pre-shared keys are used, each hub router and spoke router in the network must use the same pre-shared key.

Pre-shared keys should be exchanged with the administrator of the remote site through some secure and convenient method, such as an encrypted e-mail message.

How to get to this page

Configure > Security > VPN > Dynamic Multipoint VPN > Create a hub (server or head-end) in a DMVPN.

Related Topics

- DMVPN Hub Wizard—IKE Proposals Page, page 29-14
- Cisco CP Warning Message Dialog Box, page 29-12

Field Reference

Table 29-7 lists the elements on the Authentication page:

Table 29-7 Authentication page

Element	Description
Digital Certificates radio button	Click the Digital Certificate radio button if your router uses digital certificates for authentication. Digital certificates are configured under **VPN Components > Public Key Infrastructure**.
Pre-shared Keys radio button	Click the Pre-shared Keys radio button if your router uses a pre-shared key for authentication.
pre-shared key field	Enter the pre-shared key used in the DMVPN network. Question marks (?) and spaces must not be used in the pre-shared key. The pre-shared key can contain a maximum of 128 characters. The pre-shared key field is available if the Pre-shared Keys radio button is clicked.
Reenter key field	Reenter the key for confirmation. If the values in this field and the Pre-Shared Key field do not match, Cisco CP prompts you to reenter them. The Reenter key field is available if the Pre-shared Keys radio button is clicked.

DMVPN Hub Wizard—IKE Proposals Page

See IKE Proposals, page 25-8

Primary Hub Page

If the router you are configuring is the backup hub in the DMVPN network, you need to identify the primary hub by providing its public and private IP addresses.

Field Reference

Table 29-8 lists the elements on the Primary Hub page:

Table 29-8 Primary Hub

Element	Description
Public IP Address	Enter the IP address of the interface on the primary hub that is used for this tunnel. This should be a static IP address. Obtain this information from the hub administrator.

Table 29-8 Primary Hub (continued)

Element	Description
IP Address of hub's mGRE tunnel interface	Enter the IP address of the mGRE tunnel interface on the primary hub. Obtain this information from the hub administrator.

DMVPN Hub Wizard—Transform Set

See Transform Set, page 25-11

DMVPN Hub Wizard—Select Routing Protocol Page

Use this page to specify how other networks behind your router are advertised to the other routers in the network. Select one of the protocols in Table 29-9.

How to get to this page

Configure > Security > VPN > Dynamic Multipoint VPN > Create a hub (server or head-end) in a DMVPN

Related Topics

- DMVPN Hub Wizard—Routing Information Page, page 29-16
- DMVPN Hub Wizard—Transform Set, page 29-15

Field Reference

Table 29-9 lists the elements on the Select Routing Protocol page:

Table 29-9 Select Routing Protocol

Element	Description
EIGRP radio button	Click the EIGRP radio button to select the EIGRP protocol. Extended Interior Gateway Routing Protocol.
OSPF radio button	Click the OSPF radio button to select the OSPF protocol. Open Shortest Path First.

Table 29-9 Select Routing Protocol (continued)

Element	Description
EIGRP radio button	Click the EIGRP radio button to select the EIGRP protocol. Extended Interior Gateway Routing Protocol.
RIP radio button	Click the RIP radio button to select the RIP protocol. Routing Internet Protocol.
Static Routing radio button	This option is enabled when you are configuring a GRE over IPSec tunnel.

Note RIP is not supported for DMVPN Hub and spoke topology but is available for DMVPN Full Mesh topology.

DMVPN Hub Wizard—Routing Information Page

Use this page to add or edit routing information about networks behind the router to advertise to the other routers in the network. The fields on this page vary according to the routing protocol specified.

For more information on RIP parameters, see "Add or Edit an RIP Route" section on page 13-5.

For more information on EIGRP parameters, see "Add or Edit EIGRP Route" section on page 13-7.

For more information on OSPF parameters, see "Add or Edit an OSPF Route" section on page 13-5.

How to get to this page

Configure > Security > VPN > Dynamic Multipoint VPN > Create a hub (server or head-end) in a DMVPN

Related Topics

- DMVPN Hub Wizard—Summary of the Configuration Page, page 29-18
- DMVPN Hub Wizard—Select Routing Protocol Page, page 29-15

Field Reference

Table 29-10 lists the elements on the Routing Information page:

Table 29-10 Routing Information

Element	Description
Please select the version of RIP to enable	Specify RIP version 1 or version 2.
Select an existing OSPF process ID/EIGRP AS number	You can select an existing process ID for OSPF or AS number for EIGRP if one has been previously configured. See "Recommendations for Configuring Routing Protocols for DMVPN" section on page 97-29.
Create a new OSPF process ID/EIGRP AS number	If no process IDs exist, or to use a different one, configure a process ID in this field.
OSPF Area ID for tunnel network	Enter a new OSPF area ID for the network. This area ID is for the tunnel network. Cisco CP automatically adds the tunnel network to this process using this area ID.
Private networks advertised using <*protocol-name*>	This area shows the networks advertised using the selected routing protocol. If you have already configured the routing protocol you specified in this wizard, the networks that you specified to be advertised appears in this list. Add all the private networks that you want to advertise to the DMVPN peers using this routing process. The DMVPN wizard automatically adds the tunnel network to this process.
Network	A network address. You can enter the address of a specific network, and use the wildcard mask to generalize the advertisement.
Wild card mask	EIGRP and OSPF protocols. A bit mask that specifies how much of the network address must match the address given in the network column. This mask can be used to have the router advertise networks in a particular range, based on the given address. A 0 bit specifies that the bit in the network address must match the corresponding bit in the given network address. For example, if the network address were 172.55.10.3, and the wildcard mask was 0.0.255.255, the router would advertise all networks starting with the numbers 172.55, not just the network 172.55.10.3.

Table 29-10 Routing Information (continued)

Element	Description
Area	Shown when OSPF is selected, the OSPF area number for that network. Each router in a particular OSPF area maintains a topological database for that area.
Add	Click to add a network or a group of networks, to advertise.
Edit	Click to edit the data for an advertised network or group of networks. This button is enabled for entries that you created during the current instance of this wizard.
Delete	Click to delete the data for the selected network or group of networks. This button is enabled for entries that you created during the current instance of this wizard.

DMVPN Hub Wizard—Summary of the Configuration Page

See Summary of the Configuration, page 25-14.

Dynamic Multipoint VPN Spoke Wizard

This wizard helps you to configure your router as a spoke in a DMVPN network. Before starting the configuration, you should ping the hub to be sure that your router can send traffic to it. Also you should have all the information about the hub you need before you begin. A hub administrator who uses Cisco CP to configure the hub can generate a text file that contains the hub information spoke administrators need.

You need to obtain the following information before you begin:

- The IP address of the hub's physical interface.
- The IP address of the hub's mGRE tunnel interface.
- The IP address and subnet mask the hub administrator tells you to use for your spoke. The hub administrator must assign addresses to each spoke to ensure that all routers in the DMVPN are in the same subnet, and that each is using a unique address.
- The routing protocol to use, and the AS number (EIGRP) or Process ID (OSPF) that is to be used to send routing updates in the DMVPN.

Related Topics

- Configuring a DMVPN Spoke, page 29-20
- DMVPN Spoke Reference, page 29-22

Configuring a DMVPN Spoke

Procedure

Use this procedure to configure your router as a DMVPN spoke.

Step 1 Click **Configure > Security > VPN > Dynamic Multipoint VPN**.

The Dynamic Multipoint VPN page opens with the Create Dynamic Multipoint VPN (DMVPN) tab and the Edit Dynamic Multipoint VPN (DMVPN) tab.

Step 2 Click the Create a spoke (client) in a DMVPN radio button under the Create Dynamic Multipoint VPN (DMVPN) tab.

The hub has to be configured first as spokes are configured using information about the hub.

The DMVPN Spoke Wizard is launched.

The Configure a DMVPN spoke wizard page tells you about the tasks the wizard helps you accomplish.

Step 3 Click **Next.**

The DMVPN Network Topology wizard page is displayed.

Step 4 Click the Hub and Spoke network radio button or the Fully meshed network radio button.

Step 5 Click **Next**.

The Specify Hub information wizard page is displayed.

Step 6 Enter the IP address of the hub and the IP address of the hub's mGRE tunnel interface.

Step 7 Click **Next**.

The GRE Tunnel Interface Configuration page is displayed.

Step 8 Select the interface that connects to the internet from the drop-down box.

Step 9 Enter the IP address in the IP Address field and the subnet mask in the field below it.

Step 10 Click the **Advanced** button.

Step 11 Verify the values and click **OK**.

Step 12 Click **Next**.

The Authentication wizard page is displayed.

Step 13 Click the Digital Certificates radio button or the Pre-shared keys radio button.

Step 14 Enter the pre-shared key and confirm it in the Reenter key field, if you clicked the Pre-shared keys radio button.

Step 15 Click **Next**.

The IKE Proposals wizard page is displayed.

Step 16 Click the **Add** button add more policies.

Click the **Edit** button to edit an existing policy.

Step 17 Click **Next**.

The Transform Set wizard page is displayed.

Step 18 Select the transform set from the drop-down box.

The details of the specified transform set are displayed.

Step 19 Click the **Add** button to add more transform sets.

Click the **Edit** button to edit an existing transform set.

Step 20 Click **Next**.

The Select Routing Protocol wizard page is displayed.

Step 21 Click the EIGRP radio button or the OSPF radio button.

Step 22 Click **Next**.

The Routing Information wizard page is displayed.

Step 23 Enter EIGRP or OSPF information.

Step 24 Click the **Add** button to add a private network that you want to advertise to other routers in this DMVPN.

Select an advertised private network and click the **Edit** button to edit that private network.

Select an advertised private network and click the **Delete** button to delete that private network.

Step 25 Click **Next**.

The Summary of the Configuration page is displayed.

Step 26 Click **Back** to go back and modify any settings.

Click **Cancel** to cancel all the changes you have made without sending them to the router.

Click **Finish** to send your configuration to the router.

DMVPN Spoke Reference

This section describes the pages and dialog boxes you can use when working with DMVPN spoke and includes the following topics:

- Dynamic Multipoint VPN Page, page 29-6
- DMVPN Spoke Wizard—Configure a DMVPN spoke Page, page 29-22

DMVPN Spoke Wizard—Configure a DMVPN spoke Page

Use this page to see a list of the tasks the wizard takes you through.

You need to:

- Specify the DMVPN network topology
- Provide hub information
- Configure a GRE tunnel interface
- Configure a pre-shared key

How to get to this page

Configure > Security > VPN > Dynamic Multipoint VPN > Create a spoke (client) in a DMVPN.

Related Topics

- DMVPN Spoke Wizard—DMVPN Network Topology Page, page 29-23
- DMVPN Spoke Reference, page 29-22

DMVPN Spoke Wizard—DMVPN Network Topology Page

Use this page to select the type of DMVPN network this router is a part of.

How to get to this page

Configure > Security > VPN > Dynamic Multipoint VPN > Create a spoke (client) in a DMVPN.

Related Topics

- DMVPN Spoke Wizard—Specify Hub Information Page, page 29-24
- DMVPN Spoke Wizard—Configure a DMVPN spoke Page, page 29-22

Field Reference

Table 29-11 lists the elements on the DMVPN Network Topology page:

Table 29-11 DMVPN Network Topology Page

Element	Description
Hub and Spoke Network	Select this option if you are configuring the router in a network where each spoke router has a point-to-point GRE over IPSec connection to the DMVPN hub, and will send traffic destined for other spokes through the hub. When you select this option, the graphic displays links from the spokes to the hub.
Fully Meshed Network	Select this option if you are configuring the router as a spoke capable of establishing a direct IPSec tunnel to other spokes in the network. A multipoint GRE tunnel is configured on the spoke to support this functionality. When you select this option, the graphic displays links from the spokes to the hub, and links to each other. The wizard screen lists the IOS images required to support a fully-meshed DMVPN network.

DMVPN Spoke Wizard—Specify Hub Information Page

Use this page to provide necessary information about the hub in the DMVPN.

How to get to this page

Configure > Security > VPN > Dynamic Multipoint VPN > Create a spoke (client) in a DMVPN.

Related Topics

- DMVPN Spoke Wizard—GRE Tunnel Interface Configuration Page, page 29-24
- DMVPN Spoke Wizard—DMVPN Network Topology Page, page 29-23

Field Reference

Table 29-12 lists the elements on the Specify Hub Information page:

Table 29-12 Specify Hub Information Page

Element	Description
IP Address of Hub's physical interface	Enter the IP address of the interface on the hub. Obtain this address from the hub administrator. This address will be used as the tunnel destination.
IP Address of hub's mGRE tunnel interface	Enter the IP address of the mGRE tunnel interface on the hub. The mGRE tunnel addresses for the hub and spokes must be in the same subnet.

DMVPN Spoke Wizard—GRE Tunnel Interface Configuration Page

Use this page to create a point-to-point connection for the spoke.

How to get to this page

Configure > Security > VPN > Dynamic Multipoint VPN > Create a spoke (client) in a DMVPN.

Related Topics

- DMVPN Spoke Wizard—Cisco CP Warning: DMVPN Dependency Page, page 29-26

- DMVPN Spoke Wizard—Specify Hub Information Page, page 29-24

Field Reference

Table 29-13 lists the elements on the GRE Tunnel Interface Configuration page:

Table 29-13 GRE Tunnel Interface Configuration Page

Element	Description
Select the interface that connects to the Internet	Select the router interface that connects to the Internet. The GRE over IPSec tunnel originates from this interface. Selecting an interface that uses a dialup connection may cause the connection to be always up. You can examine supported interfaces in Interfaces and Connections to determine if a dialup connection, such as an ISDN or Async connection has been configured for the physical interface you selected. **Re-register with hub when IP address of *interface-name* changes**—This option is available when the interface you selected receives a dynamic IP address via DHCP or IPCP. Specifying' this option will allow the spoke to re-register with the hub when it receives a new IP address.
IP Address	Enter the IP address for the GRE interface to this hub. This must be a private address and be in the same subnet as the GRE interfaces of the other routers in the network. For example, the GRE interfaces might share the subnet 10.10.6.0, and be given IP addresses in the range 10.10.6.1 through 10.10.6.254. If you are configuring a spoke router, you must use the IP address assigned to your router by the hub administrator. Failure to do so may result in address conflicts.
Subnet Mask	Enter the mask for the subnet that the GRE interfaces are in. This mask must be assigned by the hub administrator and be the same for all routers in the DMVPN. For example, the mask for the subnet 10.10.6.0 could be 255.255.255.0. For more information, see "IP Addresses and Subnet Masks" section on page 97-1.

Table 29-13 GRE Tunnel Interface Configuration Page (continued)

Element	Description
Advanced Button	Click this button to provide NHRP and tunnel parameters for this connection. Cisco CP provides default values for advanced tunnel settings. However, the hub administrator must decide on the tunnel settings and give them to the personnel administering spoke routers so that they can make matching settings. If you are configuring a spoke router, obtain the tunnel settings from the hub administrator, click this button, and enter them in the dialog box displayed.

DMVPN Spoke Wizard—Cisco CP Warning: DMVPN Dependency Page

This page appears when the interface you have chosen for the DMVPN tunnel source has a configuration that prevents its use for DMVPN. Cisco CP lists the conflict and gives you the option of allowing Cisco CP to modify the configuration so that the conflict is removed.

How to get to this page

Configure > Security > VPN > Dynamic Multipoint VPN > Create a spoke (client) in a DMVPN.

Related Topics

- DMVPN Spoke Wizard—Summary of the Configuration Page, page 29-27
- DMVPN Spoke Wizard—GRE Tunnel Interface Configuration Page, page 29-24

Field Reference

Table 29-14 lists the elements on the Cisco CP Warning: DMVPN Dependency page:

Table 29-14 Cisco CP Warning: DMVPN Dependency Page

Element	Description
Firewall	If a firewall has been applied to the interface that was designated as the tunnel source, Cisco CP can add access rule entries to the configuration so that GRE, IPSec, and ISAKMP traffic is allowed through the firewall.
View Details	Click this button to view the access control entries that Cisco CP will add to the access rule if you select **Allow GRE, IPSec, and ISAKMP traffic through the firewall**. These entries allow both kinds of ISAKMP traffic, GRE traffic, Encapsulating Security Protocol (ESP), and Authentication Header Protocol (AHP).

DMVPN Spoke Wizard—Summary of the Configuration Page

See Summary of the Configuration, page 25-14

Edit Dynamic Multipoint VPN (DMVPN)

This window displays the existing DMVPN tunnel configurations. DMVPN enables you to create a network with a central hub that connects other remote routers, referred to as spokes. Cisco CP supports hub-and-spoke network topology, in which GRE over IPSec traffic is routed through the hub. Cisco CP allows you to configure your router as a primary or a secondary DMVPN hub, or as a spoke router in a DMVPN network.

Cisco CP supports the configuration of a hub-and-spoke DMVPN that uses IPSec profiles to define encryption. You can configure a fully meshed DMVPN, and use crypto-maps to define encryption in the DMVPN using the CLI. Fully meshed DMVPNs and DMVPNs using crypto maps are managed and modified using the CLI.

Cisco CP supports the configuration of a single DMVPN on a router.

The hub should be configured first, to establish the hub IP addresses and the routing parameters that the *spokes* must be configured with. For other recommendations on how to configure the routers in a DMVPN, see "DMVPN Configuration Recommendations" section on page 97-29.

How to get to this page

Configure > Security > VPN > Dynamic Multipoint VPN > Edit Dynamic Multipoint VPN (DMVPN).

Related Topics

- Dynamic Multipoint VPN, page 29-1
- General Panel, page 29-30
- NHRP Panel, page 29-31
- Routing Panel, page 29-34

Field Reference

Table 29-15 lists the elements on the Edit Dynamic Multipoint VPN page:

Table 29-15 Edit Dynamic Multipoint VPN

Element	Description
Interface	Physical interface from which this tunnel originates.
IPSec Profile	IPSec profile that the tunnel uses. The IPSec profile defines the transform sets that are used to encrypt traffic on the tunnel. Cisco CP supports the use of only IPSec profiles to define encryption in a DMVPN. If you want to use crypto-maps, configure the DMVPN using the CLI.
IP Address	IP address of the GRE tunnel. The GRE tunnel is used to send routing updates to the DMVPN.
Description	Description of this tunnel.
Details panel	Details panel shows the values for the entire configuration of the DMVPN tunnel.
Add	Click to add a new DMVPN tunnel configuration.
Edit	Click to edit a selected DMVPN tunnel configuration.
Delete	Click to delete a DMVPN tunnel configuration.

Why Are some Tunnel Interfaces Shown as Read-Only?

A tunnel interface is shown as read-only if it has already been configured with crypto-map associations and NHRP parameters. You can modify NHRP parameters and routing information from this window, but you must edit the IP address, tunnel source, and tunnel destination from the Interfaces and Connections window.

General Panel

Use this panel to add or edit general configuration parameters of the DMVPN tunnel.

How to get to this page

Configure > Security > VPN > Dynamic Multipoint VPN > Edit Dynamic Multipoint VPN (DMVPN) > Add.

Related Topics

- NHRP Panel, page 29-31
- Edit Dynamic Multipoint VPN (DMVPN), page 29-28

Field Reference

Table 29-16 lists the elements on the General Panel page:

Table 29-16 General Panel

Element	Description
IP Address	Enter the IP address of the tunnel. This must be a private address and must be in the same subnet as the other tunnel addresses in the DMVPN. If you are configuring a spoke, you must use the address that the hub administrator has assigned to your router so that no address conflicts occur.
Mask	Enter the subnet mask that the hub administrator has assigned to the DMVPN. For more information, see "IP Addresses and Subnet Masks" section on page 97-1.
Tunnel Source	Select the interface that the tunnel is to use, or enter that interface's IP address. See "Using Interfaces with Dialup Configurations" section on page 97-30 before you select an interface configured for a dialup connection.
Tunnel Destination	Click **This is a multipoint GRE tunnel** if this is a DMVPN tunnel in a fully meshed network. Click **IP/Hostname** and specify an IP address or hostname if this is a hub-and-spoke network
IPSec Profile	Select a configured IPSec profile for this tunnel. The IPSec profile defines the transform sets that are used to encrypt traffic on this tunnel.

Table 29-16 General Panel (continued)

Element	Description
MTU	Enter the largest amount of data, in bytes, that should be allowed in a packet traveling through the tunnel.
Bandwidth	Enter the intended bandwidth, in kilobytes per second (kbps). Default bandwidth values are set during startup; the bandwidth values can be displayed using the show interfaces EXEC command. The value 1000 is a typical bandwidth setting in DMVPN configurations.
Delay	Set a delay value for an interface, in tens of microseconds. The value 1000 is a typical delay setting in DMVPN configurations.
Tunnel Key	Enter the key to use for this tunnel. This key should be the same for all mGRE tunnels in the network.
This is a multipoint GRE Tunnel	Check if this to be an mGRE tunnel interface, an interface capable of maintaining connections to multiple peers. If this router is being configured as a DMVPN hub, you must check this box to allow the hub to establish connections with all spokes. If the router is being configured as a spoke, check this box if you are configuring a fully meshed DMVPN. In this way, a spoke can establish a connection to the hub to send traffic and receive next hop information to directly connect to all other spokes in the DMVPN.

NHRP Panel

Use this panel to provide NHRP configuration parameters.

How to get to this page

Configure > Security > VPN > Dynamic Multipoint VPN > Edit Dynamic Multipoint VPN (DMVPN) > Add.

Related Topics

- NHRP Map Configuration, page 29-32
- General Panel, page 29-30

Field Reference

Table 29-17 lists the elements on the NHRP Panel page:

Table 29-17 NHRP Panel

Element	Description
Authentication String	Enter the string that DMVPN hubs and spokes must use to authenticate themselves for NHRP transactions. The string can be up to eight characters long. All NHRP stations in the DMVPN must be configured with the same authentication string.
Hold Time	Enter the number of seconds that NHRP network IDs should be advertised as valid.
Network ID	Enter the NHRP Network ID. The network ID is a globally unique, 32-bit network identifier for a nonbroadcast, multiaccess (NBMA) network. The range is 1 to 4294967295. The network ID must be unique for each NHRP station.
Next Hop Server	This area lists the IP addresses of the next hop servers that this router can contact. This area must contain the IP address of the primary and secondary hub if this is a spoke router. If this is a hub, this area must contain the IP addresses of the other hub routers in the DMVPN. Click **Add** to enter the IP address of a next hop server. Select a server, and click **Delete** to delete it from the list.
NHRP Map	This area lists the available IP-to-NBMA address mappings. Click **Add** to create a new map. After you create the map, it will be added to this list. Click **Edit** to modify a selected map. Click **Delete** to remove a selected map configuration.

NHRP Map Configuration

Use this window to create or edit a mapping between IP and NBMA addresses.

How to get to this page

Configure > Security > VPN > Dynamic Multipoint VPN > Edit Dynamic Multipoint VPN (DMVPN) > Add > NHRP > NHRP Map > Add.

Related Topics

- Routing Panel, page 29-34
- NHRP Panel, page 29-31

Field Reference

Table 29-18 lists the elements on the NHRP Map Configuration page:

Table 29-18 NHRP Map Configuration

Element	Description
Statically configure the IP-to-NMBA address mapping of IP destinations connected to an NBMA network.	Click this button if you are configuring a spoke in a fully meshed network. Cisco CP treats backup hubs as spokes to primary hubs, so also click this if you are configuring a backup hub. In this part of the window you are providing the address information that the spoke or backup hub needs to contact the primary hub.
Destination Reachable through NBMA network	Enter the IP address of the mGRE tunnel configured on the primary hub. Spokes and backup hubs use this tunnel information to establish contact with the hub and create an mGRE tunnel to it. Spokes use the tunnel to send encrypted data to the hub and to query the hub for next hop information to other spokes.
NBMA Address directly reachable	Enter the static IP Address of the interface on the primary hub that supports the mGRE tunnel.
Configure NBMA addresses used as destinations for broadcast or multicast packets to be sent over a tunnel network.	Use this area of the window to provide information used by routing protocols.
Dynamically add spokes' IP addresses to hub's multicast cache	Configure this option if you are configuring a primary or a backup hub. This option is needed by the hub to send routing updates to all connected DMVPN spokes.
IP address of NBMA address directly reachable	If you are configuring a spoke in a full meshed DMVPN, or a backup hub, check this box, and provide the static IP Address of the interface on the primary hub that supports the mGRE tunnel.

Routing Panel

Use this panel to configure routing information for the DMVPN cloud.

How to get to this page

Configure > Security > VPN > Dynamic Multipoint VPN > Edit Dynamic Multipoint VPN (DMVPN) > Add

Related Topics

- NHRP Panel, page 29-31
- General Panel, page 29-30

Field Reference

Table 29-19 lists the elements on the Routing Panel page:

Table 29-19 Routing Panel

Element	Description
Routing Protocol	Select the dynamic routing protocol that the hub and spoke routers in this DMVPN use to perform routing. Note that all the routers in the DMVPN must be configured for the routing protocol that you select. • RIP—Routing Internet Protocol • OSPF—Open Shortest Path First • EIGRP—Extended Interior Gateway Routing Protocol
RIP Fields	If you selected RIP as the dynamic routing protocol, select **Version 1**, **Version 2**, or **Default**. If you select **Version 2**, the router will include the subnet mask in the routing update. If you select **Default**, the router will send out Version 2 updates, but it will be able to receive RIP Version 1 or Version 2 updates. **Turn off split horizon**—If this is the hub router, check this box to turn off split horizon on the GRE tunnel interface. Turning off split horizon allows the router to advertise the routes that it has learned from the tunnel interface out the same interface.
OSPF Fields	If you selected OSPF, the following fields must be completed:

Table 29-19 Routing Panel (continued)

Element	Description
OSPF process ID	Enter the process ID. This value identifies the OSPF process to other routers. See "Recommendations for Configuring Routing Protocols for DMVPN" section on page 97-29.
OSPF Network Type	Select point-to-multipoint or broadcast. Point-to-multipoint causes OSPF to add routes to the routing table on spoke routers. If you wish to avoid this, you can select broadcast.
OSPF Priority	OSPF priority identifies this router as a hub or as a spoke. If this is a hub router, enter a priority value of 2. If this is a spoke router, enter a priority value of 0.
EIGRP Fields	If you selected EIGRP, complete the following fields:
Autonomous System Number	Enter the Autonomous System Number for the group of routers using EIGRP. Routers with the same EIGRP autonomous system number maintain a topological database of routers in the region identified by that number. See "Recommendations for Configuring Routing Protocols for DMVPN" section on page 97-29.
Turn off split Horizon	If this is the hub router, check this box to turn off split horizon on the mGRE tunnel interface. Leave it unchecked to enable split horizon. Turning off split horizon allows the router to advertise the routes that it has learned from the tunnel interface out the same interface.
Use original next hop	If this is a DMVPN hub router, EIGRP will advertise this router as the next hop. Check this box to have EIGRP use the original IP next hop when advertising routes to the DMVPN spoke routers.

How Do I Configure a DMVPN Manually?

You can configure your router as a DMVPN hub or spoke using the VPN Components windows and the Edit Dynamic Multipoint VPN (DMVPN) window. You need to complete the following tasks:

- Configure an IPSec profile. You cannot configure a DMVPN connection until you have configured at least one IPSec profile.
- Configure the DMVPN connection.
- Specify the networks you want to advertise to the DMVPN cloud.

Procedures for these tasks are given below:

To configure an IPSec Profile:

You need to configure an IPSec policy, and then configure a DMVPN tunnel.

Step 1 In the Feature bar, click **Configure > Security > VPN > VPN Components > IPSec.**

Step 2 Click the IPSec Profiles branch, and then click **Add** in the IPSec Profiles window.

Step 3 Name the profile, and select the transform sets it is to contain in the Add an IPSec profile window. You can enter a short description.

Step 4 Click **OK**.

To configure a DMVPN connection:

Step 1 In the Feature bar, click **Configure > Security > VPN > Dynamic Multipoint VPN**.

Step 2 Click **Edit Dynamic Multipoint VPN** (**DMVPN**).

Step 3 Click **Add**.

Step 4 In the DMVPN Tunnel Configuration window, complete the General, NHRP, and Routing tabs to create a DMVPN tunnel. Consult the online help for more information about a particular field.

To specify the networks you want to advertise to the DMVPN:

If there are networks behind your router that you want to advertise to the DMVPN, you can do so by adding the network numbers in the Routing windows.

Step 1 From the Feature bar, click **Configure > Router > Static and Dynamic Routing**.

Step 2 In the Routing window, select the routing protocol that you specified in DMVPN configuration, and click **Edit**.

Step 3 Add the network numbers to advertise.

Related Topics

- Configuring a DMVPN Hub, page 29-3
- Configuring a DMVPN Spoke, page 29-20
- Dynamic Multipoint VPN Hub Wizard, page 29-2
- Dynamic Multipoint VPN Spoke Wizard, page 29-19

CHAPTER 30

GETVPN

For information about how to use Cisco Configuration Professional (Cisco CP) to configure the GETVPN feature, see the screencast at: http://www.cisco.com/en/US/docs/net_mgmt/cisco_configuration_professional/scrcst/ccpsc.html.

Note You must have internet access to view the screencast.

CHAPTER 31

Cisco IOS SSL VPN

Cisco IOS SSL VPN provides Secure Socket Layer (SSL) VPN remote-access connectivity from almost any Internet-enabled location using only a web browser and its native SSL encryption. This enables companies to extend their secure enterprise networks to any authorized user by providing remote-access connectivity to corporate resources from any Internet-enabled location.

Cisco IOS SSL VPN also enables access from noncorporate-owned machines, including home computers, Internet kiosks, and wireless hotspots, where an IT department cannot easily deploy and manage the VPN client software necessary for IPsec VPN connections.

There are three modes of SSL VPN access: clientless, thin-client and full-tunnel client. Cisco CP supports all three. Each mode is described below:

- **Clientless SSL VPN**—Clientless mode provides secure access to private web resources and will provide access to web content. This mode is useful for accessing most content that you would expect to use within a web browser, such as intranet access, and online tools that employ a web interface.
- **Thin Client SSL VPN** (port-forwarding Java applet)—Thin Client mode extends the capability of the cryptographic functions of the web browser to enable remote access to TCP-based applications such as POP3, SMTP, IMAP, Telnet, and SSH.
- **Full Tunnel Client SSL VPN**—Full tunnel client mode offers extensive application support through its dynamically downloaded SSL VPN client software for Cisco IOS SSL VPN. With the Full tunnel Client for Cisco IOS SSL VPN, we delivers a lightweight, centrally configured and easy-to-support SSL VPN tunneling client that allows network layer connectivity access to virtually any application.

To read more, you can click Cisco IOS SSL VPN Links on Cisco.com for links to Cisco IOS SSL VPN documents.

This chapter contains the following sections:

- Creating an SSL VPN Connection
- Editing SSL VPN Connections
- Editing SSL VPN Gateways
- Installing Software Packages
- Additional Help Topics

Creating an SSL VPN Connection

To create an SSL VPN connection, complete the following tasks:

Step 1 On the Cisco CP Feature bar, click **Configure > Security > VPN > SSL VPN > SSL VPN Manager**.

Step 2 In the Create SSL VPN tab, complete any recommended tasks that are displayed by clicking the link for the task. Cisco CP either completes the task for you, or displays the necessary configuration screens for you to make settings in.

Step 3 Choose the task you want to complete. If you are creating the first SSL VPN connection, choose **Create a new SSL VPN**.

Step 4 Click **Launch the selected task** to begin configuring the connection.

Step 5 Make configuration settings in the wizard screens. Click **Next** to go from the current screen to the next screen. Click **Back** to return to a screen you have previously visited.

Step 6 Cisco CP displays the Summary screen when you have completed the configuration. Review the configuration. If you need to make changes, click **Back** to return to the screen in which you need to make changes, then return to the Summary screen.

Create an SSL VPN Connection Reference describes the screens that you use to complete this task.

Cisco IOS SSL VPN Contexts, Gateways, and Policies provides a complete configuration example.

Create an SSL VPN Connection Reference

The topics in this section describe the Create SSL VPN screens.

- Create SSL VPN
- Persistent Self-Signed Certificate
- Welcome
- SSL VPN Gateways
- User Authentication
- Configure Intranet Websites
- Add or Edit URL
- Customize SSL VPN Portal
- SSL VPN Passthrough Configuration
- User Policy
- Details of SSL VPN Group Policy: Policyname
- Select the SSL VPN User Group
- Select Advanced Features
- Thin Client (Port Forwarding)
- Add or Edit a Server
- Full Tunnel
- Enable Cisco Secure Desktop
- Common Internet File System
- Enable Clientless Citrix
- Summary

Create SSL VPN

You can use Cisco IOS SSL VPN wizards to create a new Cisco IOS SSL VPN or to add new policies or features to an existing Cisco IOS SSL VPN.

Related Links

- Cisco IOS SSL VPN
- Cisco IOS SSL VPN Contexts, Gateways, and Policies
- Cisco IOS SSL VPN Links on Cisco.com

Prerequisite Tasks

AAA and certificates must be configured on the router before you can begin a Cisco IOS SSL VPN configuration. If either or both of these configurations are missing, a notification appears in this area of the window, and a link is provided that enables you to complete the missing configuration. When all prerequisite configurations are complete, you can return to this window and start configuring Cisco IOS SSL VPN.

Cisco CP enables AAA without user input. Cisco CP can help you generate public and private keys for the router, and enroll them with a certification authority to obtain digital certificates. See Public Key Infrastructure for more information. Alternatively, you can configure a persistent self-signed certificate that does not require approval by a CA. For more information on the persistent self-signed certificate feature, see the information at this link:

http://www.cisco.com/en/US/products/sw/iosswrel/ps5207/products_feature_guide09186a008040adf0.html#wp1066623

Make sure that the entire URL is present in the link field in your browser.

Field Reference

Table 31-1 Create SSL VPN

Element	Description
Create a new SSL VPN	Select this option to create a new Cisco IOS SSL VPN configuration. This wizard enables you to create a Cisco IOS SSL VPN with one user policy and a limited set of features. After you complete this wizard, you can use the other wizards to configure addition policies and features for the Cisco IOS SSL VPN. You can return to this wizard to create additional Cisco IOS SSL VPN configurations. When you use Cisco CP to create the first Cisco IOS SSL VPN configuration on a router, you create a Cisco IOS SSL VPN context, configure a gateway, and create a group policy. After you complete the wizard, click **Edit SSL VPN** to view the configuration and familiarize yourself with how Cisco IOS SSL VPN components work together. For information that will help you understand what you see, click Cisco IOS SSL VPN Contexts, Gateways, and Policies.
Add a new policy to an existing SSL VPN for a new group of users	Select this option to add a new policy to an existing Cisco IOS SSL VPN configuration for a new group of users. Multiple policies allow you to define separate sets of capabilities for different groups of users. For example, you might define a policy for engineering, and a separate policy for sales.
Configure advanced features for an existing SSL VPN	Select this option to configure additional features for an existing Cisco IOS SSL VPN policy. You must specify the context under which this policy is configured.
Launch the selected task button	Click to begin the configuration that you selected. You will receive a warning message if you cannot complete the task that you chose. If there is a prerequisite task that you need to complete, you will be told what it is and how to complete it.

Persistent Self-Signed Certificate

You can provide the information for a persistent self-signed certificate in this dialog. Using the information that you provide, the HTTPS server will generate a certificate that will be used in the SSL handshake. Persistent self-signed

certificates remain in the configuration even if the router is reloaded, and are presented during the SSL handshake process. New users must manually accept these certificates, but users who have previously done so do not have to accept them again if the router was reloaded.

For more information on the persistent self-signed certificate feature, see the information at this link:

http://www.cisco.com/en/US/docs/ios/12_3t/12_3t14/feature/guide/gtpsscer.html

Make sure that the entire URL is present in the link field in your browser.

Field Reference

Table 31-2 Persistent Self-Signed Certificate

Element	Description
Name	Cisco CP places the name Router_Certificate in this field. You can change the name if you want to do so. This corresponds to the subject name that would be used in a certificate request.
Length of RSA Key	Cisco CP places the value 512 in this field. You can specify a longer key, such as 1024, if you want to do so. The key length should be a multiple of 64.
Subject	Provide the information for the fields in the subject area. For more information on these fields, see the information in Other Subject Attributes.
Generate Button	After providing the information in this window, click **Generate** to have the router create the persistent self-signed certificate.

Welcome

The Welcome window for each wizard lists the tasks that the wizard enables you to complete. Use this information to ensure that you are using the correct wizard. If you are not, click **Cancel** to return to the Create SSL VPN window and choose the wizard that you want to use.

When you provide all the information asked for by the wizard, the Summary window displays the information that you provided. To see the Cisco IOS CLI commands that you are delivering to the router, click **Cancel** to leave the wizard, and go to **Edit > Preferences**, and check **Preview commands before delivering**

to router. Then restart the wizard and provide the information that it asks for. When you deliver the configuration to the router, an additional window is displayed that allows you to view the Cisco IOS CLI commands you are delivering.

SSL VPN Gateways

A Cisco IOS SSL VPN gateway provides the IP address and the digital certificate for the SSL VPN contexts that use it. You can provide the information for a gateway in this window, and the information that will allow users to access a portal.

Field Reference

Table 31-3 SSL VPN Gateway

Element	Description
IP Address and Name	Use these fields to create the URL that users will enter to access the Cisco IOS SSL VPN portal. The IP address list contains the IP addresses of all configured router interfaces, and all existing Cisco IOS SSL VPN gateways. You can use the IP address of a router interface if it is a public address that the intended clients can reach, or you can use another public IP address that the clients can reach. If you use an IP address that has not already been used for a gateway, you create a new gateway.
Allow Cisco CP access through *IP Address*	Check if you want to continue to access Cisco CP from this IP address. This check box appears if you entered the IP address you are currently using to access Cisco CP. **Note** If you check this check box, the URL that you must use to access Cisco CP changes after you deliver the configuration to the router. Review the information area at the bottom of the window to learn which URL to use. Cisco CP places a shortcut to this URL on the desktop of your PC that you can use to access Cisco CP in the future.

Table 31-3 SSL VPN Gateway (continued)

Element	Description
Digital certificate	If you are creating a new gateway, select the digital certificate that you want the router to present to clients when they log in to the gateway. If you chose the IP address of an existing gateway, the router will use the digital certificate configured for that gateway, and this field is disabled.
Information area	When you provide the information in the IP Address and Name fields, this area contains the URL that users will enter. You must provide this URL to the users for whom you are creating this Cisco IOS SSL VPN. If you checked Allow Cisco CP access through IP address, the URL that you must use in the future to access Cisco CP is shown in this area. Cisco CP places a shortcut to this URL on the desktop of your PC after you deliver the Cisco IOS SSL VPN configuration to the router.

User Authentication

Use this window to specify how the router is to perform user authentication. The router can authenticate Cisco IOS SSL VPN users locally, or it can send authentication requests to remote AAA servers.

Field Reference

Table 31-4 User Authentication

Element	Description
External AAA server	Click if you want the router to use an AAA server to authenticate Cisco IOS SSL VPN users. The router will use the AAA servers that are listed in this window. If there are no AAA servers configured, you can configure them in this window. To use this option, there must be at least one AAA server configured on the router.
Locally on this router	Click if you want the router to authenticate users itself. The router will authenticate each user displayed in this window. If no users are configured on the router, you can add users in this window.

Table 31-4 User Authentication (continued)

Element	Description
First on an external AAA server and then locally on this router	Click if you want the router to authenticate using a AAA server first, and if authentication fails, to attempt local authentication. If the user is not configured on either a configured AAA server or locally on the router, authentication for that user fails.
Use the AAA authentication method list	Click if you want the router to use a method list for authentication. A method list contains the authentication methods that should be used. The router attempts the first authentication method in the list. If authentication fails, the router tries the next method in the list and continues until the user is authenticated, or until it reaches the end of the list.
AAA servers configured for this router	This list contains the AAA servers that the router uses to authenticate users. If you choose to authenticate users with AAA servers, this list must contain the name or IP address of at least one server. Use the **Add** button to add information for a new server. To manage AAA configurations on the router, leave the wizard, click **Router > AAA**. This list does not appear if you have chosen **Locally on this router**.
Create user accounts locally on this router	Enter the users that you want the router to authenticate in this list. Use the **Add and Edit** buttons to manage the users on the router. This list does not appear if you chose **External AAA server**.

Configure Intranet Websites

Configure groups of intranet websites that you want users to have access to in this window. These links will appear in the portal that the users of this Cisco IOS SSL VPN see when they log in.

Field Reference

Table 31-5 Configure Intranet Websites

Element	Description
Action and URL List Columns	If you are adding a policy to an existing Cisco IOS SSL VPN context, there may be URL lists present in the table that is displayed. Check **Select** if you want to use a displayed URL list for the policy. To create a new list, click **Add** and provide the required information in the dialog displayed. Use the **Edit** and **Delete** keys to change or remove URL lists in this table.

Add or Edit URL

Add or edit the information for a Cisco IOS SSL VPN link in this window.

Field Reference

Table 31-6 Add or Edit URL

Element	Description
Label	The label appears in the portal that is displayed when users log in to the Cisco IOS SSL VPN. For example, might use the label Payroll calendar if you are providing a link to the calendar showing paid holidays and paydays.
URL Link	Enter or edit the URL to the corporate intranet website that you want to allow users to visit.

Customize SSL VPN Portal

The settings that you make in this screen determine the appearance of the portal to the user. You can select among the predefined themes listed, and obtain a preview of the portal as it would appear if that theme were used.

Field Reference

Table 31-7 Customize SSL VPN Portal

Element	Description
Theme	Select the name of a predefined theme.
Preview	This area shows what the portal looks like with the selected theme.You may want to preview several themes to determine which one you want to use.

SSL VPN Passthrough Configuration

In order for users to be able to connect to the intranet, access control entries (ACE) must be added to firewall and Network Access Control (NAC) configurations to permit SSL traffic to reach the intranet. Cisco CP can configure these ACE for you, or you can configure them yourself by going to **Basic Security > Firewall and ACL > Edit Firewall Policy/ACL** and making the necessary edits.

If you are working in the Cisco IOS SSL VPN wizard, click **Allow SSL VPN to work with NAC and Firewall** if you want Cisco CP to configure these ACEs. Click **View Details** to view the ACEs that Cisco CP would create. An entry that Cisco CP adds might look like this example:

```
permit tcp any host 172.16.5.5 eq 443
```

If you are editing a Cisco IOS SSL VPN context, Cisco CP displays the affected interface and ACL that is applied to it. Click **Modify** to allow Cisco CP to add entries to the ACL to allow SSL traffic to pass through the firewall. Click **Details** to view the entry that Cisco CP adds. The entry will be one similar to the one already shown.

User Policy

This window allows you to choose an existing Cisco IOS SSL VPN and add a new policy to it. For example, you might have created a Cisco IOS SSL VPN named Corporate, and you want to define intranet access for a new group of users that you name Engineering.

Field Reference

Table 31-8 User Policy

Element	Description
Select existing SSL VPN	Choose the Cisco IOS SSL VPN for which you want to create a new group of users. The policies already configured for that Cisco IOS SSL VPN are displayed in a box under the list. You can click any of them to display the details of the policy. See Details of SSL VPN Group Policy: Policyname for more information.
Name of new policy	Enter the name that you want to give the new group of users. The area below this field lists the group policies that already exist for this Cisco IOS SSL VPN.

Details of SSL VPN Group Policy: Policyname

This window displays the details of an existing Cisco IOS SSL VPN policy.

Field Reference

Table 31-9 Details of SSL VPN Group Policy

Element	Description
Services	This area lists the services, such as URL mangling, and Cisco Secure Desktop, that this policy is configured for.
URLs exposed to users	This area lists the intranet URLs exposed to users who are governed by this policy.
Servers exposed to users	This area displays the IP addresses of the port forwarding servers that this policy is configured to use.
WINS servers	This area displays the IP addresses of the WINS servers that this policy is configured to use.

Select the SSL VPN User Group

Choose the Cisco IOS SSL VPN and associated user group for which you want to configure advanced services in this window.

Field Reference

Table 31-10 Select SSL VPN User Group

Element	Description
SSL VPN	Choose the Cisco IOS SSL VPN that the user group is associated with from this list.
User Group	Choose the user group for which you will configure advanced features. The contents of this list is based on the Cisco IOS SSL VPN that you chose.

Select Advanced Features

Choose the features that you want to configure in this window. The wizard will display windows that allow you to configure the features that you choose.

For example, if you click Thin Client (Port Forwarding), Cisco Secure Desktop, and Common Internet File System (CIFS), the wizard will display configuration windows for these features.

You must choose at least one feature to configure.

Thin Client (Port Forwarding)

Remote workstations must sometimes run client applications to be able to communicate with intranet servers. For example Internet Mail Access Protocol (IMAP) or Simple Mail Transfer Protocol (SMTP) servers may require workstations to run client applications in order to send and receive e-mail. The Thin-Client feature, also known as port forwarding, allows a small applet to be downloaded along with the portal so that a remote workstation can communicate with the intranet server.

This window contains a list of the servers and port numbers configured for the intranet. Use the **Add** button to add a server IP address and port number. Use the **Edit** and **Delete** buttons to make changes to the information in this list and to remove information for a server.

The list that you build appears in the portal that clients see when they log in.

Add or Edit a Server

Add or edit server information in this window.

Field Reference

Table 31-11 Add or Edit a Server

Element	Description
Server IP Address	Enter the IP address or hostname of the server.
Server port on which service is listening	Enter the port the server is listening on for this service. This may be a standard port number for the service, such as port number 23 for Telnet, or it may be a nonstandard port number for which a Port-to-Application Map (PAM) has been created. For example if you changed the Telnet port number on the server to 2323, and you created a PAM entry for that port on that server, you would enter 2323 in this window.
Port on Client PC	Cisco CP enters a number in this field, beginning with the number 3000. Each time you add an entry, Cisco CP increments the number by 1. Use the entries that Cisco CP has placed in this field.
Description	Enter a description for the entry. For example, if you are adding an entry that enables users to telnet to a server at 10.10.11.2, you could enter "Telnet to 10.10.11.2." The description you enter appears on the portal.
Learn More	Click this link for more information. You can view that information now by clicking Learn More about Port Forwarding Servers.

Full Tunnel

Full tunnel clients must download the full tunnel software and obtain an IP address from the router. Use this window to configure the IP address pool that full tunnel clients will draw from when they log in and to specify the location of the full tunnel install bundle.

Routers running Cisco IOS 12.4(20)T and later releases can host Cisco AnyConnect full-tunnel clients. See About Cisco AnyConnect for more information.

Note If the software install bundle is not already installed, there must be sufficient memory in router flash for Cisco CP to install it after you complete this wizard.

Field Reference

Table 31-12 Full Tunnel

Element	Description
Enable Full Tunnel	Check to allow the router to download the full tunnel client software to the user's PC, and to enable the other fields in this window.
IP Address Pool	Specify the IP address pool that full tunnel clients will draw from. You can enter the name of an existing pool in the field, or you can click the button to the right of the field and choose **Select an existing IP pool** to browse the list of pools, Choose **Create a new pool** and complete the dialog that is displayed to create a new pool. The address pool that you choose or create must contain addresses in the corporate intranet.
Keep the Full Tunnel Client software installed on client's PC	Check if you want the Full Tunnel software to remain on the client's PC after they have logged off. If you do not check this check box, clients download the software each time they establish communication with the gateway.
Install Full Tunnel Client	Check if you want to install the full tunnel client software at this time. You can also install the client software when editing this Cisco IOS SSL VPN.The full tunnel client software must be installed on the router so that clients can download it to establish full-tunnel connectivity. If the Full Tunnel software was installed along with Cisco CP, the path to it automatically appears in the Location field, as shown in Example 31-1 in this help topic.
Advanced Button	Click to configure advanced options such as split tunneling, split DNS, and client Microsoft Internet Explorer settings.

Example 31-1 Full Tunnel Package Installed on Router

```
flash:sslclient-win-1.0.2.127.pkg
```
or
```
flash:/anyconnect-win-2.2.0140-k9.pkg
```

In Example 31-1, the Full Tunnel install bundle is loaded in router flash. If your router's primary device is a disk or a slot, the path that you see will start with `diskn` or `slotn`.

If this field is empty, you must locate the install bundle so that Cisco CP can load it onto the router primary device, or download the software install bundle from Cisco.com by clicking on the Download latest... link at the bottom of the window. You will be taken to one of the following pages:

- http://www.cisco.com/cgi-bin/tablebuild.pl/anyconnect
- http://www.cisco.com/cgi-bin/tablebuild.pl/sslvpnclient

Note You may need a CCO username and password in order to obtain software from Cisco software download sites. To obtain these credentials, click **Register** at the top of any Cisco.com webpage and provide the information asked for. Your userid and password will be e-mailed to you.

Click Locating the Install Bundle to learn how to locate the Full Tunnel software install bundle, and supply a path to it for Cisco CP to use.

Enable Cisco Secure Desktop

The router can install Cisco Secure Desktop on the user PC when the user logs in to the Cisco IOS SSL VPN. Web transactions can leave cookies, browser history files, e-mail attachments, and other files on the PC after the user logs out. Cisco Secure Desktop create a secure partition on the desktop and uses a Department of Defense algorithm to remove the files after the session terminates.

Install Cisco Secure Desktop

Clients must download the Cisco Secure Desktop software install bundle from the router. If this software was installed along with Cisco CP, the path to it automatically appears in the **Location** field as shown in Example 31-2.

Example 31-2 Cisco Secure Desktop Package Installed on Router

```
flash:/securedesktop-ios-3.1.0.29-k9.pkg
```

In Example 31-2, the Cisco Secure Desktop install bundle is loaded in router flash. If your router's primary device is a disk or a slot, the path that you see will start with `diskn` or `slotn`.

If this field is empty, you must locate the install bundle so that Cisco CP can load it onto the router primary device, or download the software install bundle from Cisco.com by clicking the **Download latest...** link at the bottom of the window. This link takes you to the following web page:

http://www.cisco.com/cgi-bin/tablebuild.pl/securedesktop

Note You may need a CCO username and password in order to obtain software from Cisco software download sites. To obtain these credentials, click **Register** at the top of any Cisco.com webpage and provide the information asked for. Your userid and password will be e-mailed to you.

Click Locating the Install Bundle to learn how to locate the Cisco Secure Desktop software install bundle, and supply a path to it for Cisco Cisco CP to use.

Common Internet File System

Common Internet File System (CIFS) allows clients to remotely browse, access, and create files on Microsoft Windows-based file servers using a web browser interface.

Field Reference

Table 31-13 Common Internet File System

Element	Description
WINS Servers	Microsoft Windows Internet Naming Service (WINS) servers maintain the database that maps client IP addresses to their corresponding NetBIOS names. Enter the IP addresses of the WINS servers in your network in this box. Use semicolons (;) to separate addresses.For example, to enter the IP addresses 10.0.0.18 and 10.10.10.2, you enter 10.0.0.18;10.10.10.2 in this box.
Permissions	Specify the permissions to grant to users.

Enable Clientless Citrix

Clientless Citrix allows users to run applications such as Microsoft Word or Excel on remote servers in the same way that they would run them locally, without the need for client software on the PC. The Citrix software must be installed on one or more servers on a network that the router can reach.

Field Reference

Table 31-14 Clientless Citrix

Element	Description
URL List Area	
Label	The label for the link that will be seen on the portal page that users of the SSL VPN will see.
URL	The URL that will be used to connect to the shared application on the Citrix server.
Citrix Server List Area	
Name	The name of a Citrix server on the network.
URL	The URL for the Citrix server.

Citrix Server

To create a new list, click **Add** and provide the required information in the dialog displayed. Use the **Edit** and **Delete** keys to change or remove URL lists in this table.

Summary

This window displays a summary of the Cisco IOS SSL VPN configuration that you have created. Click **Finish** to deliver the configuration to the router, or click **Back** to return to a wizard window to make changes.

Editing SSL VPN Connections

To edit an SSL VPN connection, complete the following tasks:

Step 1 In the Cisco CP Feature bar, click **Configure** > **Security** > **VPN** > **SSL VPN** > **SSL VPN Manager** > **Edit SSL VPN**.

Step 2 Choose the SSL VPN connection that you want to edit.

Step 3 Click **Edit**. Then, make changes to the settings in the displayed dialogs. Editing SSL VPN Connection Reference describes the configuration screens you use to edit a connection.

Step 4 Click **OK** to close the dialog and send the changes to the router.

Step 5 Click **Deliver** to send the configuration to the router, or click **Cancel** to discard it.

Editing SSL VPN Connection Reference

The topics in this section describe the SSL VPN Edit screens.

- Edit SSL VPN
- SSL VPN Context
- Designate Inside and Outside Interfaces
- Select a Gateway
- Context: Group Policies
- Group Policy: General Tab
- Group Policy: Clientless Tab
- Group Policy: Thin Client Tab
- Group Policy: SSL VPN Client (Full Tunnel) Tab
- Advanced Tunnel Options
- DNS and WINS Servers
- Context: HTML Settings
- Select Color
- Context: NetBIOS Name Server Lists
- Add or Edit a NBNS Server List
- Add or Edit an NBNS Server

- Context: Port Forward Lists
- Add or Edit a Port Forward List
- Context: URL Lists
- Add or Edit a URL List
- Context: Cisco Secure Desktop
- Packages
- Install Package

Edit SSL VPN

The Edit SSL VPN window allows you modify or create Cisco IOS SSL VPN configurations. The top portion of the tab lists the configured Cisco IOS SSL VPN contexts. The bottom portion displays details for that context.

Related Links

- Cisco IOS SSL VPN
- Cisco IOS SSL VPN Contexts, Gateways, and Policies
- Cisco IOS SSL VPN Links on Cisco.com

Field Reference

Table 31-15 Edit SSL VPN

Element	Description
SSL VPN Contexts	
This area displays the Cisco IOS SSL VPN contexts configured on the router. Click a context in this area to display the detailed information for it in the lower part of the window. Add a new context by clicking **Add** and entering information in the dialog displayed. Edit a context by selecting it and clicking **Edit**. Remove a context and its associated group policies by selecting it and clicking **Delete**. You can enable a context that is not in service by choosing it and clicking **Enable**. Take a context out of service by choosing it and clicking **Disable**. The following information is displayed for each context.	

Table 31-15 Edit SSL VPN (continued)

Element	Description
Name	The name of the Cisco IOS SSL VPN context. If you created the context in the Cisco IOS SSL VPN wizard, the name is the string that you entered in the IP Address and Name window.
Gateway	The gateway that the context uses contains the IP address, and digital certificate that the Cisco IOS SSL VPN context will use.
Domain	If a domain has been configured for the context, it is displayed in this column. If a domain is configured, users must enter that domain in the web browser to access the portal.
Status	Contains icons for quick status identification.
Administrative Status	Textual description of status. • In Service—Context is in service. Users specified in policies configured under the context can access their Cisco IOS SSL VPN portal. • Not in Service—Context is not in service. Users specified in policies configured under the context cannot access their Cisco IOS SSL VPN portal.
Sample Display	The Sample Display shows a sample Cisco IOS SSL VPN contexts display.
Details about SSL VPN Context: *Name*	
This area displays details about the context with the name *name* that you selected in the upper part of the window. You can modify the settings that you see by clicking **Edit** in the top part of the window.	

Sample Display

The following table shows a sample Cisco IOS SSL VPN contexts display.

Name	Gateway	Domain	Status	Administrative Status
WorldTravel	Gateway1	wtravel.net		In Service
A+Insurance	Gateway2	aplus.com		Not in Service

SSL VPN Context

Use this window to add or edit a Cisco IOS SSL VPN context.

Field Reference

Table 31-16 SSL VPN Context Fields

Element	Description
Name	Enter the name of a new context, or choose the name of an existing context to edit it.
Associated Gateway	Select an existing gateway, or click **Create gateway** to configure a new gateway for the context. The gateway contains the IP address and digital certificate is used for this context. Each gateway requires a unique public IP address.
Domain	If you have a domain for this context, enter it in this field. Cisco IOS SSL VPN users will be able to use this domain name when accessing the portal, instead of an IP address. An example is mycompany.com.
Authentication List	Choose the AAA method list to be used to authenticate users to this context.
Authentication Domain	Enter the domain name that is to be appended to the username before it is sent for authentication. This domain must match the domain used on the AAA server for the users that will be authenticated for this context.
Enable Context	Check **Enable Context** if you want the context to be enabled when you finish configuring it. You do not have to return to this window to disable it if you enable it here. You can enable and disable individual contexts in the Edit SSL VPN tab.
Maximum Number of Users	Enter the maximum number of users that should be allowed to use this context at one time.
VRF Name	Enter the VPN Routing and Forwarding (VRF) name for this context. This VRF name must have already been configured on the router.

Table 31-16 SSL VPN Context Fields (continued)

Element	Description
Default Group Policy	Select the policy that you want to use as the default group policy. The default group policy will be used for users who have not been included in any policy configured on the AAA server.
Enable RADIUS Accounting	Check **Enable RADIUS Accounting** to enable this feature for the context that you are editing. If this option is disabled, the AAA authentication list chosen for the context does not include any configured AAA servers. You must choose a different authentication list, or configure a new one. To add AAA server information f to the router configuration, click **Configure > Router > AAA > AAA Servers and Groups > Servers > Add**. Enter the IP address and other required information in the displayed dialog. The AAA server information you enter becomes available for use in authentication lists.

Designate Inside and Outside Interfaces

An ACL that is applied to an interface on which a Cisco IOS SSL VPN connection is configured may block the SSL traffic. Cisco CP can automatically modify the ACL to allow this traffic to pass through the firewall. However, you must indicate which interface is the inside (trusted) interface, and which is the outside (untrusted) interface for Cisco CP to create the Access Control Entry (ACE) that will allow the appropriate traffic to pass through the firewall.

Check **Inside** if the listed interface is a trusted interface, and check **Outside** if it is an untrusted interface.

Select a Gateway

Select an existing gateway from this window. This window provides you with the information you need to determine which gateway to select. It displays the names and IP addresses of all gateways, the number of contexts each is associated with, and whether the gateway is enabled or not.

Context: Group Policies

This window displays the group policies configured for the chosen Cisco IOS SSL VPN context. Use the **Add**, **Edit**, and **Delete** buttons to manage these group policies.

For each policy, this window shows the name of the policy and whether the policy is the default group policy. The default group policy is the policy assigned to a user who has not been included in another policy. You can change the group policy by returning to the Context window and selecting a different policy as the default.

Click a policy in the list to view details about the policy in the lower part of the window. For a description of these details, click the following links

Group Policy: General Tab

Group Policy: Clientless Tab

Group Policy: Thin Client Tab

Group Policy: SSL VPN Client (Full Tunnel) Tab

Click here to learn more

Click the link in the window for important information. To get to that information from this help page, click Learn More About Group Policies.

Group Policy: General Tab

When creating a new group policy, you must enter information in each field of the General tab.

Field Reference

Table 31-17 General Tab Fields

Element	Description
Name	Enter a name for the group policy, for example Engineering, Human Resources, or Marketing.
Make this the default group policy for context	Check if you want to make this the default group policy. The default group policy is the policy assigned to a user who is not included in another policy. If you check this check box, this policy will be shown as the default policy in the Group Policy window.

Table 31-17 General Tab Fields (continued)

Element	Description
Timeouts	
Idle Timeout	Enter the number of seconds that the client can remain idle before the session is terminated.
Session Timeout	Enter the maximum number of seconds for a session, regardless of the activity on the session.
Application ACL	
Application ACL	SSLVPN uses application ACLs to specify permitted and denied URLs for groups. Choose a configured application ACL for this group. To configure application ACLs, go to the SSL VPN Context tree, click **App ACL** to display the Access Control List window, and then click **Add**.
View	Click **View** to display the details for the chosen application ACL.

Group Policy: Clientless Tab

Clientless Citrix allows users to run applications on remote servers in the same way that they would run them locally, without client software needing to be installed on the remote systems using these applications. The Citrix software must be installed on one or more servers on a network that the router can reach.

Enter information if you want Cisco IOS SSL VPN clients to be able to use Clientless Citrix.

Field Reference

Table 31-18 Clientless Tab Fields

Element	Description
Clientless Web Browsing	
Action URL List	Select one or more URL lists that you want to display in the portal that the users in this group will see. URLs in the list that you specify will be displayed in the portal.
View	To examine a URL list, choose a name from the list and click **View**.
Add	To add a URL list or a Citrix Server list, click **Add** and choose the option that you want
Hide URL bar in the portal page	If you want to restrict users to URLs in the list, and prevent them from entering additional URLs, click **Hide URL bar in the portal page**.
Enable URL Obfuscation	Click **Enable URL Obfuscation** to enable this feature for the group policy. When URL obfuscation is enabled, end users do not see the path to the web server or other internal resource in the web page that they are using. Instead, they see an obfuscated path that provides no information about the network.
Enable Citrix	Click **Enable Citrix** to enable Clientless Citrix for the group policy. Citrix allows users to run applications such as Microsoft Word or Excel on remote servers in the same way that they would run them locally, without the need for client software on the PC. The Citrix software must be installed on one or more servers on a network that the router can reach.
Enable CIFS	
Choose **Enable CIFS** if you want to allow group members to browse files on MS Windows servers in the corporate network. When you enable CIFS, the options that follow are enabled.	
Read	Click **Read** to allow group members to read files.
Write	Click **Write** to allow group members to make changes to files.

Table 31-18 Clientless Tab Fields

Element	Description
NBNS Server List	You must specify the NBNS server list that will enable the appropriate files to be displayed to these users. Choose the NBNS Server list to use for this group. To configure a list, click **NETBIOS Name Server Lists** in the SSL VPN Context tree and click **Add** to configure a list.
View	To verify the contents of a WINS server list, choose the list and click **View**.

Group Policy: Thin Client Tab

Make settings in this tab if you want to configure Thin Client, also known as port forwarding, for members of this group.

Field Reference

Table 31-19 Thin Client Tab Fields

Element	Description
Enable Thin Client	Click **Enable Thin Client** (**Port Forwarding**) and specify a port forward list to enable this feature. At least one port forward list must be configured for the Cisco IOS SSL VPN context under which this group policy is configured.
View	To examine the port forwarding list you have chosen, click **View**.
Automatically Download Applet	The Automatically Download Applet option causes the Thin Client applet to be downloaded automatically to clients when they have logged on. This option is checked by default.

Group Policy: SSL VPN Client (Full Tunnel) Tab

Make setting in this tab if you want to enable the group members to download and use full-tunnel client software.

Note You must specify the location of the Full Tunnel client software by clicking **Packages** in the SSL VPN tree, specifying the location of the install bundle, and then clicking **Install**.

Enable Full Tunnel connections by choosing **Enable** from the list. If you want to require Full Tunnel connections, choose **Required**. If you choose **Required**, Clientless and Thin Client communication will work only if the Cisco IOS SSL VPN client software is successfully installed on the client PC.

Field Reference

Table 31-20 Group Policy: SSL VPN Client (Full Tunnel) Tab

Element	Description
IP address pool from which clients will be assigned an IP address	Clients who establish Full Tunnel communication are assigned IP addresses by the router. Specify the name of the pool, or click the **...** button to create a new pool from which the router can assign addresses.
Keep full-tunnel client software installed on client's PC check box	Check if you want the Full Tunnel software to remain on the client's PC after they have logged off. If you do not check this check box, clients download the software each time they establish communication with the gateway.
Renegotiate Key field	Enter the number of seconds after which the tunnel should be brought down so that a new SSL key can be negotiated and the tunnel can be reestablished.
ACL to restrict access for users in this group to corporate resources	You can choose or create an access list (ACL) that specifies the resources on the corporate network that group members will be restricted to.
Home page client should see when a web browser is opened with full tunnel software installed	Enter the URL to the home page that is to be displayed to full-tunnel clients in this group.

Table 31-20 Group Policy: SSL VPN Client (Full Tunnel) Tab (continued)

Element	Description
Dead Peer Detection Timeouts	Dead Peer Detection (DPD) allows a system to detect a peer that is no longer responding. You can set separate timeouts that the router can use to detect clients that are no longer responding, and servers that are no longer responding. The range for both is from 0 to 3600 seconds.
Configure DNS and WINS servers Button	Click to display the DNS and WINS Servers dialog, which allows you to provide the IP addresses of the DNS and WINS servers on the corporate intranet that clients should use when accessing intranet hosts and services.
Configure Advanced Tunnel Options Button	Click to display the Advanced Tunnel Options dialog, which allows you to configure tunnel settings for split tunneling, split DNS, and proxy server settings for clients using Microsoft Internet Explorer.

Advanced Tunnel Options

The settings that you make in this dialog allow you to control the traffic that is encrypted, specify the DNS servers on the corporate intranet, and specify the proxy server settings that are to be sent to client browsers.

Field Reference

Table 31-21 Advanced Tunnel Options

Element	Description
Split Tunneling Tab	
Split Tunneling	Encrypting all tunnel traffic may take excessive system resources. Split tunneling allows you to specify the networks whose traffic should be encrypted, and exempt traffic destined for other networks from encryption. You can either specify which tunnel traffic is to be encrypted or you can specify the traffic that is *not* to be encrypted and allow the router to encrypt all other tunnel traffic. You can only build one list; included and excluded traffic are mutually exclusive. The section "Learn More About Split Tunneling" contains more information about this topic.

Table 31-21 Advanced Tunnel Options (continued)

Element	Description
Include traffic	To create a list of destination networks whose traffic is to be encrypted, click **Include traffic** and use the **Add**, **Edit**, and **Delete** keys next to Destination Networks list.
Exclude traffic	To build a list of destination networks whose traffic is to *not* to be encrypted, click **Exclude traffic** and use the **Add**, **Edit**, and **Delete** keys next to Destination Networks list.
Exclude Local LANs	To explicitly exclude from encryption client traffic destined for LANs that the router is connected to, click **Exclude Local LANs**. If there are networked printers on these LANs, you must use this option.
Split DNS	If you want Cisco IOS SSL VPN clients to use the DNS server in the corporate network only to resolve specific domains, you can enter those domains in this area. They should be domains within the corporate intranet. Separate each entry with a semicolon and do not use carriage returns. Here is a sample list of entries: yourcompany.com;dev-lab.net;extranet.net Clients must use the DNS servers provided by their ISPs to resolve all other domains.
Browser Proxy Settings Tab	
The settings in this area are sent to client Microsoft Internet Explorer browsers with full tunnel connections. These settings have no effect if clients use a different browser.	
Bypass proxy settings for local addresses	Click if you want clients connecting to local addresses to be able to bypass normal proxy settings.
Auto-detect proxy settings	Click if you want the Cisco IOS SSL VPN client browsers to auto detect proxy server settings.
Do not use proxy server	Click to instruct Cisco IOS SSL VPN client browsers not to use a proxy server.
Proxy Server	Enter the IP address of the proxy server and the port number for the service that it provides in these fields. For example, if the proxy server supports FTP requests, enter the IP address of the proxy server and port number 21.

Table 31-21 Advanced Tunnel Options (continued)

Element	Description
Do not use proxy server for addresses beginning with the following	If you do not want clients to use proxy servers when sending traffic to specific IP addresses or networks, you can enter them here. Use a semicolon to separate each entry. For example, if you do not want clients to use a proxy server when connecting to any server in the 10.10.0.0 or 10.11.0.0 networks, enter 10.10;10.11. You can enter as many networks as you want.
DNS and WINS Servers Tab	
DNS Servers	Enter the IP addresses for the corporate DNS servers that will be sent to Cisco IOS SSL VPN clients. Cisco IOS SSL VPN clients will use these servers to access hosts and services on the corporate intranet. Provide addresses for primary and for secondary DNS servers.
WINS Servers	Enter the IP addresses for the corporate WINS servers that will be sent to Cisco IOS SSL VPN clients. Cisco IOS SSL VPN clients will use these servers to access hosts and services on the corporate intranet. Provide addresses for primary and for secondary WINS servers

DNS and WINS Servers

Enter the IP addresses for the corporate DNS and WINS servers that will be sent to Cisco IOS SSL VPN clients. Cisco IOS SSL VPN clients will use these servers to access hosts and services on the corporate intranet.

Provide addresses for primary and for secondary DNS servers and WINS servers.

Context: HTML Settings

The settings that you make in this window control the appearance of the portal for the selected Cisco IOS SSL VPN context.

Field Reference

Table 31-22 HTML Settings

Element	Description
Select theme	
You can specify the appearance of the portal by selecting a predefined theme instead of by selecting each color yourself. When you select a theme, the settings for that theme are displayed in the fields associated with the **Customize** button.	
Customize	
Click if you want to select each color used in the portal and specify a login message and title. If you selected a predefined theme, the values for that theme are displayed in the fields in this section. You can change these values, and the values you enter are used in the portal for the selected context. Changes that you make in this window only affect the portal you are creating. They do not change the default values for the theme.	
Login Message	Enter the login message that you want clients to see when their browsers display the portal. For example: `Welcome to the` *`company-name`* `network. Log off if you are not an authorized user.`
Title	Enter the title that you want to give the portal. For example: *`Company-name`* `network login page`
Background Color for Title	The default value for the background color that appears behind the title is #9999CC. Change this value by clicking the **...** button and selecting a different color.
Background Color for Secondary Titles	The default value for the background color that appears behind the title is #9729CC. Change this value by clicking the **...** button and selecting a different color, or by entering the hexadecimal value for a different color.
Text Color	The default value for the text color is white. Change this value by clicking the down arrow and selecting a different color.
Secondary Text Color	The default value for the secondary text color is black. Change this value by clicking the down arrow and selecting a different color.

Table 31-22 HTML Settings (continued)

Element	Description
Logo File	If you have a logo that you want to display on the portal, click the **...** button to browse for it on your PC. It is saved to router flash after you click **OK**, and will appear in the upper-left corner of the portal.
Preview Button	Click to see a preview of the portal as it will look with the predefined theme or custom values you have specified.

Select Color

Click **Basic** to select a predefined color, or click **RGB** to create a custom color.

Field Reference

Table 31-23 Select Color

Element	Description
Basic	Select the color that you want to use from the palette on the left. The color you select appears in the large square in the right side of the dialog.
RGB	Use the Red, Green, and Blue sliders in combination to create a custom color. The color you create appears in the large square in the right side of the dialog.

Context: NetBIOS Name Server Lists

View all the NetBIOS name server lists that are configured for the selected Cisco IOS SSL VPN context in this window. CIFS uses NetBIOS servers to display the corporate Microsoft Windows file system to Cisco IOS SSL VPN users.

Each name server list configured for the context is shown in the **NetBIOS Name Server Lists** area. Use the **Add**, **Edit**, and **Delete** buttons to manage these lists. Click a list name to view the contents of the list in the **Details of NetBIOS Name Server** area.

Add or Edit a NBNS Server List

Create or maintain a NBNS server list in this window. You must enter a name for each list that you create, and provide the IP address, timeout and number of retries to attempt for each server in the list. One server in each list must be designated as the master server.

Each server in the list is displayed in this dialog, along with its master status, timeout, and retries values.

Add or Edit an NBNS Server

You must enter the IP address of each server, along with the number of seconds that the router is to wait before attempting to connect to the server again, and the number of times the router is to attempt to contact the server.

Check **Make this server the master server** if you want this server to be the first server that the router contacts on the list.

Context: Port Forward Lists

Configure the port forwarding lists for the selected context in this window. The lists can be associated to any group policy configured under the selected context. Port forward lists reveal TCP application services to Cisco IOS SSL VPN clients.

The upper part of the window displays the port forward lists configured for the selected context. Click a list name to display the details for the list in the lower part of the window.

The window displays the IP address, port number used, corresponding port number on the client, and a description if one was entered.

Add or Edit a Port Forward List

Create and maintain port forward lists in this window. Each list must be given a name, and contain at least one server entry. Use the **Add**, **Edit**, and **Delete** buttons to create, modify, and remove entries from the list.

Context: URL Lists

URL lists specify which links can appear on the portal for users in a particular group. Configure one or more URL lists for each context, then use the group policy windows to associate these lists with specific group policies.

The upper part of the window displays all the URL lists configured for the context. The lower part of the window displays the contents of the selected list. For each list, it displays the heading that is displayed at the top of the URL list, and each URL that is in the list.

Use the **Add**, **Edit**, and **Delete** buttons to create and manage URL lists.

Add or Edit a URL List

You must enter a name for each URL list, and heading text that will appear at the top of the URL list.

Heading text should describe the overall contents of the links in the list. For example, if a URL list provides access to the health plan web pages and insurance web pages, you might use the heading text `Benefits`.

Use the **Add** button to create a new entry for the list, and the **Edit** and **Delete** buttons to maintain the list. Each entry that you add appears in the list area.

Context: Cisco Secure Desktop

Cisco Secure Desktop encrypts cookies, browser history files, temporary files, and e-mail attachments that could create security problems if left unencrypted. After a Cisco IOS SSL VPN session is terminated, Cisco Secure Desktop removes the data using a Department of Defense sanitation algorithm.

Click **Enable Cisco Secure Desktop** to allow all users of this context to download and use **Cisco Secure Desktop**. This window displays a message if the install bundle for this software is not found on the router.

To load the install bundle for Cisco Secure Desktop on the router, click Packages in the Cisco IOS SSL VPN tree and follow the instructions in the window.

Editing SSL VPN Gateways

When you use the wizard to create a Cisco IOS SSL VPN connection, a gateway for the connection is automatically created. You can view the details of the gateways that you create and edit gateway settings.

To edit a Cisco IOS SSL VPN gateway complete these tasks:

Step 1 In the Cisco CP Feature bar, click **Configure > Security > VPN > SSL VPN > SSL VPN Gateways**.

Step 2 Choose the Cisco IOS SSL VPN gateway that you want to edit.

Step 3 Click **Edit**. Then, make changes to the settings in the displayed dialogs. Editing SSL VPN Connection Reference describes the configuration screens you use to edit a connection.

Step 4 Click **OK** to close the dialog and send the changes to the router.

Step 5 Click **Deliver** to send the configuration to the router, or click **Cancel** to discard it.

Editing SSL VPN Gateway Reference

This section contains the following parts:

- SSL VPN Gateways
- Add or Edit a SSL VPN Gateway

SSL VPN Gateways

This window displays the Cisco IOS SSL VPN gateways configured on the router and enables you to modify existing gateways and configure new ones. A Cisco IOS SSL VPN gateway is the user portal to the secure network.

Related Links

- Add or Edit a SSL VPN Gateway
- SSL VPN Context
- Cisco IOS SSL VPN Contexts, Gateways, and Policies

Field Reference

Table 31-24 SSL VPN Gateways

Element	Description
SSL VPN Gateways	
This area of the window lists the Cisco IOS SSL VPN gateways that are configured on the router. It shows the name and IP address of the gateway, the number of contexts configured to use the gateway, and the status of the gateway.	
Name	The name of the gateway.
IP Address	The IP address given to the gateway.
Number of Contexts	The number of contexts that are using this gateway.
Status	One of the following icons that display the status of the gateway: • —The gateway is enabled and in service. • —The gateway is disabled and not in service.
Administrative Status	One of the following values: • In service • Out of service
Details of SSL VPN Gateway	
This area of the window displays configuration details about the gateway selected in the SSL VPN Gateways area, and the names of the Cisco IOS SSL VPN contexts that are configured to use this gateway.	
IP Address	The IP address of the gateway.
Hostname	The hostname of the gateway, if configured.
HTTP Redirect	One of the following values: • Disabled—HTTP redirects are not enabled. • Enabled (Port *number*)—HTTP redirects from the port specified in *number* are enabled.
Digital Certificate	The digital certificate that the gateway uses. For example, `From Trustpoint TP-self-signed-995375956`

Table 31-24 SSL VPN Gateways (continued)

Element	Description
Associated Contexts	The contexts that use this gateway. Context names are displayed on the same line, separated by commas. For example, `c_fin, c_dev, c_mkt`

Add or Edit a SSL VPN Gateway

Create or edit a Cisco IOS SSL VPN gateway in this window.

Field Reference

Table 31-25 Add or Edit a SSL VPN Gateway

Element	Description
Gateway Name	The gateway name uniquely identifies this gateway on the router, and is the name used to refer to the gateway when configuring Cisco IOS SSL VPN contexts.
IP Address	Choose or enter the IP address that the gateway is to use. This must be a public IP address, and cannot be an address used by another gateway on the router.
Digital Certificate	Choose the certificate that is to be sent to Cisco IOS SSL VPN clients for SSL authentication.
HTTP Redirect	Uncheck if you do not want HTTP redirect to be used. HTTP redirect automatically redirects HTTP requests to port 443, the port used for secure Cisco IOS SSL VPN communication.
Enable Gateway	Uncheck if you do not want to enable the gateway. You can also enable and disable the gateway from the SSL VPN Gateways window.

Installing Software Packages

The router must download Cisco IOS SSL VPN client software and Cisco Secure Desktop software to clients. The packages screens enable you to load the install bundles for these applications on the router so they are available when the router must download them to clients.

To install these software packages to the router, complete the following tasks:

Step 1 In the Cisco CP Feature bar, click **Configure > Security > VPN > SSL VPN > Packages.**

Step 2 In the packages screen, click the download link for each software package, and download the install bundle to the PC.

Step 3 Click **Browse** to locate the bundle on the PC. The path to this bundle is displayed in the Location of client software field.

Step 4 Click **Install** to load them onto the router so they are available to be downloaded to clients.

Packages Reference

This section contains the following parts:

- Packages
- Install Package
- Locating the Install Bundle

Packages

This window enables you to obtain software install bundles that must be downloaded to clients to support Cisco IOS SSL VPN features, and to load them on the router.

Follow the steps described in the window to download the install bundles from Cisco.com to your PC, and then copy them from your PC to the router. If you need to obtain any of the install bundles, start with Step 1 by clicking on the link to the download site.

Note Access to these download sites requires a CCO username and password. If you don't have a CCO username and password, you can obtain one by clicking Register at the top of any Cisco.com webpage, and completing the form that is displayed. Your username and password will be mailed to you.

If you have already loaded install bundles onto your PC or the router, complete steps 2 and 3 to specify the current location of the install bundles and copy them to router flash.

Click the **...** button in each section to specify the current location of the install bundle.

After you specify the current location, and where you want to copy it to in router flash, click **Install**.

After the bundles have been loaded onto the router, the window displays name, version, and build date information about the package. If an administration tool is available with the package, the window displays a button enabling you to run this tool.

The Cisco IOS SSL VPN client install bundle is available from the following link:

http://www.cisco.com/cgi-bin/tablebuild.pl/sslvpnclient

The Cisco Secure Desktop install bundle is available from the following link:

http://www.cisco.com/cgi-bin/tablebuild.pl/securedesktop

Install Package

Specify the current location of an install bundle by browsing for it in this window. If the install bundle is already located on the router, click **Router** and browse for it. If it is located on the PC, click **My Computer** and browse for it. When you have specified the current location of the install bundle, click **OK**.

The location will be visible in the Packages window.

Locating the Install Bundle

Use the following procedure to locate software install bundles for Cisco CP so that it can use that location in the Cisco IOS SSL VPN configuration, or, if necessary, load the software onto the router.

Note You may need a CCO username and password in order to obtain software from Cisco software download sites. To obtain these credentials, click **Register** at the top of any Cisco.com webpage and provide the information asked for. Your userid and password will be e-mailed to you.

Step 1 Look at the **Location** field. If the path to the install bundle is in that field, no further action need be taken. Cisco CP configures the router to download the software from that location. Example 31-3 shows a path to a software install bundle.

Example 31-3 Full Tunnel Package Installed on Router

```
flash:sslclient-win-1.0.2.127.pkg
```

Step 2 If the Location field is empty, click the **...** button to the right of the field to specify the location of the software.

Step 3 If the software is installed on the router, choose **Router File System** and then browse for the file.

If the software is on your PC, choose **My Computer** and browse for the file.

Cisco CP places the router file system or PC path you specified in the Location field.

Step 4 If the software is not on the router or on your PC, you must download it to your PC, and then provide the path to the file in this field.

a. Click the Download latest... link in the window. You are connected to the download page for the software you want.

b. There may be software packages available for Cisco IOS platforms and other platforms on the web page that appears. Double-click the latest version of the software that you want to download for Cisco IOS platforms, and provide your CCO username and password when prompted to do so.

c. Download the package to the PC.

d. In the Cisco IOS SSL VPN wizard, click the **...** button to the right of the Location field, choose **My Computer** in the Select Location window that is displayed, and navigate to the directory in which you placed the file.

e. Select the install bundle file then click **OK** in the Select Location window. Cisco CP places that path in the Location field. examples shows an install bundle located on the PC's desktop.

Example 31-4 Full Tunnel Package Installed on Router

```
C:\Documents and Settings\username\Desktop\sslclient-win-1.1.0.154.pkg
```

Cisco CP installs the software onto the router from the PC directory that you specified when you deliver the configuration to the router by clicking **Finish**.

Additional Help Topics

The help topics in this section provide additional background information, and procedures that you may need to perform manually.

This section contains the following topics:

- Cisco IOS SSL VPN Contexts, Gateways, and Policies
- Learn More about Port Forwarding Servers
- Learn More About Group Policies
- Learn More About Split Tunneling
- Cisco IOS SSL VPN Links on Cisco.com
- How do I verify that my Cisco IOS SSL VPN is working?
- How do I configure a Cisco IOS SSL VPN after I have configured a firewall?
- How do I associate a VRF instance with a Cisco IOS SSL VPN context?

Cisco IOS SSL VPN Contexts, Gateways, and Policies

Cisco CP provides an easy way to configure Cisco IOS SSL VPN connections for remote users. However, the terminology used in this technology can be confusing. This help topic discusses the Cisco IOS SSL VPN terms used in Cisco CP configuration windows and describes how Cisco IOS SSL VPN components work together. An example of using the Cisco IOS SSL VPN wizard and edit windows in Cisco CP is also provided.

Before discussing each component individually, it is helpful to note the following:

- One Cisco IOS SSL VPN context can support multiple group policies.
- Each context must have one associated gateway.
- One gateway can support multiple contexts.
- If there is more than one group policy on the router, a AAA server must be used for authentication.

Cisco IOS SSL VPN Contexts

A Cisco IOS SSL VPN context identifies resources needed to support SSL VPN tunnels between remote clients and a corporate or private intranet, and supports one or more group policies. A Cisco IOS SSL VPN context provides the following resources:

- An associated Cisco IOS SSL VPN gateway, which provides an IP address that clients can reach and a certificate used to establish a secure connection.
- Means for authentication. You can authenticate users locally, or by using AAA servers.
- The HTML display settings for the portal that provides links to network resources.
- Port forwarding lists that enable the use of Thin Client applets on remote clients. Each list should be configured for use in a specific group policy.
- URL lists that contain links to resources in the corporate intranet. Each list should be configured for use in a specific group policy.
- NetBIOS Name Server lists. Each list should be configured for use in a specific group policy.

These resources are available when configuring Cisco IOS SSL VPN group policies.

A Cisco IOS SSL VPN context can support multiple group policies. A Cisco IOS SSL VPN context can be associated with only one gateway.

Cisco IOS SSL VPN Gateways

A Cisco IOS SSL VPN gateway provides a reachable IP address and certificate for one or more Cisco IOS SSL VPN contexts. Each gateway configured on a router must be configured with its own IP address; IP addresses cannot be shared among gateways. It is possible to use the IP address of a router interface, or another reachable IP address if one is available. Either a digital certificate or a self-signed certificate must be configured for gateways to use. All gateways on the router can use the same certificate.

Although one gateway can serve multiple Cisco IOS SSL VPN contexts, resource constraints and IP address reachability must be taken into account.

Cisco IOS SSL VPN Policies

Cisco IOS SSL VPN group policies allow you to accommodate the needs of different groups of users. A group of engineers working remotely needs access to different network resources than sales personnel working in the field. Business partners and outside vendors must access the information they need to work with your organization, but you must ensure that they do not have access to confidential information or other resources they do not need. Creating a different policy for each of these groups allows you provide remote users with the resources they need, and prevent them from accessing other resources.

When you configure a group policy, resources such as URL lists, Port Forwarding lists, and NetBIOS name server lists configured for the policy's associated context are available for selection.

If there is more than one group policy configured on the router, you must configure the router to use a AAA server to authenticate users and to determine which policy group a particular user belongs to. Click Learn More About Group Policies for more information.

Example

In the example presented in Table 31-26 on page 31-45, a user clicks **Create a new SSL VPN** and uses the wizard to create the first Cisco IOS SSL VPN configuration on the router. Completing this wizard creates a new context, gateway, and group policy. The following table contains the information the user enters in each wizard window, and the configuration that Cisco CP creates with that information.

Table 31-26 Creating a New SSLVPN

Cisco IOS SSL VPN Wizard Window	Configuration
Create SSL VPN Window	
Prerequisite Tasks area indicates that digital certificates are not configured on the router. User clicks **self signed certificate** and configures a certificate in the Persistent Self Signed Certificate dialog. The user does not change the Cisco CP-supplied name Router_Certificate. User clicks **Create new SSL VPN**.	Cisco CP configures a self-signed certificate named "Router_Certificate" that will be available for use in all Cisco IOS SSL VPN configurations.
IP Address and Name Window	
User enters the following information: IP Address: 172.16.5.5 Name: Asia Check **Enable secure access through 192.168.1.1**. Certificate: **Router_Certificate**	Cisco CP creates a context named "Asia." Cisco CP creates a gateway named "gateway_1" that uses the IP address 172.16.5.5 and Router_Certificate. This gateway can be associated with other Cisco IOS SSL VPN contexts. Users will access the Cisco IOS SSL VPN portal by entering http://172.16.5.5/Asia. If this gateway is associated with additional contexts, the same IP address will be used in the URL for those contexts. For example if the context Europe is also configured to use gateway_1, users enter https://172.16.5.5/Europe to access the portal. After the configuration is delivered to the router, users must enter http://172.16.5.5:4443 to launch Cisco CP using this IP address. Cisco CP also begins to configure the first group policy, named policy_1.
User Authentication Window	

Table 31-26 Creating a New SSLVPN (continued)

Cisco IOS SSL VPN Wizard Window	Configuration
User chooses **Locally on this router**. User adds one user account to the existing list.	Cisco CP creates the authentication list "sdm_vpn_xauth_ml_1." This list will be displayed in the Cisco IOS SSL VPN Contexts window when the user completes the wizard. Those users listed in the User Authentication window are the members of this authentication list, and will be governed by policy_1.
Configure Intranet Websites Window	
User configures the URL list Ulist_1. The heading is "Taiwan."	The URL list with the heading Taiwan will be visible in the portal that users in "sdm_vpn_xauth_ml_1" see when they log in. The URL list will be available for configuration in other group policies configured under the context "Asia."
Enable Full Tunnel Window	
User clicks **Enable Full Tunnel**, and selects a predefined address pool. No advanced options are configured.	Client PCs will download Full Tunnel client software when they log in for the first time, and a full tunnel is established between the PC and the router when the user logs in to the portal.
Customize SSL VPN Portal Window	
User chooses **Ocean Breeze**.	Cisco CP configures the HTTP display settings with this color scheme. The portal displayed when policy_1 users log in uses these settings. These portal settings also apply to all policies configured under the context "Asia." The user can customize the HTTP display settings in the Edit SSL VPN windows after completing the wizard.
SSL VPN Passthrough Configuration Window	
User checks **Allow SSL VPN to work with NAC and Firewall**	Cisco CP adds an ACL with the following entry. `permit tcp any host 172.16.5.5 eq 443`

Table 31-26 Creating a New SSLVPN (continued)

Cisco IOS SSL VPN Wizard Window	Configuration
Summary Window	
The Summary window displays the information shown at the right. Additional details can be viewed in the Edit SSL VPN windows.	SSL VPN Policy Name: policy_1 SSL VPN Gateway Name: gateway_1 User Authentication Method List: Local Full Tunnel Configuration SVC Status: Yes IP Address Pool: Pool_1 Split Tunneling: Disabled Split DNS: Disabled Install Full Tunnel Client: Enabled

When this configuration is delivered, the router has one Cisco IOS SSL VPN context named Asia, one gateway named gateway_1, and one group policy named policy_1. This is displayed in the Edit SSL VPN window as shown in the following table:

Name	Gateway	Domain	Status	Administrative Status
Asia	gateway_1	Asia		In Service

Details about SSL VPN context Asia:	
Item Name	**Item Value**
Group Policies	
policy_1	
Services	URL Mangling, Full Tunnel
URLs exposed to Users	http://172.16.5.5/pricelist
	http://172.16.5.5/catalog
Servers Exposed to users	<None>
WINS servers	<None>

policy_1 provides the basic Cisco IOS SSL VPN service of URL mangling, and specifies that a full tunnel be established between clients and the router. No other features are configured. You can add features to policy_1, such as Thin Client and Common Internet File System by choosing **Configure advanced features for an existing SSL VPN**, choosing **Asia** and **policy_1** in the Select the Cisco IOS SSL VPN user group window, then choosing the features in the Advanced Features window. Additional URL lists can also be configured in this wizard.

You can create a new group policy under context "Asia" by choosing **Add a new policy to an existing SSL VPN for a new group of users**.

You can customize settings and the policies configured for context Asia by choosing Asia in the context list and clicking **Edit**. The Edit SSL VPN Context Asia window displays a tree that allows you to configure more resources for the context, and to edit and configure additional policies. You can edit the settings for gateway_1 by clicking **SSL VPN Gateways** under the SSL VPN node, selecting gateway_1, then clicking **Edit**.

Learn More about Port Forwarding Servers

Port forwarding enables a remote Cisco IOS SSL VPN user to connect to static ports on servers with private IP addresses on the corporate intranet. For example, you can configure port forwarding on a router to give remote users Telnet access to a server on the corporate intranet. To configure port forwarding, you need the following information:

- The IP address of the server.
- The static port number on the server.
- The remote port number for the client PC. In the dialog, Cisco CP supplies a port number that is safe to use.

To allow users to use Telnet to connect to a server with the IP address 10.0.0.100 (port 23) for example, you would create a port mapping entry with the following information:

Server IP address: 10.0.0.100

Server port on which user is connecting: 23

Port on client PC: Cisco CP-supplied value. 3001 for this example.

Description: SSL VPN Telnet access to server-a. This description will be on the portal.

When the client's browser connects to the gateway router, a portal applet is downloaded to the client PC. This applet contains the server's IP address and static port number, and the port number that the client PC is to use. The applet does the following:

- Creates a mapping on the client PC that maps traffic for port 23 on 10.0.0.100 to the PC's loopback IP address 127.0.0.1, port 3001.
- Listens on port 3001, IP address 127.0.0.1

When the user runs an application that connects to port 23 on 10.0.0.100, the request is sent to 127.0.0.1 port 3001. The portal applet listening on that port and IP address gets this request and sends it over the Cisco IOS SSL VPN tunnel to the gateway. The gateway router forwards it to the server at 10.0.0.100, and sends return traffic back to the PC.

Learn More About Group Policies

Cisco IOS SSL VPN group policies define the portal and links for the users included in those policies. When a remote user enters the Cisco IOS SSL VPN URL they have been given, the router must determine which policy the user is a member of so that it can display the portal configured for that policy. If only one Cisco IOS SSL VPN policy is configured on the router, it can authenticate users locally or using a AAA server, and then display the portal.

However, if more than one policy is configured, the router must rely on a AAA server to determine which policy to use each time a remote user attempts to log in. If you have configured more than one Cisco IOS SSL VPN group policy, you must configure at least one AAA server for the router, and you must configure a policy on that server for each group of users for which you created a Cisco IOS SSL VPN policy. The policy names on the AAA server must be the same as the names of the group policies configured on the router, and they must be configured with the credentials of the users who are members of the group.

For example, if a router has been configured with local authentication for Bob Smith, and only the group policy Sales has been configured, there is only one portal available to display when Bob Smith attempts to log in. However, if there are three Cisco IOS SSL VPN group policies configured, Sales, Field, and Manufacturing, the router cannot, by itself, determine which policy group Bob Smith is a member of. If a AAA server is configured with the proper information

for those policies, the router can contact that server, and receive the information that Bob Smith is a member of the group Sales. The router can then display the correct portal for the Sales group.

For information on how to configure the AAA server, see the "Configuring RADIUS Attribute Support for SSL VPN" section in the *SSL VPN Enhancements* document at the following link:

http://www.cisco.com/en/US/products/ps6441/products_feature_guide09186a00805eeaea.html#wp1396461

Learn More About Split Tunneling

When a Cisco IOS SSL VPN connection is set up with a remote client, all traffic that the client sends and receives may travel through the Cisco IOS SSL VPN tunnel, including traffic that is not on the corporate intranet. This can degrade network performance. Split tunneling allows you to specify the traffic that you want to send through the Cisco IOS SSL VPN tunnel and allow other traffic to remain unprotected and be handled by other routers.

In the Split Tunneling area, you can specify the traffic to *include* in the Cisco IOS SSL VPN and exclude all other traffic by default, or you can specify the traffic to *exclude* from the CCisco IOS SSL VPN and include all other traffic by default.

For example, suppose that your organization uses the 10.11.55.0 and the 10.12.55.0 network addresses. Add these network addresses to the Destination Network list, then click the **Include traffic** radio button. All other Internet traffic, such as traffic to Google or Yahoo, would go directly to the Internet.

Or suppose it is more practical to exclude traffic to certain networks from the Cisco IOS SSL VPN tunnel. In that case, enter the addresses for those networks in the Destination Networks list, then click the **Exclude traffic** radio button. All traffic destined for the networks in the Destination Networks list is sent over nonsecure routes, and all other traffic is sent over the Cisco IOS SSL VPN tunnel.

If users have printers on local LANs that they want to use while connected to the Cisco IOS SSL VPN, you must click **Exclude local LAN** in the Split Tunneling area.

Note The Destination Network list in the Split Tunneling area may already contain network addresses. The traffic settings you make in the Split Tunneling area override any settings previously made for the listed networks.

Cisco IOS SSL VPN Links on Cisco.com

This help topic lists the current links that provide the most useful information on Cisco IOS SSL VPN.

The following link provides access to documents that describe Cisco IOS SSL VPN. Return to this link from time to time for the latest information.

www.cisco.com/go/iosSSLVPN

The following link explains how to configure a AAA server using the RADIUS protocol for Cisco IOS SSL VPN.

http://www.cisco.com/en/US/products/ps6441/products_feature_guide09186a00805eeaea.html#wp1396461

How do I verify that my Cisco IOS SSL VPN is working?

The best way to determine that a Cisco IOS SSL VPN context will provide the access that you configured for users is to configure yourself as a user, then attempt to access all the websites and services that the context is configured to provide for them. Use the following procedure as a guide in setting up this test.

Step 1 Ensure that credentials you can use are included in all appropriate policies on the AAA server.

Step 2 If you can do so, open a Cisco CP session to the router so that you can monitor the Cisco IOS SSL VPN traffic that you will create. This must be done on a separate PC if the PC you use to test the Cisco IOS SSL VPN context is not in a network from which you can access Cisco CP. Go to **Monitor > VPN Status > SSL VPN**.

Step 3 Enter the URL to each of the web portals that are configured for this Cisco IOS SSL VPN context. Determine that each page has the appearance that you configured for it, and that all links specified in the URL lists for the policy appear on the page.

Step 4 Test all links and services that should be available to users included in this policy. If any of the policies that you are testing provide for downloading Cisco Secure Desktop or the Full Tunnel client software, enter the URLs to the web portals for those policies and click the links that will require the download of this software. Determine that the software downloads properly and that you are able to access the services that a user should be able to access from these links.

Step 5 If you were able to establish a Cisco CP session before you began testing, click the branch for the context that you are testing and observe the Cisco IOS SSL VPN traffic statistics in the Cisco IOS SSL VPN window.

Step 6 Based on the results of your tests, go back to Cisco CP if necessary and fix any configuration problems you discovered.

How do I configure a Cisco IOS SSL VPN after I have configured a firewall?

If you have already configured a firewall, you can still use the Cisco IOS SSL VPN wizards in Cisco CP to create Cisco IOS SSL VPN contexts and policies. Cisco CP validates the Cisco IOS SSL VPN CLI commands that it generates against the existing configuration on the router. If it detects an existing firewall configuration that would have to be modified to allow Cisco IOS SSL VPN traffic to pass through, you are informed. You can allow Cisco CP to make the necessary modifications to the firewall, or you can leave the firewall intact and make the changes manually by going to **Configure > Security > Firewall > Firewall > Edit Firewall Policy/ACL** and entering the permit statements that allow Cisco IOS SSL VPN traffic to pass through the firewall.

How do I associate a VRF instance with a Cisco IOS SSL VPN context?

VPN Routing and Forwarding (VFR) instances maintain a routing table and a forwarding table for a VPN. You can associate a VRF instance or name with a Cisco IOS SSL VPN context by going to **Configure > Security > VPN > SSL VPN > SSL VPN Manager > Edit SSL VPN**. Select the context that you want to associate a VRF instance to and click **Edit**. Select the name of the VRF instance in the dialog displayed.

Note The VRF instance must already be configured on the router.

CHAPTER 32

SSL VPN Enhancements

This chapter explains how to configure Cisco IOS SSL VPN enhancements available with Cisco IOS releases 12.4(9)T, and 12.4(11)T.

See SSL VPN Reference for links to the help topics.

SSL VPN Reference

- SSL VPN Context: Access Control Lists
- Add or Edit Application ACL
- Add ACL Entry
- Action URL Time Range
- Add or Edit Action URL Time Range Dialog
- Add or Edit Absolute Time Range Entry
- Add or Edit Periodic Time Range Entry

SSL VPN Context: Access Control Lists

You can create Application ACLs to control access to specific URLs. This window displays the Application ACLs created for the selected context, and enables you to edit existing ACLs and create new ones.

Field Reference

Table 32-1 SSL VPN Access Control List Fields

Element	Description
Access Control List	
Add	To create an Application ACL, click **Add** and create the Application ACL in the displayed dialog.
Edit	To edit an Application ACL, choose the ACL and click **Edit**. Edit the ACL in the displayed dialog.
Delete	To delete an ACL choose the ACL and click **Delete**.
ACL Name	This table lists the names of the ACLs created for this context.
Details of ACL	
Action	One of the following: • Permit—Access to the URL in this entry is allowed. • Deny—Access to the URL in this entry is denied.
URL	The URL to which the ACL controls access.
Action URL Time Range	The range or periods of time that this ACL is in effect.

Add or Edit Application ACL

Create or edit an application ACL in this window. Cisco IOS SSL VPN uses application ACLs to specify permitted and denied URLs. One ACL can consist of multiple entries.

Field Reference

Table 32-2 Add or Edit SSL VPN Context ACL Fields

Element	Description
ACL Name	Enter a name for this ACL.
Add	To create an entry for this ACL, click **Add** and create the entry in the displayed dialog.

Table 32-2 Add or Edit SSL VPN Context ACL Fields (continued)

Element	Description
Edit	To modify an entry, select the entry and click **Edit**. Then modify it in the displayed dialog.
Delete	To remove an entry from this ACL, select the entry and click **Delete**.
List Area	
Action	One of the following: • Permit—Access to the URL in this entry is permitted. • Deny—Access to the URL in this entry is denied.
URL	The URL to which this ACL entry controls access.
Action URL Time Range	The name of the time range applied to this ACL entry.

Add ACL Entry

Add or Edit an ACL entry in this window.

Field Reference

Table 32-3 Add or Edit SSL VPN Context ACL Entry Fields

Element	Description
Action	Choose one of the following: • Permit—Allow access to the URL in this entry. • Deny—Deny access to the URL in this entry is denied.
URL	
Any	To have this ACL entry apply to any URL, click **Any**.

Table 32-3 Add or Edit SSL VPN Context ACL Entry Fields (continued)

Element	Description

Specific URL	To have this ACL entry apply to a URL that you specify, click **Specific URL**. Then, enter the URL in the field. Be sure to enter the entire URL. The following are examples of valid URLs:
	`http://www.cisco.com`
	`https://www.foo.com`
	`ftp://ftp.bad-down-loads.com`

Action URL Time Range	The action URL time range can specify the start and end date for the action specified, as well as the time periods that the action is to be in effect.To place a time range entry in this field, click the button to the right of the field and choose one of the following: • Add Time Range List—Choose this option to create a new time range entry. • Select Time Range List—Choose this option to select an existing time range entry. • Remove Time Range List—Choose this option to remove the current time range entry.

Action URL Time Range

Add time range lists in this window. Time range lists specify when permit or deny actions are to be applied.

Field Reference

Table 32-4 Action URL Time Range Fields

Element	Description
Time Range Entry	
Add	To create a time range entry, click **Add**, and create the entry in the displayed dialog.
Edit	To edit an entry, select the entry, and click Edit. Make changes to the entry in the displayed dialog.
Delete	To remove an entry, select the entry and click **Delete**.

Table 32-4 Action URL Time Range Fields (continued)

Element	Description
Item Name	The Item Name list displays the time range entries configured for this context.
Details of Action URL Time Range	
The Details area displays additional information about the selected time range entry.	
Type	One of the following: • Absolute—The time range specifies an absolute date. There can be a start date, and there can be an end date, or both. • Periodic—The time range specifies days of the week, so that you can include some days and not others. It can also specify a start time and an end time.

Period	If the entry type is Periodic, this column shows which days are included. The following examples show possible entries:
	`daily`
	`weekdays`
	`Sun, Tue, Sat`

Start Time	The starting time and date is displayed for absolute entries, for example, 10:00 11 Nov 2007. The starting time is displayed for periodic entries, for example 8:00.
End Time	The end time and date is displayed for absolute entries, for example, 10:00 11 Dec 2007. The end time is displayed for periodic entries, for example 23:00.

Add or Edit Action URL Time Range Dialog

Create or edit a time range entry in this dialog. A time range entry can consist of multiple subentries.

Field Reference

Table 32-5 Time Range Fields

Element	Description
Time Range Name	Enter a name for the time range.
Time Range Entry List Area	
Type	One of the following: • Absolute—The time range specifies an absolute date. There can be a start date, and there can be an end date, or both. • Periodic—The time range specifies days of the week, so that you can include some days and not others. It can also specify a start time and an end time.

Period	If the entry type is Periodic, this column shows which days are included. The following examples show possible entries:
	`daily`
	`weekdays`
	`Sun, Tue, Sat`

Start	The starting time and date is displayed for absolute entries, for example, 10:00 11 Nov 2007. The starting time is displayed for periodic entries, for example 8:00.
End	The end time and date is displayed for absolute entries, for example, 10:00 11 Dec 2007. The end time is displayed for periodic entries, for example 23:00.
Add	To add an entry, click **Add,** and choose **Absolute**, or **Periodic**. If an absolute entry has been added, the Absolute option is disabled.
Edit	To edit a time range entry, select the entry and click **Edit**.
Delete	To remove a time range entry, select the entry and click **Delete**.

Add or Edit Absolute Time Range Entry

Create or edit an absolute time range entry in this window. The time range can have a start date, and end date, or both.

Field Reference

Table 32-6 Absolute Time Range Fields

Element	Description
Start	
To specify a start date, click **Start**, and enter a date and time.	
From Date	Enter the starting date in dd/mm/yyyy format. For example, entering 1/10/2007 specifies a start date of October 1, 2007.
Time	Enter the starting time in 24-hour format. For example, entering 13:00 specifies a starting time of 1:00 p.m.
End	
To specify an end date, click **End**, and enter a date and time	
Till Date	Enter the end date in dd/mm/yyyy format. For example, entering 1/1/2008 specifies an end date of January 1, 2008.
Time	Enter the ending time in 24-hour format. For example, entering 23:59 specifies an ending time of 11:59 p.m.

Add or Edit Periodic Time Range Entry

Create or edit a periodic time range entry in this window. You can specify which days to include in the range, and starting and ending days and times.

Field Reference

Table 32-7 Periodic Time Range Fields

Element	Description
Period	Choose one of the following: • Specific weekdays—To select specific days, choose this option, and then check the boxes next to the days of the week that you want to include. • weekdays—To include only Monday, Tuesday, Wednesday, Thursday, and Friday, choose this option. • weekend—To include only Saturday, and Sunday, choose this option. • daily—To include each day of the week, choose this option.
From Day	This option is available when you choose **Specific weekdays**. Check the box next to one day of the week to specify the From day.
Till Day	This option is available when you choose **Specific weekdays**, and you have specified one From day. Click the button and choose the Till day from the list. If more than one From day is checked, this option is disabled.
Duration	
Start Time	Enter the starting time in 24-hour format. For example, entering 13:00 specifies a starting time of 1:00 p.m.
End Time	Enter the ending time in 24-hour format. For example, entering 23:59 specifies an ending time of 11:59 p.m.

CHAPTER 33

IOS SSL VPN AnyConnect Client

This chapter contains the following sections:

- About Cisco AnyConnect, page 33-1
- Installing AnyConnect Packages on the Router, page 33-1
- Removing AnyConnect Packages from the Router, page 33-3
- Changing the SSL VPN Package Priority, page 33-4
- Anyconnect Client Screen Reference, page 33-5
- Installing the Cisco Secure Desktop Client on the Router, page 33-4

About Cisco AnyConnect

The Cisco AnyConnect client provides remote end users running Microsoft Vista, Windows 7, Windows XP or Windows 2000, Linux, or Macintosh OS X, with the benefits of a Cisco SSL VPN client, and supports applications and functions unavailable to a clientless, browser-based SSL VPN connection. In addition, the AnyConnect client supports IPv6 over an IPv4 network.

AnyConnect client support is available with Cisco IOS 12.4(20)T and later releases.

Installing AnyConnect Packages on the Router

Complete the following steps to install AnyConnect packages on the router:

Step 1 From the Manage Community screen, choose the community that contains the router that you want to configure.

Step 2 Discover the router.

Step 3 If you have already discovered multiple routers, choose the IP address of the router that you want to configure from the Select Community Member list.

Step 4 Click **Configure > Security > VPN > SSL VPN > Packages**.

Step 5 To verify that the router supports Anyconnect, examine the top part of the screen. If there is a box titled Cisco SSL VPN Client Software, and a list with the columns Package Installed and Sequence Number, the router supports Anyconnect. If the Packages screen does not display this list, then the router does not support this feature.

Step 6 Click **Install Package**.

Step 7 In the Install SSL VPN Client Package dialog, specify whether the Anyconnect installation bundle is located on router Flash memory, or the PC hard disk. This bundle must have a name that ends with a.pkg extension. Do one of the following:

If the installation bundle is on the router file system, do the following:

a. Choose **Router File System**.

b. Click **Browse** to locate the install bundle.

c. When you have chosen the file, click **OK**. The path to the installation bundle appears in the field next to Router File System, for example, flash:/anyconnect-win-2.2.0140-k9.pkg.

If the installation bundle is on the PC, do the following:

a. Choose **My Computer**.

b. Click **Browse** to locate the installation bundle on the PC.

c. When you have chosen the file, click **OK**. The path to the installation bundle appears in the field next to My Computer, for example C:\downloads\anyconnect-win-2.2.0140-k9.pkg.

If the installation bundle is not on the router file system or on the PC, click **Download the latest Cisco Anyconnect Installation Bundle**, go to the download page, and download the package to the PC.

The Cisco IOS Anyconnect client install bundle is available from the following link:

http://www.cisco.com/cgi-bin/tablebuild.pl/anyconnect

Note You must have a Cisco.com login user ID and password to download the installation bundle.

Step 8 If you downloaded an Installation bundle from the Cisco.com download page, it may be packaged in a zip file. Extract the contents of the zip file to a folder, return to the Install SSL VPN Client Package dialog, choose **My Computer**, and browse for the .pkg file that you want to install.

Step 9 In the Sequence field, choose the sequence number for this package. If another package is already installed, the sequence number for that package is not available in the list.

Step 10 Click **Install**. When the installation has completed, the filename appears in the Package Installed column, and the sequence number that you assigned it appears in the Sequence Number column. Other information, such as the version number and build date appear in the area under the list.

Step 11 To install additional packages, click **Install Package** and repeat steps Step 7 through Step 10

Removing AnyConnect Packages from the Router

Complete the following steps to remove AnyConnect packages from the router:

Step 1 From the Manage Community screen, choose the community that contains the router that you want to configure.

Step 2 Discover the router.

Step 3 If you have already discovered multiple routers, choose the IP address of the router that you want to configure from the Select Community Member list.

Step 4 Click **Configure > Security > VPN > SSL VPN > Packages**.

Step 5 In the Cisco SSL VPN Client Software box of the Packages screen, choose the package that you want to remove, click **Uninstall Package**, and click **OK** in the confirmation message screen. The package is removed.

Changing the SSL VPN Package Priority

To change the SSL VPN package priority, complete these steps:

Step 1 Click **Configure > Security > VPN > SSL VPN > Packages**.

Step 2 From the package list in the Cisco SSL VPN Client Software area, choose the package whose priority you want to change.

Step 3 Click **Change Sequence**.

Step 4 In the displayed dialog, review the information for the package. Verify that it displays the package whose sequence number you want to change, and verify the current sequence number.

Step 5 In the New Sequence field, choose a new sequence number for the package.

Step 6 Click **OK**. The dialog closes, and the changed sequence number is displayed in the package list.

Installing the Cisco Secure Desktop Client on the Router

Complete the following steps to install the Cisco Secure Desktop (CSD) package on the router:

Step 1 From the Manage Community screen, choose the community that contains the router that you want to configure.

Step 2 Discover the router.

Step 3 If you have already discovered multiple routers, choose the IP address of the router that you want to configure from the Select Community Member list.

Step 4 Click **Configure** > **Security** > **VPN** > **SSL VPN** > **Packages**.

Step 5 Do one of the following:

- If you have downloaded the CSD installation bundle to the PC, click **Browse**, choose **On My PC** in the dialog, and locate the file. Then, click **Install** to load the package into router memory.
- If you have not downloaded a CSD installation bundle, click **Download the latest Cisco Secure Desktop (CSD) installation bundle**. In the download screen, choose a package that is described as Secure Desktop software for IOS platforms. Save the package to the PC. Then, in the Packages screen, click **Browse**, locate the package on the PC, and click **Install**.

When the package has been installed, the filename appears in the Destination folder on the router field.

Anyconnect Client Screen Reference

- Cisco SSL VPN Client Software, page 33-5
- Change SSL VPN Package Priority, page 33-6

Cisco SSL VPN Client Software

In this screen, install SSL VPN client software packages on the router. Once installed in the router file system, the router can download these packages to clients.

How to Get to this Screen

Click **Configure** > **Security** > **VPN** > **SSL VPN** > **Packages**.

Related Links

- About Cisco AnyConnect, page 33-1
- Installing AnyConnect Packages on the Router, page 33-1

- Removing AnyConnect Packages from the Router, page 33-3
- Installing the Cisco Secure Desktop Client on the Router, page 33-4

Field Reference

Table 33-1 SSL VPN Packages Screen

Element	Description
Cisco SSL VPN Client Software Area	
Install Package	To display a dialog that enables you to install a new package on the router, click **Install Package**.
Uninstall Package	To remove a package that has been installed, choose the package name from the list, and click **Uninstall Package**.
Change Sequence	To change the sequence number for a package, choose the package name, click **Change Sequence**, and select an available sequence number.
Package Installed	This column displays a list of the packages that have been installed.
Sequence Number	This column displays the sequence number for the package.
Cisco Secure Desktop Software Area	
Install Status	One of the following values: • Installed • Not Installed
To Install procedure	If the Cisco Secure Desktop installation package is not installed on the router, you can follow the procedure in this part of the screen to install it. Clicking the link Download the latest Cisco Secure Desktop (CSD) bundle takes you to a download page from which you can download the installation bundle to the PC, and then install it on the router. See Installing the Cisco Secure Desktop Client on the Router, page 33-4 for the complete procedure.

Change SSL VPN Package Priority

In this screen, change the sequence number assigned to the package.

How to Get to this Screen

Click **Configure > Security > VPN > SSL VPN > Packages > Change Sequence**.

Related Links

- About Cisco AnyConnect, page 33-1
- Changing the SSL VPN Package Priority, page 33-4

Field Reference

Table 33-2 Change SSL VPN Package Priority

Element	Description
Package	This read-only field displays the name of the file selected in the Packages screen.
Current Priority	This read-only field displays the current sequence number of the package.
Priority	This field lists the available sequence numbers. To change the sequence number, choose an available number from this list. If a sequence number is assigned to another package, it cannot be selected from this list.

CHAPTER 34

VPN Options and VPN Keys Encryption

This chapter describes the following features:

- VPN Options
- VPN Keys Encryption

VPN Options

VPN options are default settings that apply to VPN and VPN component policies. Some of these settings can be overridden when a specific policy is created. See VPN Options Reference for a description of each screen.

VPN Options Reference

This section contains the following parts:

- VPN Options
- VPN Global Settings: IKE
- VPN Global Settings: IPSec
- VPN Global Settings: Easy VPN Server

VPN Options

This window displays the VPN global settings for the router.

How to Get to this Screen

- **Configure > Security > VPN > VPN Components > VPN Options**.

Field Reference

Table 34-1 VPN Global Settings Fields

Element	Description
Edit Button	Click the **Edit** button to add or change VPN global settings.
Enable IKE	The value is True if IKE is enabled; it is False if IKE is disabled. **Note** If IKE is disabled, VPN configurations will not operate. You can click **Edit** and enable IKE in the IKE tab of the VPN Global Settings screen.
Enable Aggressive Mode	The value is True if Aggressive Mode is enabled; it is False if Aggressive Mode is disabled.The Aggressive Mode feature allows you to specify RADIUS tunnel attributes for an IPSec peer and to initiate an IKE aggressive mode negotiation with the tunnel attributes.
XAuth Timeout	The number of seconds the router is to wait for a a system to respond to the XAuth challenge.
IKE Identity	Either the host name of the router or the IP address that the router will use to identify itself in IKE negotiations.

Table 34-1 VPN Global Settings Fields

Element	Description
Dead Peer Detection	Dead Peer Detection (DPD) enables a router to detect a dead peer and, if detected, delete the IPSec and IKE security associations with that peer. If DPD is enabled, the following additional information is displayed: • IKE Keepalive (Sec)—The value is the number of seconds that the router waits between sending IKE keepalive packets. • IKE Retry (Sec)—The value is the number of seconds that the router waits between attempts to establish an IKE connection with the remote peer. By default, "2" seconds is displayed. • DPD Type—Either **On Demand** or **Periodic**. If set to **On Demand**, DPD messages are sent on the basis of traffic patterns. For example, if a router has to send outbound traffic and the liveliness of the peer is questionable, the router sends a DPD message to query the status of the peer. If a router has no traffic to send, it never sends a DPD message. If set to **Periodic**, the router sends DPD messages at the interval specified by the IKE Keepalive value.
IPSec Security Association (SA) Lifetime (Sec)	The amount of time after which IPSec security associations (SAs) will expire and be regenerated. The default is 3600 seconds (1 hour).
IPSec Security Association (SA) Lifetime (Kilobytes)	The number of kilobytes that the router can send over the VPN connection before the IPSec SA expires. The SA will be renewed after the shortest lifetimes is reached.
Syslog Messages for Easy VPN Connections	This field can have the following values: • Enabled—Syslog messages are enabled for all Easy VPN connections. • Enabled for groups *name*, *name*—Syslog messages are enabled for the groups listed. For example, the row might display Enabled for groups SJ5, SF3. • Disabled—Syslog messages are disabled.

VPN Global Settings: IKE

This window lets you specify global settings for IKE and IPSec.

How to Get to this Screen

- **Configure > Security > VPN > VPN Components > VPN Options > Edit > IKE**.

Field Reference

Table 34-2 IKE Global Settings

Element	Description
Enable IKE	Leave this box checked if you want to use the VPN feature. **Caution** If IKE is disabled, VPN configurations will not work.
Enable Aggressive mode	The Aggressive Mode feature allows you to specify RADIUS tunnel attributes for an IPSec peer and to initiate an IKE aggressive mode negotiation with the tunnel attributes.
Identity (of this router)	This field specifies the way the router will identify itself. Select either **IP address** or **host name**.
XAuth Timeout	The number of seconds the router is to wait for a response from a system requiring XAuth authentication.
Enable Dead Peer Detection (DPD)	
Dead Peer Detection (DPD) enables a router to detect a dead peer and, if detected, delete the IPSec and IKE security associations with that peer. The Enable Dead Peer Detection check box is disabled when the Cisco IOS image that the router is using does not support DPD.	
Keepalive	Specify the number of seconds that the router should maintain a connection when it is not being used.

Table 34-2 IKE Global Settings (continued)

Element	Description
Retry	Specify the number of seconds that the router should wait between attempts to establish an IKE connection with a peer. The default value is '2' seconds.
DPD Type	Select **On Demand** or **Periodic**. If set to **On Demand**, DPD messages are sent on the basis of traffic patterns. For example, if a router has to send outbound traffic and the liveliness of the peer is questionable, the router sends a DPD message to query the status of the peer. If a router has no traffic to send, it never sends a DPD message. If set to **Periodic**, the router sends DPD messages at the interval specified by the IKE Keepalive value.

VPN Global Settings: IPSec

Edit global IPSec settings in this window.

How to Get to this Screen

- **Configure > Security > VPN > VPN Components > VPN Options > Edit > IPSec**.

Field Reference

Table 34-3 IPSec Global Settings

Element	Description
Authenticate and Generate new key after every	Check this box and specify the time interval at which the router should authenticate and generate a new key. If you do not specify a value, the router will authenticate and generate a new key every hour.
Generate new key after the current key encrypts a volume of	Check this box and specify the number of kilobytes that should be encrypted by the current key before the router authenticates and generates a new one. If you do not specify a value, the router will authenticate and generate a new key after the current key has encrypted 4,608,000 kilobytes.

VPN Global Settings: Easy VPN Server

Make global settings for Easy VPN server connections in this screen.

How to Get to this Screen

- **Configure > Security > VPN > VPN Components > VPN Options > Edit > Easy VPN Server**.

Field Reference

Table 34-4 VPN Global Settings: Easy VPN Server Fields

Element	Description
Common Pool	You can configure a common IP address pool for all clients to use. If a group does not have a specific pool, clients belonging to that group will be allocated an IP address from this common pool. Select a common pool—Select a pool name from this list. If no pools are configured, you click **Additional Tasks > Local Pools > Add**, and configure a pool in the displayed dialog. Then, return to this screen and select it.
Enable Syslog messages	Check **Enable Syslog messages** to enable Syslog messages for client connections. You can specify the scope of this option with the following options: • Enable Syslog messages for all client connections—Check this option to enable Syslog messages for all groups that connect to the Easy VPN server. • Enable Syslog messages for the following groups—Check this option to enable Syslog messages for the groups that you specify. Then, enter the group names in the box, separating one group name from another with a comma. A sample set of entries follows: `WGP-1, WGP-2, ACCTG, CSVC` The router must use Cisco IOS 12.4(4)T or later for this part of the screen to be displayed.

VPN Keys Encryption

VPN keys such as pre-shared keys, Easy VPN keys, and XAuth passwords can be encrypted using a strong symmetric AES cipher and a master key. See VPN Keys Encryption Reference for a description of the screens.

VPN Keys Encryption Reference

This section contains the following parts:

- VPN Key Encryption Settings

VPN Key Encryption Settings

The VPN Key Encryption Settings window appears if the Cisco IOS image on your router supports Type 6 encryption, also referred to as *VPN key encryption*. You can use this window to specify a master key to use when encrypting VPN keys, such as pre-shared keys, Easy VPN keys, and XAuth keys. When encrypted, these keys will not be readable by someone viewing the router's configuration file.

How to Get to this Screen

- **Configure > Security > VPN > VPN Components > VPN Keys Encryption > Edit**.

Field Reference

Table 34-5 VPN Key Encryption Settings

Element	Description
Enable VPN Keys Encryption	Check to enable encryption of these keys.
Current Master Key	This field contains asterisks (*) when a master key has been configured.
New Master Key	Enter a new master key in this field. Master keys must be at least 8 characters long and can be as long as 128 characters.
Confirm Master Key	Reenter the master key in this field for confirmation. If the values in this field and in the New Master Key field do not match, Cisco CP prompts you to reenter the key.

CHAPTER 35

VPN Troubleshooting

Cisco CP can troubleshoot VPN connections that you have configured. Cisco CP reports the success or failure of the connection tests, and when tests have failed, recommends actions that you can take to correct connection problems.

The following link provides information on VPN troubleshooting using the CLI.

http://www.cisco.com/en/US/docs/security/security_management/vms/router_mc/1.3.x/user/guide/U13_Rtrb.html

VPN Troubleshooting

This window appear when you are troubleshooting a site-to-site VPN, a GRE over IPSec tunnel, an Easy VPN remote connection, or an Easy VPN server connection.

Note VPN Troubleshooting will not troubleshoot more than two peers for site-to-site VPN, GRE over IPsec, or Easy VPN client connections.

Tunnel Details

This box provides the VPN tunnel details.

Interface

Interface to which the VPN tunnel is configured.

Peer

The IP address or host name of the devices at the other end of the VPN connection.

Summary

Click this button if you want to view the summarized troubleshooting information.

Details

Click this button if you want to view the detailed troubleshooting information.

Activity

This column displays the troubleshooting activities.

Status

Displays the status of each troubleshooting activity by the following icons and text alerts:


The connection is up.


The connection is down.


Test is successful.


Test failed.

Failure Reason(s)

This box provides the possible reason(s) for the VPN tunnel failure.

Recommended action(s)

This box provides a possible action/solution to rectify the problem.

Close Button

Click this button to close the window.

Test Specific Client Button

This button is enabled if you are testing connections for an Easy VPN server configured on the router. Click this button and specify the client to which you want to test connectivity.

This button is disabled in the following circumstances:

- The Basic testing is not done or has not completed successfully.
- The IOS image does not support the required debugging commands.
- The view used to launch Cisco CP does not have root privileges.

What Do You Want to Do?

If you want to:	Do this:
Troubleshoot the VPN connection.	Click **Start** button. When test is running, **Start** button label will change to **Stop**. You have option to abort the troubleshooting while test is in progress.
Save the test report.	Click **Save Report** button to save the test report in HTML format. This button is disabled when the test is in progress.

VPN Troubleshooting: Specify Easy VPN Client

This window allows you to specify the Easy VPN client which you want to debug.

IP Address

Enter IP address of Easy VPN client you want to debug.

Listen for request for X minutes

Enter the time duration for which Easy VPN Server has to listen to requests from Easy VPN client.

Continue Button

After selecting the traffic generation type you want, click this button to continue testing.

Close Button

Click this button to close the window.

VPN Troubleshooting: Generate Traffic

This window allows you to generate site-to-site VPN or Easy VPN traffic for debugging. You can allow Cisco CP to generate VPN traffic or you can generate VPN traffic yourself.

VPN traffic on this connection is defined as

This area lists current VPN traffic on the interface.

Action

This column denotes whether the type of traffic is allowed in the interface.

Source

Source IP address.

Destination

Destination IP address.

Service

This column lists the type of traffic on the interface.

Log

This column indicates whether logging is enabled for this traffic.

Attributes

Any additional attributes defined.

Have Cisco CP generate VPN Traffic

Select this option if you want Cisco CP to generate VPN traffic on the interface for debugging.

Note Cisco CP will not generate VPN traffic when the VPN tunnel traffic is from non-IP based Access Control List (ACL) or when the applied and current CLI View is not root view.

Enter the IP address of a host in the source network

Enter the host IP address in the source network.

Enter the IP address of a host in the destination network

Enter the host IP address in the destination network.

I will generate VPN traffic from the source network

Select this option if you want to generate VPN traffic from the source network.

Wait interval time

Enter the amount of time in seconds that the Easy VPN Server is to wait for you to generate source traffic. Be sure to give yourself enough time to switch to other systems to generate traffic.

Continue Button

After selecting the traffic generation type you want, click this button to continue testing.

Close Button

Click this button to close the window.

VPN Troubleshooting: Generate GRE Traffic

This screen appears if you are generating GRE over IPSec traffic.

Have Cisco CP generate VPN Traffic

Select this option if you want Cisco CP to generate VPN traffic on the interface for debugging.

Enter the remote tunnel IP address

Enter the IP address of the remote GRE tunnel. Do not use the address of the remote interface.

I will generate VPN traffic from the source network

Select this option if you want to generate VPN traffic from the source network.

Wait interval time

Enter the amount of time in seconds that the Easy VPN Server is to wait for you to generate source traffic. Be sure to give yourself enough time to switch to other systems to generate traffic.

Continue Button

After selecting the traffic generation type you want, click this button to continue testing.

Close Button

Click this button to close the window.

Cisco CP Warning: Cisco CP will enable router debugs...

This window appears when Cisco CP is ready to begin advanced troubleshooting. Advanced troubleshooting involves delivering debug commands to the router waiting for results to report, and then removing the debug commands so that router performance is not further affected.

This message is displayed because this process can take several minutes and may affect router performance.

CHAPTER 36

IP Security

IP Security (IPSec) is a framework of open standards that provides data confidentiality, data integrity, and data authentication between participating peers. IPSec provides these security services at the IP layer; it uses IKE to handle negotiation of protocols and algorithms based on local policy, and to generate the encryption and authentication keys to be used by IPSec.

Cisco CP lets you configure IPSec transform sets, rules, and policies.

Use the IPSec tree to go to the IPSec configuration windows that you want to use.

IPSec Policies

This window displays the IPSec policies configured on the router, and the crypto maps associated with each policy. IPSec policies are used to define VPN connections. To learn about the relationship between IPSec policies, crypto maps, and VPN connections, see More about VPN Connections and IPSec Policies.

Icon

If this icon appears next to the IPSec policy, it is read-only, and it cannot be edited. An IPSec policy may be read-only if it contains commands that Cisco CP does not support.

Name

The name of this IPSec policy.

Type

One of the following:

- ISAKMP—IKE will be used to establish the IPSec security associations for protecting the traffic specified by this crypto map entry. Cisco CP supports Internet Security Association and Key Management Protocol (ISAKMP) crypto maps.
- Manual—IKE will not be used to establish the IPSec security associations for protecting the traffic specified by this crypto map entry.

  Cisco CP does not support the creation of manual crypto maps. Cisco CP treats as read-only any manual crypto maps that have been created using the command-line interface (CLI).
- Dynamic—Specifies that this crypto map entry is to reference a preexisting dynamic crypto map. Dynamic crypto maps are policy templates used in processing negotiation requests from a peer IPSec device.

  Cisco CP does not support the creation of dynamic crypto maps. Cisco CP treats as ready only any dynamic crypto maps created using the CLI.

Crypto Maps in this IPSec policy

Name

The name of the IPSec policy of which the crypto map is a part.

Seq. No.

When an IPSec policy is used in a VPN connection, the combination of the sequence number and IPSec policy name uniquely identifies the connection.

Peers

This column lists the IP addresses or host names of the peer devices specified in the crypto map. Multiple peers are separated by commas.

Transform Set

This column lists the transform sets used in the crypto map.

Dynamic Crypto Maps Sets in this IPSec Policy

Dynamic Crypto Map Set Name

The name of this dynamic crypto map set. Names enable administrators to understand how the crypto map set is used.

Sequence Number

The sequence number for this dynamic crypto map set.

Type

Type is always Dynamic.

What Do You Want to Do?

If you want to:	Do this:
Add an IPSec policy to the configuration.	Click **Add**.
Edit an existing IPSec policy.	Select the policy, and click **Edit**.
Remove a crypto map entry from a policy.	Select the policy, and click **Edit**. In the window, select the crypto map you want to remove, and click **Delete**. Then, click **OK** to return to this window.
Remove an IPSec policy.	Select the policy, and click **Delete**.

Add or Edit IPSec Policy

Use this window to add or edit an IPSec policy.

Name

The name of this IPSec policy. This name can be any set of alphanumeric characters. It may be helpful to include the peer names in the policy name, or to include other information that will be meaningful to you.

Crypto Maps in this IPSec policy

This box lists the crypto maps in this IPSec policy. The list includes the name, the sequence number, and the transform set that makes up this crypto map. You can select a crypto map and edit it or delete it from the IPSec policy.

If you want to add a crypto map, click Add. If you want Cisco CP to guide you through the process, check **Use Add Wizard**, and then click **Add**.

Icon

If a crypto map is read-only, the read-only icon appears in this column. A crypto map may be read-only if it contains commands that Cisco CP does not support.

Dynamic Crypto Maps Sets in this IPSec Policy

This box lists the dynamic crypto map sets in this IPSec policy. Use the **Add** button to add an existing dynamic crypto map set to the policy. Use the **Delete** button to remove a selected dynamic crypto map set from the policy.

What Do You Want to Do?

If you want to:	Do this:
Add a crypto map to this policy.	Click **Add**, and create a crypto map in the Add crypto map panels. Or, check **Use Add Wizard**, and then click **Add**. **Note** The wizard allows you to add only one transform set to the crypto map. If you need multiple transform sets in the crypto map, do not use the wizard.
Edit a crypto map in this policy.	Select the crypto map, click **Edit**, and edit the crypto map in the Edit crypto map panels.
Remove a crypto map from this policy.	Select the crypto map, and click **Delete**.

Add or Edit Crypto Map: General

Change general crypto map parameters in this window. This window contains the following fields.

Name of IPSec Policy

A read-only field that contains the name of the policy in which this crypto map is used. This field does not appear if you are using the Crypto Map Wizard.

Description

Enter or edit a description of the crypto map in this field. This description appears in the VPN Connections list, and it can be helpful in distinguishing this crypto map from others in the same IPSec policy.

Sequence Number

A number that, along with the IPSec policy name, is used to identify a connection. Cisco CP generates a sequence number automatically. You can enter your own sequence number if you wish.

Security Association Lifetime

IPSec security associations use shared keys. These keys, and their security associations time out together. There are two lifetimes: a timed lifetime and a traffic-volume lifetime. The security association expires when the first of these lifetimes is reached.

You can use this field to specify a different security association lifetime for this crypto map than the lifetime that is specified globally. In the Kilobytes field, you can specify the lifetime in the number of kilobytes sent, up to a maximum of 4608000. In the HH:MM:SS fields, you can specify the lifetime in hours, minutes, and seconds. You can also specify both a timed and a traffic-volume lifetimes. If both are specified, the lifetime will expire when the first criterion has been satisfied.

Enable Perfect Forwarding Secrecy

When security keys are derived from previously generated keys, there is a security problem, because if one key is compromised, then the others can be compromised also. Perfect Forwarding Secrecy (PFS) guarantees that each key is derived independently. It thus ensures that if one key is compromised, no other keys will be. If you enable PFS, you can specify use of the Diffie-Hellman group1, group2, or group5 method.

Note If your router does not support group5, it will not appear in the list.

Enable Reverse Route Injection

Reverse Route Injection (RRI) is used to populate the routing table of an internal router running Open Shortest Path First (OSPF) protocol or Routing Information Protocol (RIP) for remote VPN clients or LAN-to-LAN sessions.

Reverse Route Injection dynamically adds static routes to the clients connected to the Easy VPN server.

Add or Edit Crypto Map: Peer Information

A crypto map includes the hostnames or IP addresses of the peers involved in the security association. This screen allows you to add and remove peers associated with this crypto map. Multiple peers provide the router with multiple routes for encrypted data.

If you want to:	Do this:
Add a peer to the Current List.	Enter the IP address or host name of the peer, and click **Add**.
Remove a peer from the Current List.	Select the peer, and click **Remove**.

Add or Edit Crypto Map: Transform Sets

Use this window to add and edit the transform set used in the crypto map. A crypto map includes the hostnames or IP addresses of the peers involved in the security association. Multiple peers provide the router with multiple routes for encrypted data. However, the devices at both ends of the VPN connection must use the same transform set.

Use the Crypto Map Wizard if it is sufficient for your router to offer a crypto map with one transform set.

Use **Add New Crypto Map...** with **Use Add Wizard** unchecked if you want to manually configure a crypto map with multiple transforms sets (up to six) to ensure that the router can offer one transform set that the peer it is negotiating with will accept. If you are already in the Crypto Map Wizard, exit the wizard, uncheck **Use Add Wizard**, and click **Add New Crypto Map...**.

If you manually configure a crypto map with multiple transforms sets, you can also order the transform sets. This will be the order that the router will use to negotiate which transform set to use.

Available Transform Sets

Configured transform sets available for use in crypto maps. In the Crypto Map Wizard, the available transform sets are in the **Select Transform Set** drop-down list.

If no transform sets have been configured on the router, only the default transform sets provided with Cisco CP are shown.

Note

- Not all routers support all transform sets (encryption types). Unsupported transform sets will not appear in the window.
- Not all IOS images support all the transform sets that Cisco CP supports. Transform sets unsupported by the IOS image will not appear in the window.
- If hardware encryption is turned on, only those transform sets supported by both hardware encryption and the IOS image will appear in the window.

Details of Selected Transform Set (Crypto Map Wizard Only)

Shows the name, encryption, authentication characteristics, and other parameters of the chosen crypto map.

If this icon appears next to the transform set, it is read-only, and it cannot be edited.

Selected Transform Sets In Order of Preference (Manual Configuration of Crypto Map Only)

The transform sets that have been chosen for this crypto map, in the order in which they will be used. During negotiations with a peer, the router will offer transform sets in the order given in this list. You can use the up and down arrow buttons to reorder the list.

What Do You Want to Do? (Crypto Map Wizard Only)

If you want to:	Do this:
Use the selected transform set for the crypto map.	Click **Next**.
Use another existing transform set.	Select it in the Select Transform Set list, and click **Next**.
Use a new transform set.	Click **Add**, and create the transform set in the Add Transform Set window. Then, return to this window, and click **Next**.
Edit the selected transform set.	Click **Edit**, and edit the transform set in the Edit Transform Set window.
Add more transform sets to this crypto map. You may wish to do this to ensure that the router can offer a transform set that the peer will agree to use.	Leave the crypto map wizard, uncheck **Use Add Wizard**, and click **Add Crypto Map**. The Transform Set tab allows you to add and order transform sets.

What Do You Want to Do? (Manual Configuration of Crypto Map Only)

If you want to:	Do this:
Add a transform set to the Selected Transform Sets box.	Select a transform set in the Available Transform Sets box, and click the right-arrow button.
Remove a transform set from the Selected Transform Sets box.	Select the transform set you want to remove, and click the left-arrow button.
Change the preference order of the selected transform sets.	Select a transform set, and click the up button or the down button.
Add a transform set to the Available Transform Sets list.	Click **Add**, and configure the transform set in the Add Transform Set window.
Edit a transform set in the Available Transform Sets list.	Click **Edit**, and configure the transform set in the Edit Transform Set window.

Add or Edit Crypto Map: Protecting Traffic

You can configure the crypto map to protect all traffic (Crypto Map Wizard only) or choose an IPSec rule to protect specified traffic.

Protect all traffic between the following subnets (Crypto Map Wizard Only)

Use this option to specify a single source subnet (a subnet on the LAN) whose traffic you want to encrypt, and one destination subnet supported by the peer that you specified in the Peers window. All traffic flowing between other source and destination subnets will be sent unencrypted.

Source

Enter the address of the subnet whose outgoing traffic you want to protect, and specify the subnet mask. You can either select a subnet mask from the list or type in a custom mask. The subnet number and mask must be entered in dotted decimal format. For more information, see IP Addresses and Subnet Masks.

All traffic from this source subnet that has a destination IP address on the destination subnet will be encrypted.

Destination

Enter the address of the destination subnet, and specify the mask for that subnet. You can either select a subnet mask from the list or type in a custom mask. The subnet number and mask must be entered in dotted decimal format.

All traffic going to the hosts in this subnet will be encrypted.

IPSec Rule (Create/Select an access-list for IPSec traffic)

You can add or change the IPSec rule used in this crypto map. Use this option if you need to specify multiple sources and destinations, and/or specific types of traffic to encrypt. An IPSec rule can consist of multiple entries, each specifying different traffic types and different sources and destinations. Any packets that do not match the criteria in the IPSec rule are sent unencrypted.

Note If you are adding an IPSec rule for a VPN connection that uses a tunnel interface, the rule must specify the same source and destination data as the tunnel configuration.

To add or change the IPSec rule for the crypto map, click the **...** button to the right of the IPSec rule field and choose one of the following:

- **Select an existing rule (ACL)**—If the rule you want to use has already been created, choose the rule, then click **OK**.
- **Create a new rule and select**—If the rule you need has not been created, create the rule, then click **OK**.
- **None**—If you want to clear a rule association. The IPSec rule field shows the name of the IPSec rule in use, but if you choose **None**, the field becomes blank.

Another way to add or change the IPSec rule for this crypto map is to enter the number of the IPSec rule directly in the IPSec rule field.

Note IPSec rules must be extended rules, not standard rules. If the number or name you enter identifies a standard rule, Cisco CP will display a warning message when you click OK.

Dynamic Crypto Map Sets

This window lists the dynamic crypto map sets configured on the router.

Add/Edit/Delete Buttons

Use these buttons to manage the crypto maps in the window. If you try to delete a crypto map set associated with an IPSec policy, Cisco CP prevents you from doing so. You must disassociate the crypto map from the policy before deleting it. You can do this in the IPSec Policies window.

Name

The name of the dynamic crypto map.

Type

Always Dynamic.

Add or Edit Dynamic Crypto Map Set

Add or edit a dynamic crypto map set in this window.

Name

If you are adding a dynamic crypto map, enter the name in this field. If you are editing a crypto map set, this field is disabled, and you cannot change the name.

Crypto maps in this IPSec Policy

This area lists the crypto maps used in this set. Use the **Add**, **Edit**, and **Delete** buttons to add, remove, or modify crypto maps in this list.

Associate Crypto Map with this IPSec Policy

Sequence Number

Enter a sequence number to identify this crypto map set. This sequence number cannot be in use by any other crypto map set.

Select the Dynamic Crypto Map Set

Select the dynamic crypto map set you want to add from this list.

Crypto Maps in this Dynamic Crypto Map Set

This area lists the names, sequence numbers, and peers in the dynamic crypto map set you selected.

IPSec Profiles

This window lists configured IPSec profiles on the router. IPSec profiles consist of one or more configured transform sets; the profiles are applied to mGRE tunnels to define how tunneled traffic is encrypted.

Name

The name of the IPSec profile.

Transform Set

The transform sets used in this profile.

Description

A description of the IPSec profile.

Add

Click to add a new IPSec profile.

Edit

Select an existing profile and click **Edit** to change the profile configuration.

Delete

Click to edit a selected IPSec profile. If the profile you are deleting is currently used in a DMVPN tunnel, you must configure the DMVPN tunnel to use a different IPSec profile.

Details of IPSec Profile

This area displays the configuration of the selected IPSec profile. For a description of the information displayed in this area see Add or Edit IPSec Profile.

Add or Edit IPSec Profile

Enter the information to create an IPSec profile in this dialog. An IPSec profile specifies the transform sets to be used, how the Security Association (SA) lifetime is to be determined, and other information.

Transform Set Columns

Use the two columns at the top of the dialog to specify the transform sets that you want to include in the profile. The left-hand column contains the transform sets configured on the router. To add a configured transform set to the profile, select it and click the >> button. If there are no transform sets in the left-hand column, or if you need a transform set that has not been created, click **Add** and create the transform set in the displayed dialog.

IKE Profile Association

If you want to associate an IKE profile with this IPSec profile, choose an existing profile from the list. If an IKE profile has already been associated, this field is read only.

Time Based IPSec SA Lifetime

Click **Time Based IPSec SA Lifetime** if you want a new SA to be established after a set period of time has elapsed. Enter the time period in the HH:MM:SS fields to the right.

Traffic Volume Based IPSec SA Lifetime

Click **Traffic Volume Based IPSec SA Lifetime** if you want a new SA to be established after a specified amount of traffic has passed through the IPSec tunnel. Enter the number of kilobytes that should pass through the tunnel before an existing SA is taken down and a new one is established.

IPSec SA Idle Time

Click IPSec SA Idle Time if you want a new SA to be established after the peer has been idle for a specified amount of time. Enter the idle time period in the HH:MM:SS fields to the right.

Perfect Forwarding Secrecy

Click **Perfect Forwarding Secrecy** if IPSec should ask for perfect forward secrecy (PFS) when requesting new security associations for this virtual template interface, or should require PFS in requests received from the peer. You can specify the following values:

- group1—The 768-bit Diffie-Hellman prime modulus group is used to encrypt the PFS request.
- group2—The 1024-bit Diffie-Hellman prime modulus group is used to encrypt the PFS request.
- group5—The 1536-bit Diffie-Hellman prime modulus group is used to encrypt the PFS request.

Add or Edit IPSec Profile and Add Dynamic Crypto Map

Use this window to add or to edit an IPSec profile, or to add a dynamic crypto map.

Name

Enter a name for this profile.

Available Transform Sets

This column lists the transform sets configured on this router. To add a transform set from this list to the Selected Transform Sets column, select a transform set and click the right arrow (>>) button.

If you need to configure a new transform set, click the **Transform Sets** node in the IPSec tree to go to the Transform Sets window. In that window, click **Add** to create a new transform set.

Selected Transform Sets

This column lists the transform sets that you are using in this profile. You can select multiple transform sets so that the router you are configuring and the router at the other end of the tunnel can negotiate which transform set to use.

Transform Set

This screen allows you to view transform sets, add new ones, and edit or remove existing transform sets. A transform set is a particular combination of security protocols and algorithms. During the IPSec security association negotiation, the peers agree to use a particular transform set for protecting a particular data flow.

You can create multiple transform sets and then specify one or more of them in a crypto map entry. The transform set defined in the crypto map entry will be used in the IPSec security association negotiation to protect the data flows specified by that crypto map entry's access list.

During IPSec security association negotiations with IKE, the peers search for a transform set that is the same at both peers. When that transform set is found, it is selected and applied to the protected traffic as part of both peers' IPSec security associations.

Name

Name given to the transform set.

ESP Encryption

Cisco CP recognizes the following ESP encryption types:

- ESP_DES—Encapsulating Security Payload (ESP), Data Encryption Standard (DES). DES supports 56-bit encryption.
- ESP_3DES—ESP, Triple DES. This is a stronger form of encryption than DES, supporting 168-bit encryption.
- ESP_AES_128—ESP, Advanced Encryption Standard (AES). Encryption with a 128-bit key. AES provides greater security than DES and is computationally more efficient than 3DES.
- ESP_AES_192—ESP, AES encryption with a 192-bit key.
- ESP_AES_256—ESP, AES encryption with a 256-bit key.
- ESP_NULL—Null encryption algorithm, but encryption transform used.
- ESP_SEAL—ESP with the 160-bit encryption key Software Encryption Algorithm (SEAL) encryption algorithm. SEAL (Software Encryption Algorithm) is an alternative algorithm to software-based Data Encryption Standard (DES), Triple DES (3DES), and Advanced Encryption Standard (AES). SEAL encryption uses a 160-bit encryption key and has a lower impact to the CPU when compared to other software-based algorithms.

ESP Integrity

Indicates the integrity algorithm being used. This column will contain a value when the transform set is configured to provide both data integrity and encryption. The column will contain one of the following values:

- ESP-MD5-HMAC—Message Digest 5, Hash-based Message Authentication Code (HMAC).
- ESP-SHA-HMAC—Security Hash Algorithm, HMAC.

AH Integrity

Indicates the integrity algorithm being used. This column will contain a value when the transform set is configured to provide data integrity but not encryption. The column will contain one of the following values:

- AH-MD5-HMAC—Message Digest 5.
- AH-SHA-HMAC—Security Hash Algorithm.

IP Compression

Indicates whether IP data compression is used.

Note If your router does not support IP compression, this box will be disabled.

Mode

This column contains one of the following values:

- Tunnel—Both the headers and data are encrypted. The mode used in VPN configurations.
- Transport—Only the data is encrypted. This mode is used when the encryption endpoints and the communication endpoints are the same.

Type

Either User Defined or Cisco CP Default.

What Do You Want to Do?

If you want to:	Do this:
Add a new transform set to the router's configuration.	Click Add, and create the transform set in the Add Transform Set window.
Edit an existing transform set.	Select the transform set, and click **Edit**. Then edit the transform set in the Edit Transform Set window. **Note** Cisco CP Default transform sets are read-only and cannot be edited.
Delete an existing transform set.	Select the transform set, and click **Delete**. **Note** Cisco CP Default transform sets are read-only and cannot be deleted.

Add or Edit Transform Set

Use this window to add or edit a transform set.

To obtain a description of the allowable transform combinations, and descriptions of the transforms, click **Allowable Transform Combinations**.

Note

- Not all routers support all transform sets (encryption types). Unsupported transform sets will not appear in the screen.
- Not all IOS images support all the transform sets that Cisco CP supports. Transform sets unsupported by the IOS image will not appear in the screen.
- If hardware encryption is turned on, only those transform sets supported by both hardware encryption and the IOS image will appear in the screen.
- Easy VPN servers only support tunnel mode. Transport mode is not supported by Easy VPN servers.
- Easy VPN Servers only support transform sets with ESP encryption. Easy VPN servers do not support the AH algorithm.
- Easy VPN Servers do not support ESP-SEAL encryption.

Name of this transform set

This can be any name that you want. The name does not have to match the name in the transform set that the peer uses, but it may be helpful to give corresponding transform sets the same name.

Data integrity and encryption (ESP)

Check this box if you want to provide Encapsulating Security Payload (ESP) data integrity and encryption.

Integrity Algorithm

Select one of the following:

- ESP_MD5_HMAC. Message Digest 5.
- ESP_SHA_HMAC. Security Hash Algorithm.

Encryption

Cisco CP recognizes the following ESP encryption types:

- ESP_DES. Encapsulating Security Payload (ESP), Data Encryption Standard (DES). DES supports 56-bit encryption.
- ESP_3DES. ESP, Triple DES. This is a stronger form of encryption than DES, supporting 168-bit encryption.
- ESP_AES_128. ESP, Advanced Encryption Standard (AES). Encryption with a 128-bit key. AES provides greater security than DES and is computationally more efficient than 3DES.
- ESP_AES_192. ESP, AES encryption with a 192-bit key.
- ESP_AES_256. ESP, AES encryption with a 256-bit key.
- ESP_SEAL—ESP with the 160-bit encryption key Software Encryption Algorithm (SEAL) encryption algorithm. SEAL (Software Encryption Algorithm) is an alternative algorithm to software-based Data Encryption Standard (DES), Triple DES (3DES), and Advanced Encryption Standard (AES). SEAL encryption uses a 160-bit encryption key and has a lower impact to the CPU when compared to other software-based algorithms.
- ESP_NULL. Null encryption algorithm, but encryption transform used.

Note The types of ESP encryption available depend on the router. Depending on the type of router you are configuring, one or more of these encryption types may not be available.

Data and address integrity without encryption (AH)

This check box and the fields below it appear if you click **Show Advanced**.

Check this box if you want the router to provide Authentication Header (AH) data and address integrity. The authentication header will not be encrypted.

Integrity Algorithm

Select one of the following:

- AH_MD5_HMAC—Message Digest 5.
- AH_SHA_HMAC—Security Hash Algorithm.

Mode

Select which parts of the traffic you want to encrypt:

- Transport. Encrypt data only—Transport mode is used when both endpoints support IPsec; this mode places the AH or ESP after the original IP header; thus, only the IP payload is encrypted. This method allows users to apply network services such as quality-of-service (QoS) controls to encrypted packets. Transport mode should be used only when the destination of the data is always the remote VPN peer.
- Tunnel. Encrypt data and IP header—Tunnel mode provides stronger protection than transport mode. Because the entire IP packet is encapsulated within AH or ESP, a new IP header is attached, and the entire datagram can be encrypted. Tunnel mode allows network devices such as a router to act as an IPsec proxy for multiple VPN users; tunnel mode should be used in those configurations.

IP Compression (COMP-LZS)

Check this box if you want to use data compression.

Note Not all routers support IP compression. If your router does not support IP compression, this box is disabled.

IPSec Rules

This window shows the IPSec rules configured for this router. IPSec rules define which traffic IPSec will encrypt. The top part of the window lists the access rules defined. The bottom part shows the access rule entries for the access rule selected in the rule list.

IPSec rules contain IP address and type-of-service information. Packets that match the criteria specified in the rule are encrypted. Packets that do not match the criteria are sent unencrypted.

Name/Num

The name or number of this rule.

Used By

Which crypto maps this rule is used in.

Type

IPSec rules must specify both source and destination and must be able to specify the type of traffic the packet contains. Therefore, IPSec rules are extended rules.

Description

A textual description of the rule, if available.

Action

Either **Permit** or **Deny**. **Permit** means that packets matching the criteria in this rules are protected by encryption. **Deny** means that matching packets are sent unencrypted. For more information see Meanings of the Permit and Deny Keywords.

Source

An IP address or keyword that specifies the source of the traffic. **Any** specifies that the source can be any IP address. An IP address in this column may appear alone, or it may be followed by a wildcard mask. If present, the wildcard mask specifies the portions of the IP address that the source IP address must match. For more information, see IP Addresses and Subnet Masks.

Destination

An IP address or keyword that specifies the destination of the traffic. **Any** specifies that the destination can be any IP address. An IP address in this column may appear alone, or it may be followed by a wildcard mask. If present, the wildcard mask specifies the portions of the IP address that the destination IP address must match.

Service

The type of traffic that the packet must contain.

What Do You Want to Do?

If you want to:	Do this:
See the access rule entries for a particular rule.	Select the rule in the rule list. The entries for that rule appear in the lower box.
Add an IPSec rule.	Click **Add**, and create the rule in the rule window displayed.
Delete an IPSec rule.	Select the rule in the rule list, and click **Delete**.
Delete a particular rule entry.	Select the rule in the rule list, and click **Edit**. Then, delete the entry in the rule window displayed.
Apply an IPSec rule to an interface.	Apply the rule in the interface configuration window.

CHAPTER 37

Internet Key Exchange

The help topics in this section describe the Internet Key Exchange (IKE) configuration screens.

Internet Key Exchange (IKE)

Internet Key Exchange (IKE) is a standard method for arranging for secure, authenticated communications. IKE establishes session keys (and associated cryptographic and networking configuration) between two hosts across the network.

Cisco CP lets you create IKE policies that will protect the identities of peers during authentication. Cisco CP also lets you create pre-shared keys that peers exchange.

IKE Policies

IKE negotiations must be protected; therefore, each IKE negotiation begins by each peer agreeing on a common (shared) IKE policy. This policy states which security parameters will be used to protect subsequent IKE negotiations. This window shows the IKE policies configured on the router, and allows you to add, edit, or remove an IKE policy from the router's configuration. If no IKE policies have been configured on the router, this window shows the default IKE policy.

After the two peers agree on a policy, the security parameters of the policy are identified by a security association established at each peer. These security associations apply to all subsequent IKE traffic during the negotiation.

The IKE policies in this list are available to all VPN connections.

Priority

An integer value that specifies the priority of this policy relative to the other configured IKE policies. Assign the lowest numbers to the IKE policies that you prefer that the router use. The router will offer those policies first during negotiations.

Encryption

The type of encryption that should be used to communicate this IKE policy.

Hash

The authentication algorithm for negotiation. There are two possible values:

- Secure Hash Algorithm (SHA)
- Message Digest 5 (MD5)

Authentication

The authentication method to be used.

- Pre-SHARE. Authentication will be performed using pre-shared keys.
- RSA_SIG. Authentication will be performed using digital signatures.

Type

Either SDM_DEFAULT or User Defined. SDM_DEFAULT policies cannot be edited.

Add or Edit IKE Policy

Add or edit an IKE policy in this window.

Note

- Not all routers support all encryption types. Unsupported types will not appear in the screen.
- Not all IOS images support all the encryption types that Cisco CP supports. Types unsupported by the IOS image will not appear in the screen.
- If hardware encryption is turned on, only those encryption types supported by both hardware encryption and the IOS image will appear in the screen.

Priority

An integer value that specifies the priority of this policy relative to the other configured IKE policies. Assign the lowest numbers to the IKE policies that you prefer that the router use. The router will offer those policies first during negotiations.

Encryption

The type of encryption that should be used to communicate this IKE policy. Cisco CP supports a variety of encryption types, listed in order of security. The more secure an encryption type, the more processing time it requires.

Note If your router does not support an encryption type, the type will not appear in the list.

Cisco CP supports the following types of encryption:

- Data Encryption Standard (DES)—This form of encryption supports 56-bit encryption.
- Triple Data Encryption Standard (3DES)—This is a stronger form of encryption than DES, supporting 168-bit encryption.
- AES-128—Advanced Encryption Standard (AES) encryption with a 128-bit key. AES provides greater security than DES and is computationally more efficient than triple DES.
- AES-192—Advanced Encryption Standard (AES) encryption with a 192-bit key.

- AES-256—Advanced Encryption Standard (AES) encryption with a 256-bit key.

Hash

The authentication algorithm to be used for the negotiation. There are two options:

- Secure Hash Algorithm (SHA)
- Message Digest 5 (MD5)

Authentication

The authentication method to be used.

- Pre-SHARE. Authentication will be performed using pre-shared keys.
- RSA_SIG. Authentication will be performed using digital signatures.

D-H Group

Diffie-Hellman (D-H) Group. Diffie-Hellman is a public-key cryptography protocol that allows two routers to establish a shared secret over an unsecure communications channel. The options are as follows:

- group1—768-bit D-H Group. D-H Group 1.
- group2—1024-bit D-H Group. D-H Group 2. This group provides more security than group 1, but requires more processing time.
- group5—1536-bit D-H Group. D-H Group 5. This group provides more security than group 2, but requires more processing time.

Note

- If your router does not support group5, it will not appear in the list.
- Easy VPN servers do not support D-H Group 1.

Lifetime

This is the lifetime of the security association, in hours, minutes and seconds. The default is one day, or 24:00:00.

IKE Pre-shared Keys

This window allows you to view, add, edit, and remove IKE pre-shared keys in the router's configuration. A pre-shared key is exchanged with a remote peer during IKE negotiation. Both peers must be configured with the same key.

Icon

If a pre-shared key is read-only, the read-only icon appears in this column. A pre-shared key will be marked as read-only if it is configured with the **no-xauth** CLI option

Peer IP/Name

An IP address or name of a peer with whom this key is shared. If an IP address is supplied, it can specify all peers in a network or subnetwork, or just an individual host. If a name is specified, then the key is shared by only the named peer.

Network Mask

The network mask specifies how much of the peer IP address is used for the network address and how much is used for the host address. A network mask of 255.255.255.255 indicates that the peer IP address is an address for a specific host. A network mask containing zeros in the least significant bytes indicates that the peer IP address is a network or subnet address. For example a network mask of 255.255.248.0 indicates that the first 22 bits of the address are used for the network address and that the last 10 bits are for the host part of the address.

Pre-Shared Key

The pre-shared key is not readable in Cisco CP windows. If you need to examine the pre shared key, go to **View->Running Config**. This will display the running configuration. The key is contained in the **crypto isakmp key** command.

Add or Edit Pre Shared Key

Use this window to add or edit a pre-shared key.

Key

This is an alphanumeric string that will be exchanged with the remote peer. The same key must be configured on the remote peer. You should make this key difficult to guess. Question marks (?) and spaces must not be used in the pre-shared key.

Reenter Key

Enter the same string that you entered in the Key field, for confirmation.

Peer

Select **Hostname** if you want the key to apply to a specific host. Select **IP Address** if you want to specify a network or subnetwork, or if you want to enter the IP address of a specific host because there is no DNS server to translate host names to IP addresses

Hostname

This field appears if you selected "**Hostname**" in the Peer field. Enter the peer's host name. There must be a DNS server on the network capable of resolving the host name to an IP address.

IP Address/Subnet Mask

These fields appear if you selected "IP Address" in the Peer field. Enter the IP address of a network or subnet in the IP Address field. The pre-shared key will apply to all peers in that network or subnet. For more information, refer to IP Addresses and Subnet Masks.

Enter a subnet mask if the IP address you entered is a subnet address, and not the address of a specific host.

User Authentication [Xauth]

Check this box if site-to-site VPN peers use XAuth to authenticate themselves. If Xauth authentication is enabled in VPN Global Settings, it is enabled for site-to-site peers as well as for Easy VPN connections.

IKE Profiles

IKE profiles, also called ISAKMP profiles, enable you to define a set of IKE parameters that you can associate with one or more IPSec tunnels. An IKE profile applies parameters to an incoming IPSec connection identified uniquely through its concept of match identity criteria. These criteria are based on the IKE identity that is presented by incoming IKE connections and includes IP address, fully qualified domain name (FQDN), and group (the virtual private network [VPN] remote client grouping).

For more information on ISAKMP profiles, and how they are configured using the Cisco IOS CLI, go to Cisco.com and follow this path:

Products and Services > Cisco IOS Software > Cisco IOS Security > Cisco IOS IPSec > Product Literature > White Papers > ISAKMP Profile Overview

IKE Profiles

The IKE Profiles area of the screen lists the configured IKE profiles and includes the profile name, the IPSec profile it is used by, and a description of the profile if one has been provided. If no IPSec profile uses the selected IKE profile, the value <none> appears in the Used By column.

When you create an IKE profile from this window, the profile is displayed in the list. When you use the Easy VPN server wizard to create a configuration, IKE profiles are created automatically, named by Cisco CP, and displayed in this list.

Details of IKE Profile

The details area of the screen lists the configuration values for the selected profile. You can use it to view details without clicking the Edit button and displaying an additional dialog. If you need to make changes, click Edit and make the changes you need in the displayed dialog. To learn more about the information shown in this area, click Add or Edit an IKE Profile.

Add or Edit an IKE Profile

Enter information and make settings in this dialog to create an IKE profile and associate it with a virtual tunnel interface.

Field Reference

Table 37-1 describes the fields in this screen.

Table 37-1 Add or Edit IKE Profile

Element	Description
IKE Profile Name	Enter a name for this IKE profile. If you are editing a profile, this field is enabled.
Match Identity Type	The IKE profile includes match criteria that allow the router to identify the incoming and outgoing connections to which the IKE connection parameters are to apply. Match criteria can currently be applied to VPN groups. Group is automatically chosen in the Match Identity Type field.
Add VPN groups to be associated with this IKE profile.	Build a list of groups that you want to be included in the match criteria. The groups you add are listed. • Add—Click **Add** to display a menu with the following options: – Add External Group Name—Choose **Add External Group Name** to add the name of a group that is not configured on the router, and enter the name in the dialog displayed. – Select From Local Groups—Choose **Select From Local Groups** to add the name of a group that is configured on the router. In the displayed dialog, check the box next to the group that you want to add. If all the local groups are used in other IKE profiles, Cisco CP informs you that all groups have been selected. • Delete—Choose a group and click **Delete** to remove it from the list.
Virtual Tunnel Interface	Choose the virtual tunnel interface to which you want to associate this IKE profile from the Virtual Tunnel Interface list. If you need to create a virtual tunnel interface, click **Add** and create the interface in the displayed dialog.

Table 37-1 Add or Edit IKE Profile (continued)

Element	Description
Mode Configuration	Choose one of the following options to specify how the Easy VPN server is to handle mode configuration requests: • Respond—Choose **Respond** in the Mode Configuration field if the Easy VPN server is to respond to mode configuration requests. • Initiate—Choose **Initiate** if the Easy VPN server is to initiate mode configuration requests. • Both—Choose **Both** if the Easy VPN server is to both initiate and respond to mode configuration requests.
Group Policy Lookup Authorization Policy	Specify an authorization policy that controls access to group policy information on the AAA server. • default—Choose **default** if you want to grant access to group policy lookup information. • Policyname—To specify a policy, choose an existing policy in the list. • Add—Click **Add** to create a policy in the displayed dialog.
User Authentication Policy	Check **User Authentication Policy** if you want to allow XAuth logins, or if you want to specify a user authentication policy to use for XAuth logins. Choose one of the following options: • default—Choose **default** if you want to allow XAuth logins. • Policyname—If policies have been configured on the router, they are displayed in this list and you can select a policy to use. Click **Add** to create a policy in the displayed dialog and use it in this IKE policy.

Table 37-1 Add or Edit IKE Profile (continued)

Element	Description
Dead Peer Discovery	Click **Dead Peer Discovery** to enable the router to send dead peer detection (DPD) messages to Easy VPN Remote clients. If a client does not respond to DPD messages, the connection with it is dropped. • Keepalive Interval—Specify the number of seconds between DPD messages in the Keepalive Interval field. The range is from 10 to 3600 seconds. • Retry Interval—Specify the number of seconds between retries if DPD messages fail in the Retry Interval field. The range is from 2 to 60 seconds. Dead peer discovery helps manage connections without administrator intervention, but it generates additional packets that both peers must process in order to maintain the connection.
Download user attributes from RADIUS server based on PKI certificate fields.	Check this option if you want the Easy VPN server to download user-specific attributes from the RADIUS server and push them to the client during mode configuration. The Easy VPN server obtains the username from the client's digital certificate. This option is displayed under the following conditions: • The router runs a Cisco IOS 12.4(4)T or later image. • You choose digital certificate authentication in the IKE policy configuration. • You choose RADIUS or RADIUS and Local group authorization.
Description	You can add a description of the IKE profile that you are adding or editing.

CHAPTER 38

Certificate Authority Server

You can configure a Cisco IOS router to serve as a Certificate Authority (CA) server. A CA server handles certificate enrollment requests from clients, and can issue and revoke digital certificates.

To create, back up, restore, or edit a CA server, go to **Configure > Security > Public Key Infrastructure > Certificate Authority > Overview**.

To manage certificates on an existing CA server, go to **Configure > Security > Public Key Infrastructure > Certificate Authority > Manage Certificates**.

To monitor a CA server, go to **Monitor > VPN Status > CA Server**.

Create CA Server

This window allows you to launch a wizard for creating a Certificate Authority (CA) server, or a wizard for restoring a CA server. Only one CA server can be set up on a Cisco IOS router.

The CA server should be used to issue certificates to hosts on the private network so that they can use the certificates to authenticate themselves to other

Prerequisite Tasks

If Cisco CP finds that there are configuration tasks that should be performed before you begin configuring the CA server, it alerts you to them in this box. A link is provided next to the alert text so that you can go to that part of Cisco CP

and complete the configuration. If Cisco CP does not discover missing configurations, this box does not appear. Possible prerequisite tasks are described in Prerequisite Tasks for PKI Configurations.

Create Certificate Authority (CA) Server

Click this button to create a CA server on the router. Because only one CA server can be configured on the router, this button is disabled if a CA server is already configured.

Note The CA server you configure using Cisco CP allows you to grant and revoke certificates. Although the router does store the serial numbers and other identifying information about the certificates that it grants, it does not store the certificates themselves. The CA server should be configured with a URL to a Registration Authority (RA) server that can store certificates that the CA server grants.

Restore Certificate Authority (CA) Server

If a CA server already operates on the router, you can restore the CA server configuration, and the information. If no CA server is configured on the router, this option is disabled.

Prerequisite Tasks for PKI Configurations

Before you begin a certificate enrollment or CA server configuration, it may be necessary for you to complete supporting configuration tasks first. Cisco CP reviews the running configuration before allowing you to begin, alerts you to configurations you must complete, and provides links that take you to the areas of Cisco CP that allow you to complete these configurations.

Cisco CP may generate alerts about the following configuration tasks:

- SSH credentials not verified—Cisco CP requires you to provide your SSH credentials before beginning.
- NTP not configured—The router must have accurate time for certificate enrollment to work. Identifying a Network Time Protocol server from which your router can obtain accurate time provides a time source that is not

affected if the router needs to be rebooted. If your organization does not have an NTP server, you may want to use a publicly available server, such as the server described at the following URL:

http://www.pool.ntp.org/

- DNS not configured—Specifying DNS servers helps ensure that the router is able to contact the certificate server. DNS configuration is required to contact the CA server and any other server related to certificate enrollment such as OCSP servers or CRL repositories if those servers are entered as names and not as IP addresses.
- Domain and/or Hostname not configured—It is recommended that you configure a domain and hostname before beginning enrollment.

CA Server Wizard: Welcome

The Certificate Authority (CA) server wizard guides you through the configuration of a CA server. Be sure to have the following information before you begin:

- General information about the CA server—The name that you intend to give the server, the certificate issuer name that you want to use, and the username and password that enrollees will be required to enter when sending an enrollment request to the server.
- More detailed information about the server—Whether the server will operate in Registration Authority (RA) mode or Certificate Authority (CA) mode, the level of information about each certificate that the server will store, whether the server should grant certificates automatically, and the lifetimes of the certificates granted, and open enrollment requests.
- Supporting information—Links to the RA server that will store the certificates and to the Certificate Revocation List Distribution Point (CDP) server.

CA Server Wizard: Certificate Authority Information

Enter basic information about the CA server that you are configuring in this window.

CA Server Name

Provide a name to identify the server in the CA Server Name field. This could be the host name of the router, or another name that you enter.

Grant

Choose **Manual** if you want to grant certificates manually. Choose **Auto** if you want the server to grant certificates automatically. Auto, used mostly for debug purposes, is not recommended since it will issue certificates to any requester without requiring enrollment information.

Caution Do not set **Grant** to Auto if your router is connected to the Internet. **Grant** should be set to Auto only for internal purposes such as when executing debugging procedures.

CDP URL

Enter the URL to a Certificate Revocation List Distribution Point (CDP) server in the CDP URL field. The URL must be an HTTP URL. A sample URL follows:

```
http://172.18.108.26/cisco1cdp.cisco1.crl
```

The Certificate Revocation List (CRL) is the list of revoked certificates. Devices needing to check the validity of another device's certificate will fetch the CRL from the CA server. Since many devices may attempt to fetch the CRL, offloading it to a remote device, preferably an HTTP server, will reduce the performance impact on the Cisco IOS router hosting the CA server. If the checking device cannot connect to the CDP, as a backup it will use SCEP to fetch the CRL from the CA server.

Issuer Name Attributes

Common Name (cn)

Enter the common name that you want to use for the certificate. This might be the CA server name, the router hostname or another name you choose.

Organizational Unit (ou)

Enter the Organizational Unit, or department name to use for this certificate. For example, IT support, or Engineering might be organizational units.

Organization (o)

Enter the organization or company name.

State (st)

Enter the state or province in which the organization is located.

Country (c)

Enter the country in which the organization is located.

Email (e)

Enter the email address to be included in the router certificate.

Advanced Options

Click this button to enter advanced options for the CA server.

Advanced Options

The Advanced Options screen allows you to change default values for server settings and to specify the URL for the database that is to contain the certificate information.

Database

Configure the database level, the database URL, and database format in this section of the dialog.

Database Level

Choose the type of data that will be stored in the certificate enrollment database:

- **minimal—**Enough information is stored to continue issuing new certificates without conflict. This is the default.
- **names—**In addition to the information given by the minimal option, this includes the serial number and subject name of each certificate.

- **complete—**In addition to the information given by the minimal and names options, each issued certificate is written to the database.

Database URL

Enter the location to which the CA server will write certificate enrollment data. If no location is given, certificate enrollment data will be written to flash memory by default.

For example, to write certificate enrollment data to a tftp server, enter tftp://mytftp. To reset the database URL to flash memory, enter nvram.

Database Archive

Choose **pem** to create the archive in pem format, or **pkcs12** to create the archive in pkcs12 format.

Database Username

Enter a username for the database archive in the Database Username field. The username and password will be used to authenticate the server to the database.

Database Password and Confirm Password

Enter a password in the Database Password field, and reenter it in the Confirm Password field.

Lifetimes

Set the lifetime, or time before expiration, of items associated with the CA server. To set the lifetime for a specific item, choose it from the Lifetime drop-down list and enter a value in the Lifetime field.

You can set lifetimes for the following items:

- **Certificate**—Certificates issued by the CA server. Lifetime is entered in days, in the range 1–1825. If no value is entered, a certificate expires after one year. If a new value is entered, it affects certificates created only after that value is in effect.
- **CRL**—The Certificate Revocation List for certificates issued by the CA server. Lifetime is entered in hours, in the range 1–336. If no value is entered, a CRL expires after 168 hours (one week).

- **Enrollment-Request**—Open certificate requests existing in the enrollment database, but not including requests received through SCEP. Lifetime is entered in hours, in the range 1–1000. If no value is entered, an open enrollment request expires after 168 hours (one week).

CA Server Wizard: RSA Keys

The CA server uses public and private RSA keys to encrypt data and to sign certificates. Cisco CP automatically generates a new key pair and gives it the name of the CA server. You can change the key modulus and type, and you can make the key exportable. You must enter a pass phrase to use when restoring the CA server.

Label

This field is read-only. Cisco CP uses the name of the CA server as the name of the key pair.

Modulus

Enter the key modulus value. If you want a modulus value between 512 and 1024 enter an integer value that is a multiple of 64. If you want a value higher than 1024, you can enter 1536 or 2048. If you enter a value greater than 512, key generation may take a minute or longer.

The modulus determines the size of the key. The larger the modulus, the more secure the key, but keys with large modulus take longer to generate, and encryption/decryption operations take longer with larger keys.

Type

By default, Cisco CP creates a general purpose key pair that is used for both encryption and signature. If you want Cisco CP to generate separate key pairs for encrypting and signing documents, choose **Usage Keys.** Cisco CP will generate usage keys for encryption and signature.

Key is exportable

Check **Key is exportable** if you want the CA server key to be exportable.

Passphrase and Confirm Passphrase

In the Passphrase field, enter a passphrase to use when restoring the CA server from backup. Reenter the same passphrase in the Confirm Passphrase field.

Open Firewall

The Open Firewall window appears when a firewall configuration must be modified in order to allow communication between the CDP server and the CA server. Select the interface, and check the **Modify** box to allow Cisco CP to modify the firewall to allow this traffic. Click **Details** to view the ACE that would be added to the firewall.

CA Server Wizard: Summary

The Summary window displays the information that you entered in the wizard screens so that you can review the information before sending it to the router. A sample summary display follows:

```
------------------------------------------------------------
CA Server Configuration
------------------------------------------------------------
CA Server Name :CASvr-a
Grant:Manual
CDP URL:http://192.27.108.92/snrs.com
Common Name (cn):CS1841
Organization Unit (ou):IT Support
Organization (o):Acme Enterprises
State (st):CA
Country (c):US

------------------------------------------------------------
Advanced CA Server Configuration
------------------------------------------------------------
Database URL:nvram:
Database Archive:pem
Database Username:bjones
Database Password:*********

------------------------------------------------------------
RSA Keys:
------------------------------------------------------------
```

```
CA Server will automatically generate RSA key pair with following
defaults:-
Modulus:1024
Type of Key:General Purpose
Exportable Key:No
Passphrase configured:******


------------------------------------------------------------
Firewall Pass-through ACEs for Interface(s):
------------------------------------------------------------

FastEthernet0/0
    permit tcp host 192.27.108.92 eq www host 192.27.108.91 gt 1024
```

The summary display contains four sections, the CA Server Configuration section, the CA Server Advanced Configuration section, the RSA Keys section, and the Firewall Pass-through section. The name of this CA server is CAsvr-a. Certificates will be manually granted. Certificate information will be stored in nvram, in PEM format. Cisco CP will generate a general-purpose key pair with the default modulus 1024. The key will not be exportable. an ACE will be configured to allow traffic to between the router and the CDP host with the IP address 192.27.108.92.

Manage CA Server

You can start and stop the CA server from this window, grant and reject certificate requests, and revoke certificates. If you need to change the CA server configuration, you can uninstall the server from this window and return to the Create CA Server window to create the server configuration that you need.

Name

Displays the name of the server. The name of the server was created when the server was created.

Status Icon

If the CA server is running, the word **Running** and a green icon is displayed. If the CA server is not running, the word **Stopped** and a red icon is displayed.

Start Server

The Start Server button is displayed if the server is stopped. Click **Start Server** to start the CA server.

Stop Server

The Stop Server button is displayed if the server the server is running, click **Stop Server** if you need to stop the CA server.

Backup Server

Click **Backup Server** to backup the server configuration information onto the PC. Enter the backup location in the displayed dialog.

Uninstall Server

Click to uninstall the CA server from your Cisco IOS router. All of the CA server configuration and data will be removed. If you backed up the CA server before uninstalling it, you can restore its data only after you create a new CA server. See Create CA Server.

Details of CA Server

The Details of CA Server table provides a snapshot of the CA Server configuration. The following table shows sample information.

Item Name	Item Value
CA Certificate Lifetime	1095 days
CDP URL	http://192.168.7.5
CRL Lifetime	168 hours
Certificate Lifetime	365 days
Database Level	minimal
Database URL	nvram:
Enrollment Request Lifetime	168 hours
Grant	manual

Item Name	Item Value
Issuer Name	CN=CertSvr
Mode	Certificate Authority
Name	CertSvr

See CA Server Wizard: Certificate Authority Information and Advanced Options for descriptions of these items.

Backup CA Server

You can back up the files that contain the information for the CA server to your PC. The Backup CA Server window lists the files that will be backed up. The listed files must be present in the router NVRAM for the backup to be successful.

Click **Browse** and specify a folder on the PC to which the CA server files should be backed up.

Manage CA Server Restore Window

If you have backed up and uninstalled a CA server, you can restore the server configuration to the router by clicking the **Restore CA Server** button. You must be able to provide the CA server name, complete database URL, and the backup passphrase that was used during initial configuration. When you restore the CA server, you are given the opportunity to change configuration settings.

Restore CA Server

If you have backed up the configuration for a CA server that was uninstalled, you can restore it by providing the information about it in the Restore CA Server window. You can edit settings for the server by clicking **Edit CA server settings before restoration**. You must provide the name, file format, URL to the database, and passphrase in order to back up the server or edit server settings.

CA Server Name

Enter the name of the CA server that you backed up.

File Format

Choose the file format that was specified in server configuration, either PEM or PKCS12.

Complete URL

Enter the router database URL that was provided when the CA server was configured. This is the location to which the CA server writes certificate enrollment data. Two sample URLs follow:

```
nvram:/mycs_06.p12
tftp://192.168.3.2/mycs_06.pem
```

Passphrase

Enter the passphrase that was entered when the CA server was configured.

Copy CA Server Files from PC

Check the **Copy CA Server Files from PC checkbox** if you want to copy the server information that you backed up to the PC to router nvram.

Edit CA Server settings before restoration

Click **Edit CA Server settings before restoration** if you want to change CA server configuration settings before restoring the server. See CA Server Wizard: Certificate Authority Information and CA Server Wizard: RSA Keys for information about the settings that you can change.

Edit CA Server Settings: General Tab

Edit general CA server configuration settings in this window. You cannot change the name of the CA server. For information on the settings that you can change, see CA Server Wizard: Certificate Authority Information.

Edit CA Server Settings: Advanced Tab

You can change any of the advanced CA server settings in this window. For information on these settings, see Advanced Options.

Manage CA Server: CA Server Not Configured

This window appears when you click **Manage CA Server** but no CA server is configured. Click **Create CA Server** and complete the wizard to configure a CA server on your router.

Manage Certificates

Clicking **Configure > Security > VPN > Public Key Infrastructure > Certificate Authority > Manage Certificates** displays the Pending Requests tab and the Revoked Certificates tab. To go to the help topics for these tabs, click the following links:

- Pending Requests
- Revoked Certificates

Pending Requests

This window displays a list of certificate enrollment requests received by the CA server from clients. The upper part of the window contains CA server information and controls. For information on stopping, starting, and uninstalling the CA server, see Manage CA Server.

You can choose a certificate enrollment request in the list, then choose to issue (accept), reject, or delete it. The actions available depend on the status of the chosen certificate enrollment request.

Select All

Click **Select All** to select all outstanding certificate requests. When all certificate requests are selected, clicking **Grant** grants all requests. Clicking **Reject** when all certificate requests are selected rejects all the requests.

Grant

Click **Grant** to issue the certificate to the requesting client.

Note The CA server windows do not show the IDs of the certificates that are granted. In case it is ever necessary to revoke a certificate, you should obtain the certificate ID from the administrator of the client that the certificate was issued for. The client administrator can determine the certificate ID by entering the Cisco IOS command sh crypto pki cert**.**

Delete

Click **Delete** to remove the certificate enrollment request from the database.

Reject

Click **Reject** to deny the certificate enrollment request.

Refresh

Click **Refresh** to update the certificate enrollment requests list with the latest changes.

Certificate Enrollment Requests Area

The certificate enrollment requests area has the following columns:

Request ID—A unique number assigned to the certificate enrollment request.

Status—The current status of the certificate enrollment request. The status can be Pending (no decision), Granted (issued certificate), Rejected (denied request).

Fingerprint—A unique digital client identifier.

Subject Name—The subject name in the enrollment request.

A sample enrollment request follows:

Request ID	State	Fingerprint	Subject Name
1	pending	serialNumber=FTX0850Z0GT+ hostname=c1841.snrsprp.com	B398385E6BB6604E9E98B8FDBBB5E8BA

Revoke Certificate

Click **Revoke Certificate** to display a dialog that allows you to enter the ID of the certificate that you want to revoke.

Note The certificate ID does not always match the request ID shown in the CA server windows. It may be necessary to obtain the ID of the certificate to be revoked from the administrator of the client for which the certificate was granted. See Pending Requests for information on how the client administrator can determine the certificate ID.

Revoked Certificates

This window displays a list of issued and revoked certificates. Only issued certificates can be revoked. The upper part of the window contains CA server information and controls. For information on stopping, starting, and uninstalling the CA server, see Manage CA Server.

The list of certificates has the following columns:

- **Certificate Serial Number**—A unique number assigned to the certificate. This number is displayed in hexadecimal format. For example, the decimal serial number 1 is displayed as 0x01.
- **Revocation Date**—The time and date that the certificate was revoked. If a certificate was revoked at 41 minutes and 20 seconds after midnight on February 6, 2007, the revocation date is displayed as 00:41:20 UTC Feb 6 2007.

Revoke Certificate

Click **Revoke Certificate** to display a dialog that allows you to enter the ID of the certificate that you want to revoke.

Note The certificate ID does not always match the request ID shown in the CA server windows. It may be necessary to obtain the ID of the certificate to be revoked from the administrator of the client for which the certificate was granted. See Pending Requests for information on how the client administrator can determine the certificate ID.

Revoke Certificate

You can revoke certificates that have been granted by this CA server in this window.

Certificate ID

Enter the ID of the certificate that you are revoking.

Note The certificate ID does not always match the request ID shown in the CA server windows. It may be necessary to obtain the ID of the certificate to be revoked from the administrator of the client for which the certificate was granted. See Pending Requests for information on how the client administrator can determine the certificate ID.

CHAPTER 39

Public Key Infrastructure

The Public Key Infrastructure (PKI) windows enable you to generate enrollment requests and RSA keys, and manage keys and certificates. You can use the Simple Certificate Enrollment Process (SCEP) to create an enrollment request and an RSA key pair and receive certificates online, or create an enrollment request that you can submit to a Certificate Authority (CA) server offline.

If you want to use Secure Device Provisioning (SDP) to enroll for certificates, see Secure Device Provisioning.

Certificate Wizards

This window allows you to select the type of enrollment you are performing. It also alerts you to configuration tasks that you must perform before beginning enrollment, or tasks that Cisco recommends you perform before enrolling. Completing these tasks before beginning the enrollment process helps eliminate problems that may occur.

Select the enrollment method Cisco CP uses to generate the enrollment request.

Prerequisite Tasks

If Cisco CP finds that there are configuration tasks that should be performed before you begin the enrollment process, it alerts you to them in this box. A link is provided next to the alert text so that you can go to that part of Cisco CP and complete the configuration. If Cisco CP does not discover missing configurations, this box does not appear. Possible prerequisite tasks are described in Prerequisite Tasks for PKI Configurations.

Simple Certificate Enrollment Protocol (SCEP)

Click this button if you can establish a direct connection between your router and a Certificate Authority (CA) server. You must have the server's enrollment URL in order to do this. The wizard will do the following:

- Gather information from you to configure a trustpoint and deliver it to the router.
- Initiate an enrollment with the CA server you specified in the trustpoint.
- If the CA server is available, display the CA server's fingerprint for your acceptance.
- If you accept the CA server fingerprint , complete the enrollment.

Cut and Paste/Import from PC

Click this button if your router cannot establish a direct connection to the CA server or if you want to generate an enrollment request and send it to the CA at another time. After generation, the enrollment request can be submitted to a CA at another time. Cut-and-Paste enrollment requires you to invoke the Digital Certificates wizard to generate a request, and then to reinvoke it when you have obtained the certificates for the CA server and for the router.

Note Cisco CP supports only base-64-encoded PKCS#10-type cut and paste enrollment. Cisco CP does not support importing PEM and PKCS#12 type certificate enrollments.

Launch the selected task button

Click to begin the wizard for the type of enrollment that you selected. If Cisco CP has detected a required task that must be performed before enrollment can begin, this button is disabled. Once the task is completed, the button is enabled.

Welcome to the SCEP Wizard

This screen indicates that you are using the SCEP wizard. If you do not want to use the Simple Certificate Enrollment Process, click **Cancel** to leave this wizard.

After the wizard completes and the commands are delivered to the router, Cisco CP attempts to contact the CA server. If the CA server is contacted, Cisco CP displays a message window with the server's digital certificate.

Certificate Authority (CA) Information

Provide information to identify the CA server in this window. Also specify a challenge password that will be sent along with the request.

Note The information you enter in this screen is used to generate a trustpoint. The trustpoint is generated with a default revocation check method of CRL. If you are editing an existing trustpoint with the SCEP wizard, and a revocation method different from CRL, such as OCSP, already exists under the trustpoint, Cisco CP will not modify it. If you need to change the revocation method, go to Router Certificates window, select the trustpoint you configured, and click the **Check Revocation** button.

CA server nickname

The CA server nickname is an identifier for the trustpoint you are configuring. Enter a name that will help you identify one trustpoint from another.

Enrollment URL

If you are completing an SCEP enrollment, you must enter the enrollment URL for the CA server in this field. For example,

```
http://CAuthority/enrollment
```

The URL must begin with the characters http://. Be sure there is connectivity between the router and the CA server before beginning the enrollment process.

This field does not appear if you are completing a cut-and-paste enrollment.

Challenge Password and Confirm Challenge Password

A challenge Password can be sent to the CA for you to use if you ever need to revoke the certificate. It is recommended that you do so, as some CA servers do not issue certificates if the challenge Password is blank. If you want to use a

challenge Password, enter that password and then reenter it in the confirm field. The challenge Password will be sent along with the enrollment request. For security purposes, the challenge password is encrypted in the router configuration file, so you should record the password and save it in a location you will remember.

This password is also referred to as a challenge password.

Advanced Options Button

Advanced options allow you to provide more information to enable the router to contact the CA server.

Advanced Options

Use this window to provide more information to enable the router to contact the CA server.

HTTP Proxy and HTTP Port

If the enrollment request will be sent through a proxy server, enter the proxy server IP address, and the port number to use for proxy requests in these fields.

Certificate Subject Name Attributes

Specify the optional information that you want to be included in the certificate. Any information that you specify be included in the certificate request will be placed in the certificate, and be viewable by any party to whom the router sends the certificate.

Include router's fully qualified Domain Name (FQDN) in the certificate.

It is recommended that the router's fully qualified domain name be included in the certificate. Check this box if you want Cisco CP to include the router's fully qualified domain name in the certificate request.

Note If the Cisco IOS image running on the router does not support this feature, this box is disabled.

FQDN

If you enabled this field, enter the routers FQDN in this field. An example of an FQDN is

`sjrtr.mycompany.net`

Include router's IP Address

Check if you want to include a valid IP address configured on your router in the certificate request. If you check this box, you can manually enter an IP address, or you can select the interface whose IP address you want to be used.

IP Address

Click if you want to enter an IP address, and enter an IP address configured on the router in the field that appears. Enter an IP address that has been configured on the router or an address that has been assigned to the router.

Interface

Select a router interface whose IP address you want to be included in the certificate request.

Include router's serial number

Check this box if you want the serial number of the router included in the certificate.

Other Subject Attributes

The information you enter in this window will be placed in the enrollment request. CAs use the X.500 standard to store and maintain information for digital certificates. All fields are optional, but it is recommended that you enter as much information as possible.

Common Name (cn)

Enter the common name to be included in this certificate. This would be the name used to search for the certificate in the X.500 directory.

Organizational Unit (ou)

Enter the Organizational Unit, or department name to use for this certificate. For example, Development, or Engineering might be organizational units

Organization (o)

Enter the organization or company name. This is the X.500 organizational name.

State (st)

Enter the state or province in which the router or the organization is located.

Country (c)

Enter the country in which the router or the organization is located.

Email (e)

Enter the email address to be included in the router certificate.

Note If the Cisco IOS image running on the router does not support this attribute, this field is disabled.

RSA Keys

You must include an RSA public key in the enrollment request. Once the certificate has been granted, the public key will be included in the certificate so that peers can use it to encrypt data sent to the router. The private key is kept on the router and used to decrypt the data sent by peers, and also used to digitally sign transactions when negotiating with peers.

Generate new key pair(s)

Click this button if you want to generate a new key to use in the certificate. When you generate a key pair, you must specify the modulus to determine the size of the key. This new key appears in the RSA Keys window when the wizard is completed.

Modulus

Enter the key modulus value. If you want a modulus value between 512 and 1024 enter an integer value that is a multiple of 64. If you want a value higher than 1024, you can enter 1536 or 2048. If you enter a value greater than 512, key generation may take a minute or longer.

The modulus determines the size of the key. The larger the modulus, the more secure the key, but keys with large modulus take longer to generate, and encryption/decryption operations take longer with larger keys.

Generate separate key pairs for encryption and signature

By default, Cisco CP creates a general purpose key pair that is used for both encryption and signature. If you want Cisco CP to generate separate key pairs for encrypting and signing documents, check this box. Cisco CP will generate usage keys for encryption and signature.

Use existing RSA key pair

Click this button if you want to use an existing key pair, and select the key from the drop-down list.

Save to USB Token

Check the **Save keys and certificates to secure USB token** check box if you want to save the RSA keys and certificates to a USB token connected to your router. This check box appears only if a USB token is connected to your router.

Choose the USB token from the **USB token** drop-down menu. Enter the PIN needed to log in to the chosen USB token in **PIN**.

After you choose a USB token and enter its PIN, click **Login** to log in to the USB token.

Summary

This window summarizes the information that you provided. The information that you provided is used to configure a trustpoint on the router and begin the enrollment process. If you enabled **Preview commands before delivering to router** in the Preferences dialog, you will be able to preview the CLI that is delivered to the router.

If you are performing an SCEP enrollment

After the commands are delivered to the router, Cisco CP attempts to contact the CA server. If the CA server is contacted, Cisco CP displays a message window with the server's digital certificate.

If you are performing a cut-and-paste enrollment

After the commands are delivered to the router, Cisco CP generates an enrollment request and displays it in another window. You must save this enrollment request and present it to the CA server administrator in order to obtain the CA server's certificate, and the certificate for the router. The enrollment request is in Base64 encoded PKCS#10 format.

After you obtain the certificates from the CA server, you must restart the Cut and Paste wizard, and select **Continue an unfinished enrollment** to import the certificates to your router.

Enrollment Status

This window informs you of the status of the enrollment process. If errors are encountered during the process, Cisco CP displays the information it has about the error.

When status has been reported, click **Finish**.

Cut and Paste Wizard Welcome

The Cut and Paste wizard lets you generate an enrollment request and save it to your PC so that you can send it to the Certificate Authority offline. Because you cannot complete the enrollment in a single session, this wizard completes when you generate the trustpoint and the enrollment request and save it to your PC.

After you have submitted the enrollment request to the CA server manually, and received the CA server certificate and the certificate for your router, you must start the Cut and Paste wizard again to complete the enrollment and import the certificates to the router.

Enrollment Task

Specify whether you are beginning a new enrollment or you are resuming an enrollment with an enrollment request that you saved to the PC.

Begin New Enrollment

Click **Begin new enrollment** to generate a trustpoint, an RSA key pair and an enrollment request that you can save to your PC and send to the CA server. The wizard completes after you save the enrollment request. To complete the enrollment after you have receive the CA server certificate and the certificate for your router, re-enter the Cut and Paste wizard and select **Continue with an unfinished enrollment**.

Continue with an unfinished enrollment

Click this button to resume an enrollment process. You can import certificates you have received from the CA server, and you can generate a new enrollment request for a trustpoint if you need to.

Enrollment Request

This window displays the base-64-encoded PKCS#10-type enrollment request that the router has generated. Save the enrollment request to the PC. Then, send it to the CA to obtain your certificate.

Save

Browse for the directory on the PC that you want to save the enrollment request text file in, enter a name for the file, and click **Save**.

Continue with Unfinished Enrollment

If you are continuing with an unfinished enrollment you need to select the trustpoint associated with the unfinished enrollment, and then specify the part of the enrollment process you need to complete. If you are importing a CA server certificate or a router certificate, the certificate must be available on your PC.

Select CA server nickname (trustpoint)

Select the trustpoint associated with the enrollment you are completing.

Import CA and router certificate(s)

Choose this option if you want to import both the CA server's certificate and the router's certificate in the same session. Both certificates must be available on the PC.

This option is disabled if the CA certificate has already been imported.

Import CA certificate

Choose this option to import a CA server certificate that you have saved on your PC. After you import the certificate, Cisco CP will display the certificate's digital fingerprint. You can then verify the certificate and accept or reject it.

This option is disabled if the CA certificate has already been imported.

Import router certificate(s)

Choose this option to import a certificate for your router saved on your PC. After you import the router certificate, Cisco CP will report on the status of the enrollment process.

Note You must import the CA server's certificate before you import the router's certificate.

Generate enrollment request

Choose this option if you need to generate an enrollment request for the selected trustpoint. The router will generate an enrollment request that you can save to the PC and send to the CA.

Cisco CP generates a base-64 encoded PKCS#10 enrollment request.

Import CA certificate

If you have the CA server certificate on your hard disk, you can browse for it and import it to your router in this window. You can also copy and paste the certificate text into the text area of this window.

Browse Button

Click to locate the certificate file on the PC.

Import Router Certificate(s)

If you have one or more certificates for your router granted by the CA on your hard disk, you can browse for it and import it to your router.

Import more certificates

If you generated separate RSA key pairs for encryption and signature, you receive two certificates for the router. Use this button when you have more than one router certificate to import.

Remove certificate

Click the tab for the certificate you need to remove and click **Remove** certificate.

Browse

Browse to locate the certificate and import it to the router.

Digital Certificates

This window allows you to view information about the digital certificates configured on the router.

Trustpoints

This area displays summary information for the trustpoints configured on the router and allows you to view details about the trustpoints, edit trustpoints, and determine if a trustpoint has been revoked.

Details Button

The Trustpoints list only displays the name, enrollment URL, and enrollment type for a trustpoint. Click to view all the information for the selected trustpoint.

Edit Button

A trustpoint can be edited if it is an SCEP trustpoint, and if the CA server's certificate and the router's certificate have not both been successfully imported. If the trustpoint is not an SCEP trustpoint, or if both the CA server and router certificate associated with an SCEP trustpoint have been delivered, this button is disabled.

Delete Button

Click to delete the selected trustpoint. Deleting a trustpoint destroys all certificates received from the associated certificate authority.

Check Revocation Button

Click to check whether the selected certificate has been revoked. Cisco CP displays a dialog in which you select the method to use to check for revocation. See Revocation Check and Revocation Check, CRL Only for more information.

Name	Trustpoint name.

CA Server	The name or IP address of the CA server.
Enrollment Type	One of the following: • SCEP—Simple Certificate Enrollment Protocol. The enrollment was accomplished by connecting directly to the CA server • Cut and Paste—Enrollment request was imported from PC. • TFTP—Enrollment request was made using a TFTP server.

Certificate chain for trustpoint *name*

This area shows details about the certificates associated with the selected trustpoint.

Details Button

Click to view the selected certificate.

Refresh Button

Click to refresh the Certificate chain area when you select a different trustpoint in the Trustpoints list.

Type	One of the following: • RA KeyEncipher Certificate—Rivest Adelman encryption certificate • RA Signature Certificate—Rivest Adelman signature certificate. • CA Certificate—The certificate of the CA organization. • Certificate—The certificate of the router.
Usage	One of the following: • General Purpose—A general purpose certificate that the router uses to authenticate itself to remote peers. • Signature—CA certificates are signature certificates.
Serial Number	The serial number of the certificate
Issuer	The name of the CA that issued the certificate.

Status	One of the following: • Available—The certificate is available for use. • Pending—The certificate has bee applied for, but is not available for use.
Expires (Days)	The number of days the certificate can be used before it expires.
Expiry Date	The date on which the certificate expires.

Trustpoint Information

The Trustpoints list in the Router Certificates window displays the key information about each trustpoint on the router. This window displays all the information provided to create the trustpoint.

Certificate Details

This window displays trustpoint details that are not displayed in the Certificates window.

Revocation Check

Specify how the router is to check whether a certificate has been revoked in this window.

Revocation Check

Configure how the router is to check for revocations, and order them by preference. The router can use multiple methods.

Use/Method/Move Up/Move Down

Check the methods that you want to use, and use the **Move Up** and **Move Down** buttons to place the methods in the order you want to use them.

- OCSP—Contact an Online Certificate Status Protocol server to determine the status of a certificate.
- CRL—Certificate revocation is checked using a certificate revocation list.

- None—Do not perform a revocation check.

CRL Query URL

Enabled when CRL is selected. Enter the URL where the certificate revocation list is located. Enter the URL only if the certificate supports X.500 DN.

OCSP URL

Enabled when OCSP is selected. Enter the URL of the OCSP server that you want to contact.

Revocation Check, CRL Only

Specify how the router is to check whether a certificate has been revoked in this window.

Verification

One of the following:

- None—Check the Certificate Revocation List (CRL) distribution point embedded in the certificate.
- Best Effort—Download the CRL from the CRL server if it is available. If it is not available, the certificate will be accepted.
- Optional—Check the CRL only if it has already been downloaded to the cache as a result of manual loading.

CRL Query URL

Enter the URL where the certificate revocation list is located. Enter the URL only if the certificate supports X.500 DN.

RSA Keys Window

RSA keys provide an electronic encryption and authentication system that uses an algorithm developed by Ron Rivest, Adi Shamir, and Leonard Adelman. The RSA system is the most commonly used encryption and authentication algorithm, and is included as a part of Cisco IOS. To use the RSA system, a network host

generates a pair of keys. One is called the *public key*, and the other is called the *private key*. The Public key is given to anyone who wants to send encrypted data to the host. The Private key is never shared. When a remote hosts wants to send data, it encrypts it with the public key shared by the local host. The local host decrypts sent data using the private key.

RSA keys configured on your router

Name	The key name. Key names are automatically assigned by Cisco CP. The key "HTTPS_SS_CERT_KEYPAIR" and "HTTPS_SS_CERT_KEYPAIR.server" will be shown as Read-Only. Similarly, any key that is locked/encrypted on the router will be displayed with icons that indicate their status.
Usage	Either General Purpose or Usage. General purpose keys are used to encrypt data, and to sign the certificate. If separate keys are configured to encrypt data and to sign certificates, these keys are labelled Usage keys.
Exportable	If this column contains a checkmark the key can be exported to another router if it becomes necessary for that router to assume the role of the local router.

Key Data

Click to view a selected RSA key.

Save Key to PC Button

Click to save the data of the selected key to your PC.

Generate RSA Key Pair

Use this window to generate a new RSA key pair.

Label

Enter the label of the key in this field.

Modulus

Enter the key modulus value. If you want a modulus value between 512 and 1024 enter an integer value that is a multiple of 64. If you want a value higher than 1024, you can enter 1536 or 2048. If you enter a value greater than 512, key generation may take a minute or longer.

The larger the modulus size, the more secure the key is. However keys with larger modulus sizes take longer to generate and longer to process when exchanged.

Type

Select the type of key to generate, **General Purpose**, or **Usage**. General purpose keys are used for both encryption and signing of certificates. If you generate Usage keys, one set of keys will be used for encryption, and a separate set will be used for certificate signing.

Key is exportable check box

Check if you want the key to be exportable. An exportable key pair can be sent to a remote router if it is necessary for that router to take over the functions of the local router.

Save to USB Token

Check the **Save keys to secure USB token** check box if you want to save the RSA keys to a USB token connected to your router. This check box appears only if a USB token is connected to your router.

Choose the USB token from the **USB token** drop-down menu. Enter the PIN needed to log in to the chosen USB token in **PIN**.

After you choose a USB token and enter its PIN, click **Login** to log in to the USB token.

USB Token Credentials

This window appears when you add or delete credentials, such as an RSA key pair or digital certificates, that have been saved on a USB token. For the deletion to take place, you must provide the USB token name and PIN.

Choose the USB token from the **USB token** drop-down menu. Enter the PIN needed to log in to the chosen USB token in **PIN**.

USB Tokens

This window allows you to configure USB token logins. This window also displays a list of configured USB token logins. When a USB token is connected to your Cisco router, Cisco CP uses the matching login to log in to the token.

Add

Click **Add** to add a new USB token login.

Edit

Click **Edit** to edit an existing USB token login. Specify the login to edit by choosing it in the list.

Delete

Click **Delete** to delete an existing USB token login. Specify the login to delete by choosing it in the list.

Token Name

Displays the name used to log in to the USB token.

User PIN

Displays the PIN used to log in to the USB token.

Maximum PIN Retries

Displays the maximum number of times Cisco CP will attempt to log in to the USB token with the given PIN. If Cisco CP is unsuccessful after trying for the number specified, it will stop trying to log in to the USB token.

Removal Timeout

Displays the maximum number of seconds that Cisco CP will continue to use Internet Key Exchange (IKE) credentials obtained from the USB token after the token is removed from the router.

If Removal Timeout is empty, the default timeout is used. The default timeout is triggered when a new attempt to access the IKE credentials is made.

Secondary Config File

Displays the configuration file that Cisco CP attempts to find on the USB token. The configuration file can be a CCCD file or a .cfg file.

CCCD refers to a boot configuration file. On USB tokens, a CCCD file is loaded using TMS software.

Add or Edit USB Token

This window allows you to add or edit USB token logins.

Token Name

If you are adding a USB token login, enter the USB token name. The name you enter must match the name of the token that you want to log in to.

A token name is set by the manufacturer. For example, USB tokens manufactured by Aladdin Knowledge Systems are named eToken.

You can also use the name "usbtoken*x*", where *x* is the number of the USB port to which the USB token is connected. For example, a USB token connected to USB port 0 is named usbtoken0.

If you are editing a USB token login, the Token Name field cannot be changed.

Current PIN

If you are adding a USB token login, or if you are editing a USB token login that has no PIN, the Current PIN field displays <None>. If you are editing a USB token login which has a PIN, the Current PIN field displays ******.

Enter New PIN

Enter a new PIN for the USB token. The new PIN must be at least 4 digits long and must match the name of the token you want to log in to. If you are editing a USB token login, the current PIN will be replaced by the new PIN.

Reenter New PIN

Reenter the new PIN to confirm it.

Maximum PIN Retries

Choose the maximum number of times Cisco CP will attempt to log in to the USB token with the given PIN. If Cisco CP is unsuccessful after trying for the number specified, it will stop trying to log in to the USB token.

Removal Timeout

Enter the maximum number of seconds that Cisco CP will continue to use Internet Key Exchange (IKE) credentials obtained from the USB token after the token is removed from the router. The number of seconds must be in the range 0 to 480.

If you do not enter a number, the default timeout is used. The default timeout is triggered when a new attempt to access the IKE credentials is made.

Secondary Config File

Specify a configuration file that exists on the USB token. The file can be a partial or complete configuration file. The file extension must be .cfg.

If Cisco CP can log in to the USB token, it will merge the specified configuration file with the router's running configuration.

Open Firewall

This screen is displayed when Cisco CP detects firewall(s) on interfaces that would block return traffic that the router needs to receive. Two situations in which it might appear are when a firewall will block DNS traffic or PKI traffic and prevent the router from receiving this traffic from the servers. Cisco CP can modify these firewalls so that the servers can communicate with the router.

Modify Firewall

This area lists the exit interfaces and ACL names, and allows you to select which firewalls that you want Cisco CP to modify. Select the firewalls that you want Cisco CP to modify in the Action column. Cisco CP will modify them to allow SCEP or DNS traffic from the server to the router.

Note the following for SCEP traffic:

- Cisco CP will not modify firewall for CRL/OCSP servers if these are not explicitly configured on the router. To permit communication with CRL/OCSP servers, obtain the correct information from the CA server administrator and modify the firewalls using the Edit Firewall Policy/ACL window.
- Cisco CP assumes that the traffic sent from the CA server to the router will enter through the same interfaces through which traffic from the router to the CA server was sent. If you think that the return traffic from CA server will enter the router through a different interface than the one Cisco CP lists, you need to open the firewall using the Edit Firewall Policy/ACL window. This may occur if asymmetric routing is used, whereby traffic from the router to the CA server exits the router through one interface and return traffic enters the router through a different interface.
- Cisco CP determines the exit interfaces of the router the moment the passthrough ACE is added. If a dynamic routing protocol is used to learn routes to the CA server and if a route changes—the exit interface changes for SCEP traffic destined for the CA server—you must explicitly add a passthrough ACE for those interfaces using the Edit Firewall Policy/ACL window.
- Cisco CP adds passthrough ACEs for SCEP traffic. It does not add passthrough ACEs for revocation traffic such as CRL traffic and OCSP traffic. You must explicitly add passthrough ACEs for this traffic using the Edit Firewall Policy/ACL window.

Details Button

Click this button to view the access control entry that Cisco CP would add to the firewall if you allow the modification.

Open Firewall Details

This window displays the access control entry (ACE) that Cisco CP would add to a firewall to enable various types of traffic to reach the router. This entry is not added unless you check **Modify** in the Open Firewall window and complete the wizard.

CHAPTER 40

Content Filtering

This section explains URL filtering. It contains the following sections:

- Cisco Configuration Professional Content Filtering
- Creating a Content Filter
- Editing Content Filters
- Configuring Content Filtering Components
- Additional Information

Cisco Configuration Professional Content Filtering

Cisco Configuration Professional (Cisco CP) allows you to configure the Subscription-based Cisco IOS Content Filtering feature.

The Subscription-based Cisco IOS Content Filtering feature interacts with the Trend Micro URL filtering service so that HTTP requests can be allowed, blocked, or logged based on a content filtering policy. The content filtering policy specifies how to handle items such as web categories, reputations (or security ratings), trusted domains, untrusted domains, and keywords. URLs are cached on the router, so that subsequent requests for the same URL do not require a lookup request, thus improving performance.

Cisco CP also allows you to perform content filtering using Secure Computing and Websense content filter servers, and local URL filtering using URLs and keywords stored on the router.

Creating a Content Filter

Cisco CP provides a wizard to use to create content filters. This wizard allows you to do the following:

- Register with and use a Trend Micro URL filtering server.
- Use Websense or Secure Computing content filter servers.
- Associate the content filter with an ingoing and an outgoing interface.
- Create a list of keywords that, when matched, cause a URL request to be blocked.
- Create a black and white list that specifies which URLs to allow, and which URLs to block.
- Specify which content to block, based on content category and reputation.

To create a content filter, complete the following steps:

Step 1 In the navigation pane, click **Configure > Security > Web Filter Configuration**. The Create Content Filter tab is displayed.

Step 2 Click the **Configure Category based Filtering** radio button, or the **Configure Web Sense or Secure Computing** radio button.

Step 3 Download the certificate and activate the license, if you clicked the **Configure Category based Filtering** radio button.

Step 4 Click **Launch the selected task**.

If you clicked the **Configure Category based Filtering** radio button and did not download the digital certificate and activate the license, the Prerequisite Task dialog box appears. Click **Yes** to continue or **No** to cancel. It is possible to configure category-based filtering without downloading the certificate and activating the license.

Step 5 In each screen of the wizard, enter the information for which you are prompted. When you have finished entering information in a screen, click **Next** to go to the next screen.

Step 6 When the Summary screen is displayed, review the displayed information. To change something, click the **Back** button to return to the appropriate screen.

Step 7 When you have made all necessary changes, return to the Summary screen, and click **Finish**. The Deliver Configuration To Router is displayed.

Step 8 In the Deliver Configuration To Router screen, review the Cisco IOS CLI commands that you are delivering to the router.

- Click **Cancel**, to avoid sending the configuration to the router. The configuration is not delivered, and the wizard closes.
- Click **Deliver** to send the configuration to the router. The configuration is sent to the router, and saved in the running configuration.

Creating Content Filter Reference

This section describes the following help topics:

- Content Filter Wizard: Create Content Filter Tab
- Content Filter Wizard: Basic Content Filter Configuration Wizard
- Content Filter Wizard: Basic Content Filter Interface Configuration
- Content Filter Wizard and Edit Screen: Category Selection
- Content Filter Wizard and Edit Screen: Reputation Selection
- Content Filter Wizard: Content Filter Server Configuration
- Content Filter Wizard: Content Filter Web Requests
- Content Filter Wizard: Summary

Content Filter Wizard: Create Content Filter Tab

Use this screen to review the use case scenario, and launch the Content Filtering policy wizard.

How to get to this screen

In the navigation panel, click **Configure > Security > Web Filter Configuration > Create Content Filter**.

Related Links

- Cisco Configuration Professional Content Filtering
- Creating a Content Filter

Field Reference

Table 40-1 URL Filter Tab

Element	Description
Use Case Scenario	Use Case Scenario diagram illustrates the network configuration for which you can create a URL filtering policy.
Configure Category based Filtering	To perform category based filtering on the URLs, click the **Configure Category based Filtering** radio button.

Table 40-1 URL Filter Tab (continued)

Element	Description
Download Certificate	Click the Download Certificate link to download the certificate. An SSL certificate is essential for communication between the router and the Content Filter vendor. If you already have the certificate, the link is not displayed. It is possible to configure category based filtering without downloading the certificate.
Activate License	To activate the license for Content Filtering, enter the Product Authorization Key (PAK) and register the router. If you already registered the router, the link is not displayed. It is possible to configure category based filtering without activating the license.
Launch the content filter	To begin using the wizard to configure a URL-filtering policy, click **Launch the content filter**.
How do I	To learn how to create a configuration that the wizard does not help you create, choose a topic in the How do I list, and click **Go**.

Content Filter Wizard: Basic Content Filter Configuration Wizard

In this screen, review the content filtering policies that you will use the wizard to create.

How to get to this screen

In the navigation panel, click **Configure > Security > Web Filter Configuration > Create Content Filter > Launch the selected task**.

Related Links

- Cisco Configuration Professional Content Filtering
- Creating a Content Filter

Content Filter Wizard: Basic Content Filter Interface Configuration

In this screen, specify the traffic to which this content filter is to apply by identifying the inside router interface and outside router interface.

How to get to this screen

In the navigation panel, click **Configure > Security > Web Filter Configuration > Create Content Filter > Launch the selected task**. Click **Next** in each screen, until this screen appears.

Related Links

- Cisco Configuration Professional Content Filtering
- Creating a Content Filter

Field Reference

Table 40-2 Source and Destination Interfaces

Element	Description
Interface	Displays the router interfaces. For example, the column may contain the values Gigabit Ethernet 0/0, or Serial 0/1.
Outside (Untrusted)	Check the box in this column next to the interface name, to designate an interface as an outside interface through which content might arrive.
Inside (Trusted)	Check the box in this column next to the interface name, to designate an interface as an inside interface.

Content Filter Wizard: Content Filter Server Configuration

Use this screen to enter URLs and URL keywords to block and URLs to allow.

How to get to this screen

In the navigation panel, click **Configure > Security > Web Filter Configuration > Create Content Filter > Launch the selected task**. Click **Next** in each screen, until this screen appears.

Related Links

- Cisco Configuration Professional Content Filtering
- Creating a Content Filter

Field Reference

Table 40-3 Server Information

Element	Description
Enter the keywords in the URL that must be blocked	To specify keywords that should result in the URL being blocked, enter the keywords in this field, separated by spaces. For example, you might enter the following keywords: `sex, gambling, firearms`
Enter the URLs that must be blocked	To specify URLs to block, enter the URLs in this field, separated by spaces. For example you might enter the following URLs: `www.sex.com, www.gambling.com`
Enter the URLs that must be allowed	To specify URLs to allow, enter the URLs in this field, separated by spaces. For example you might enter the following URLs: `www.science.edu, www.state.gov`

Content Filter Wizard and Edit Screen: Category Selection

In this screen, choose the content categories that you want to deny access to. If you are using the Content Filter wizard, you can choose a default category profile that preselects categories to be denied.

How to get to this screen

- In the navigation panel, click **Configure > Security > Web Filter Configuration > Create Content Filter > Launch the selected task**. Click **Next** in each screen, until this screen appears.
- In the navigation panel, click **Configure > Security > Web Filter Configuration > Edit Content Filter > Category Filtering**.

Related Links

- Content Filter Wizard and Edit Screen: Reputation Selection
- Cisco Configuration Professional Content Filtering
- Creating a Content Filter
- Using the Edit Content Filter Screens

Field Reference

Table 40-4 Category and Action

Element	Description
Default Category	This field is displayed if you are using the wizard. To use one of the Cisco CP default profiles, click **Default Category**. When chosen, a default profile preselects certain categories of content to deny.
Custom Category	This field is displayed if you are using the wizard. To choose all categories that should be denied, without having any category preselected by a default profile, click **Custom Category**.
Cisco CP Default Profiles	This field is displayed if you are using the wizard. If you chose Default Category, choose the Cisco CP default profile that you want to use. When you choose a profile, check marks are placed next to the categories denied by that profile. For example, choosing the Education profile automatically places check marks next to the Adult-Mature-Content, Gambling, Marijuana, and Nudity categories, among others.

Table 40-4 Category and Action (continued)

Element	Description
Category	This column lists the content categories defined on the Content Filtering server. Activist-Groups, Brokerage-Trading, and Chat-Instant-Messaging are examples of the content categories you can choose to block.
Description	This column contains a description of the category, if one is available.
Check	To specify that a content category is to be denied, check the box in the row of the category. If you choose a default profile, some boxes are already checked. For example, if you choose Small Office/Branch Office, the Chat-Instant-Messaging, Social-Networking and other categories are preselected. You can uncheck any boxes that are pre-checked by the profile.

Content Filter Wizard and Edit Screen: Reputation Selection

In this screen, choose content to be denied based on reputation.

How to get to this screen

In the navigation panel, click **Configure > Security > Web Filter Configuration > Create Content Filter > Launch the selected task**. Click **Next** in each screen, until this screen appears.

In the navigation panel, click **Configure > Security > Web Filter Configuration > Edit Content Filter > Security Categories.**

Related Links

- Content Filter Wizard and Edit Screen: Category Selection
- Cisco Configuration Professional Content Filtering
- Creating a Content Filter
- Using the Edit Content Filter Screens

Field Reference

Table 40-5 Reputation Selection

Element	Description
Reputation	This column lists the reputation category defined on the Category server. For example, there are reputation categories such as ADWARE, DIALER, and DISEASE-VECTOR.
Description	This column contains a description of the reputation category.
Check	To deny content from websites with the reputation listed in the Category column, check the box in the same row.

Content Filter Wizard: Choose Websense or Secure Computing

If you had clicked the "Configure Web Sense or Secure Computing" radio button in Step 2, this page appears next.

In this screen, specify the type of server that you have on the network, and enter the IP address of the server.

How to get to this screen

In the navigation panel, click **Configure > Security > Web Filter Configuration > Create Content Filter > Launch the selected task**. Click **Next** in each screen, until this screen appears.

Related Links

- Creating a Content Filter, page 40-2
- Content Filter Wizard: Content Filter Web Requests, page 40-11

Table 40-6 Server Type and Server Address

Element	Description
Content Filter Server Type	Choose the server type from the drop-down list.
IP Address or Hostname	Enter the IP address or hostname of the server.

Content Filter Wizard: Content Filter Web Requests

In this screen, specify the action that the router is to take when the content filter server is unreachable.

How to get to this screen

In the navigation panel, click **Configure > Security > Web Filter Configuration > Create Content Filter > Launch the selected task**. Click **Next** in each screen, until this screen appears.

Related Links

- Cisco Configuration Professional Content Filtering
- Creating a Content Filter

Field Reference

Table 40-7 Content Filter Web Requests

Element	Description
Allow web requests	To permit web requests to be sent when the server is unreachable, click **Allow web requests**.
Deny web requests	To prevent web requests from being sent when the server is unreachable, click **Deny web requests**. By default, web requests are denied when the server is unreachable.

Content Filter Wizard: Summary

In this screen, review the configuration that you are going to send to the router.

How to get to this screen

In the navigation panel, click **Configure > Security > Web Filter Configuration > Create Content Filter > Launch the selected task**. Click **Next** in each screen, until this screen appears.

Related Links

- Cisco Configuration Professional Content Filtering
- Creating a Content Filter

Example Configuration Summary

```
Blocked Keyword :    sex: drugs; gambling
Allowed URL :    www.science.edu, www.state.gov
Blocked URL :    www.sex.com www.drugs.com www.guns.com

Category Server Filtering
Trend Server : stage-trps.trendmicro.com
DNS Configuration:
    Primary DNS: 12.12.12.12
    Secondary DNS: Not set
Swift Registration-Download Certification

Reputations:
    DIALER
    DISEASE-VECTOR
     PASSWORD-CRACKING-APPLICATIONS
    PHISHING
    POTENTIALLY-MALICIOUS-SOFTWARE
Deny Web Request
```

Editing Content Filters

You can edit a content filter that you created with the wizard, and create policies that filter by keyword, content category, reputation (security rating) of the domain name, and also identify the content filtering servers that the router will use.

This section of the document contains the following parts:

- Using the Edit Content Filter Screens
- Creating a Keyword Blocking Policy
- Creating a Black and White Listing
- Registering With a Category Server
- Filtering By URL Category
- Filtering By URL Reputation
- Configuring the Router To Use Websense or Secure Computing Servers
- Configuring Content Filtering Components

Using the Edit Content Filter Screens

This help topic tells you how to use the controls that are available in all Edit Content Filter screens. In the Edit Content Filter screens, you can display information about content filtering servers and content filtering policies and dialog boxes that enable you to create policies and edit server information. To go from one screen to another, click one of the buttons on the left side, such as Keyword Blocking, Black and White List, or Category Server Registration.

Content Filtering Policy Components

A content filtering policy can consist of these components:

- Keywords that, when found in a URL, should cause the URL to be blocked.
- A black and white listing. Black and white listings contain URLs, and the action that is to be applied to each. The action is either permit or deny.
- Category server registration information. This information consists of the IP address and transmission settings for a Trend Micro server.
- The URL categories that should be blocked.
- The URL reputations that should be blocked.
- The information for Websense or Secure Computing URL filtering servers.

How to Get to this Screen

In the navigation panel, click **Configure > Security > Web Filter Configuration > Edit Content Filter**.

Related Links

- Policy Name
- Associate With Zone Pair
- Edit Global Settings
- URL Filtering: Keyword Blocking
- Black and White List
- Category Server Registration
- Content Filter Wizard and Edit Screen: Category Selection
- Content Filter Wizard and Edit Screen: Reputation Selection
- Server Filtering

Field Reference

Table 40-8 Edit Content Filter Fields and Buttons

Element	Description
Content Filter Policy Name	Use this field to choose a content filtering policy to view. The details of the policy are displayed in the window area of the screen. If there are no content filtering policies, you can click **Action** > **Add** to create one.
Action	Use this button to create a new policy, clone an existing policy, or delete a policy. • To create a new policy, click **Action** > **Add**. Then, provide a policy name in the displayed dialog. To configure the policy, choose the name you entered, and then configure the policy using the Keyword Blocking, Black and White listing, and other buttons on this screen. • To clone an existing policy, choose the policy, and then click **Action** > **Clone**. In the Policy Name dialog, provide a name for the new policy. Then use the Keyword Blocking, Black and White listing, and other buttons on this screen to make further modifications to the policy. • To delete a policy, choose the policy in the Content Filter Policy Name list, and click **Action** > **Delete**.

Table 40-8 Edit Content Filter Fields and Buttons

Element	Description
Associate	To associate a content filtering policy with a configured zone pair, choose the policy, click Associate and choose the zone pair to which you want to associate the policy. See Associate With Zone Pair for more information.
Global Settings	To make settings that determine how the router is to handle URL responses when it cannot contact the server, buffer requests and responses, and other settings, click **Global Settings**. See Edit Global Settings for more information.
Apply Changes	To send the changed settings in the Productivity Categories list or the Security Categories list to the router, click **Apply Changes**.
Discard Changes	To discard the changes to the Productivity Categories list or the Security Categories list, click **Discard Changes**.

Edit Screen Dialogs Reference

This section describes the following help topics:

- Policy Name
- Clone Policy
- Associate With Zone Pair
- Global Settings: General Tab
- Global Settings: Category Options Tab

Policy Name

Use this screen to enter the name of a policy.

How to get to this screen

In the navigation panel, click **Configure > Security > Web Filter Configuration > Edit Content Filter > Action > Add**.

Related Links

- Cisco Configuration Professional Content Filtering
- Creating a Content Filter
- Editing Content Filters

Field Reference

Table 40-9 Policy Name

Element	Description
Enter Policy Name	Enter a name for the Content Filtering policy.

Clone Policy

In this screen, enter a name for the clone policy. A clone policy is a policy created from an existing policy, which is given a new name.

How to Get to this Screen

In the navigation panel, click **Configure > Security > Web Filter Configuration > Edit Content Filter**. Then, choose an existing policy from the Content Filter Policy Name list, and click **Action > Clone**.

Related Links

- Using the Edit Content Filter Screens

Field Reference

Table 40-10 Clone Policy

Element	Description
Policy Name	In this field, enter a name for the policy. The policy you are creating has the same settings as the existing policy, unless you make changes to the policy settings.

Associate With Zone Pair

How to get to this screen

In the navigation panel, click **Configure > Security > Web Filter Configuration > Edit Content Filter > Associate**.

Related Links

- Cisco Configuration Professional Content Filtering
- Editing Content Filters
- Zone Pairs

Field Reference

Table 40-11 Associate With Zone Pair

Element	Description
Zone Pairs	This column lists the names of the configured zone pairs.
Associate	To associate a content filtering policy with a zone pair, check the Associate box in the same row as the zone pair name.

Edit Global Settings

Use this screen to edit Content filtering global settings.

This screen contains multiple tabs. The following parts describe each tab:

- Global Settings: General Tab
- Global Settings: Category Options Tab

Global Settings: General Tab

Use this tab to:

- Specify what the router is to do when it cannot contact the content filter server
- Make settings for logging, audit trail, and alerts, cache and buffer capacity
- Choose the interface the router will use to communicate with the server.

How to get to this tab

In the navigation panel, click **Configure > Security > Web Filter Configuration > Edit Content Filter > Global Settings > General**.

Related Links

- Cisco Configuration Professional Content Filtering
- Global Settings: Category Options Tab
- Editing Content Filters

Field Reference

Table 40-12 General Tab

Element	Description
Allow Mode	To enable the router to enter allow mode when the router cannot connect to any of the URL filtering servers in the server list, check **Allow Mode**. When the router is in Allow mode, all HTTP requests are allowed to pass if the router cannot connect to any server in the URL filter server list. Allow mode is disabled by default
Content Filter Alert	To enable the router to log content filtering alert messages, check **Content Filter Alert**. Content filtering alert messages report events such as a URL filtering server going down, or an HTTP request containing a URL that is too long for a lookup request. This option is disabled by default.
Audit Trail	To enable the router to maintain an audit trail in the log, check **Audit Trail**. The router records URL request status messages that indicate whether an HTTP request has been permitted or denied and other audit trail messages. This option is disabled by default.
Content Filter Server Log	To enable the router to record system messages that pertain to the URL filter server in the log, check **Content Filter Server Log**. This option is disabled by default.
Cache Size	To set the maximum size of the cache that stores the most recently-requested IP addresses and their respective authorization status, enter the number of bytes for the cache size in this field. The default size of this cache is 5000 bytes. The range is from 0 to 2147483647. The cache is cleared every 12 hours.
Source Interface	From this list, choose the interface from which the router is to receive data from the content filter server.
Reset Settings	To return the settings in this screen to their default values, click **Reset Settings**.

Global Settings: Category Options Tab

In this tab, specify settings for how the router handles traffic with the content filtering server, and the information to display to the user when a page is blocked.

How to get to this tab

In the navigation panel, click **Configure > Security > Web Filter Configuration > Edit Content Filter Global Settings > Category Options**.

Related Links

- Global Settings: General Tab
- Cisco Configuration Professional Content Filtering
- Editing Content Filters

Field Reference

Table 40-13 Category Options

Element	Description
Block-Page	Optional Field. Enter the message that is to be displayed to users when the server blocks a requested page.
Maximum Requests	Optional Field. The value you enter in this field specifies the maximum number of pending URL requests. The range is from 1 to 2147483647. The default is 1000.
Maximum Resp-PAK	Optional Field. The value you enter in this field specifies the number of HTTP responses that can be buffered. The range is from 0 and 20000. The default is 200.
Reset Settings	To return the settings in this screen to their default values, click **Reset Settings**.

Creating a Keyword Blocking Policy

A keyword blocking policy consists of a list of words that—when included in a domain name—will cause the Cisco IOS Content Filtering service to automatically block the response to the URL request, without sending a lookup request to the Content Filtering server.

To create a keyword blocking policy, complete the following steps:

Step 1 In the navigation panel, click **Configure > Security > Web Filter Configuration > Edit Content Filter**.

Step 2 Click **Keyword Blocking**. See URL Filtering: Keyword Blocking for a description of the Keyword Blocking screen.

Step 3 In the Keyword Blocking screen, click **Add**.

Step 4 In the Add Keyword screen, enter one or more keywords to block. If you enter multiple keywords, use a comma (,) to separate each keyword. See Add or Edit Keyword for a description of the dialog, and how you can add keywords.

Step 5 Click **OK** to return to the Keyword Blocking screen.

Keyword Blocking Screen Reference

This section describes the following help topics:

- URL Filtering: Keyword Blocking
- Add or Edit Keyword

URL Filtering: Keyword Blocking

In this screen, view and maintain the list of keywords that, when encountered in a domain name, automatically block the URL response without sending a lookup request to the server.

How to get to this screen

In the navigation panel, click **Configure > Security > Web Filter Configuration > Edit Content Filter > Keyword Blocking**.

Related Links

- Cisco Configuration Professional Content Filtering
- Editing Content Filters
- Using the Edit Content Filter Screens

Field Reference

Table 40-14 Keyword Blocking

Element	Description
Add	To add a keyword to the list, click **Add** and enter the keyword in the displayed dialog.
Edit	To edit an existing keyword, choose the keyword, and click **Edit**.
Delete	To remove a keyword from the list, choose the keyword, and click **Delete**.

Keyword List	This area displays the list of keywords configured locally on the router. A sample list might contain the following words.
	`adult`
	`brokerage`
	`weapons`
	`chat`
	If these words were in the keyword list, URL responses containing these word would be automatically blocked.

Add or Edit Keyword

In this screen, enter one or more keywords to add to the keyword list, or edit a keyword that is already on the list.

How to get to this screen

In the navigation panel, click **Configure > Security > Web Filter Configuration > Edit Content Filter > Keyword Blocking > Add** or **Edit.**

Related Links

- Cisco Configuration Professional Content Filtering
- URL Filtering: Keyword Blocking
- Editing Content Filters

Field Reference

Table 40-15 Enter Keyword

Element	Description
Keyword(s) to block	If you are adding keywords, enter one or more keywords, separated by commas. For example, you might add the words “adult, brokerage, chat room.” You can use the * wildcard to indicate a word pattern. For example, whit* would cause white, whitewash, whitney and all other strings beginning with “whit” to be blocked. If you are editing a keyword, the keyword you chose before clicking Edit appears in the field. You can edit it or replace it with another word.

Creating a Black and White Listing

Black and White listings enable you to reduce the number of times that the router must send lookup requests to the content filtering server. When the domain name in a URL request matches an item on the black list, the Cisco IOS Content Filtering service blocks the URL response to the user’s browser. When the domain name in an URL request matches an item on the white list, the Cisco IOS Content Filtering service sends the URL response to the user’s browser without performing a lookup request.

To create a Black and White listing complete the following steps:

Step 1 In the navigation panel, click **Configure > Security > Web Filter Configuration > Edit Content Filter**.

Step 2 Click **Black and White Listing**.

Step 3 In the Black and White Listing page, do one of the following:

- To import a black and white listing, click **Import**, and browse for the listing.
- To create a black and white list entry, click **Add**, and create the entry in the displayed dialog. See Add Local URL for information on full and partial domain names, and on the use of wildcards.

When you have created the entries or imported the list, each entry is displayed in the Black and White Listing screen. You can return to this screen at any time to add or edit entries.

Black and White Listing Screen Reference

This section describes the following help topics:

- Black and White List
- Add Local URL

Black and White List

In this screen, view the local list of domain names and the action associated with each one. From this screen, you can also import a URL list, and display a dialog to add a domain name and associated action.

How to get to this screen

In the navigation panel, click **Configure > Security > Web Filter Configuration > Edit Content Filter > Black and White Listing**.

Related Links

- Content Filter Wizard: Content Filter Server Configuration
- Creating a Black and White Listing
- Add Local URL
- Using the Edit Content Filter Screens

Field Reference

Table 40-16 Black and White List

Element	Description
Domain Name	This column displays the list of domain names stored on the router. Domain names can full, or partial.
Action	This column displays the action that is associated with the domain name.
Add	To add a domain name to this list, click **Add**, and enter the domain name in the displayed dialog.
Edit	To edit a domain name in this list, click **Edit**, and update the domain name in the displayed dialog.
Import	To import a URL list from the PC, click Import and browse for the list. The URL list that you import must have a .txt or .CSV extension.
Delete	To remove a domain name from this list, choose the domain name, and click **Delete**.

Add Local URL

In this screen, add a URL to the Black and White listing or to a URL list for a content filtering parameter map. The URL that you add is stored on the device that you are configuring.

How to get to this screen

- In the navigation panel, click **Configure > Security > Web Filter Configuration > Edit Content Filter > Black and White Listing > Add** or **Edit.**
- In the navigation panel, click **Configure > Security > Web Filter Configuration > Content Filtering Components > Parameter Map > URLF-Parameter > URL List > Add**.

Related Links

- Black and White List
- Add Content Filtering: URL List Tab

Field Reference

Table 40-17 Add Local URL

Element	Description
Enter complete or partial domain name	In this field, enter a full or partial domain name. If you enter a full domain name, such as www.somedomain.com, all requests that include that domain name, such as www.somedomain.com/news or www.somedomain.com/index will be permitted or denied based on the setting you choose in this dialog. These requests are not sent to the URL filtering servers that the router is configured to use. If you enter a partial domain name, such as .somedomain.com, all requests that end with that string, such as www.somedomain.com/products or wwwin/somedomain.com/eng will be permitted denied based on the setting you choose in this dialog. These requests are not sent to the URL filtering servers that the router is configured to use.
Action	Choose one of the following: • Permit—Requests for this URL are to be permitted. • Deny—Requests for this URL are to be denied.

Registering With a Category Server

Trend Micro category servers maintain a database of URL domain names, tagged with a category and reputation. For example, a domain name such as some-state-u.edu might be placed in the Education category, and be given the reputation UNBLEMISHED. By registering with a Trend Micro category server, you can have the router send lookup requests to the server when it receives a URL request, and receive a response that includes the domain name's category and reputation.

To register with a category server, and to obtain a certificate the router will use to authenticate itself when making URL requests, complete the steps in the following procedure.

Note You must have a CCO login ID and password r to register with a category server. If you do not have these credentials, go to http://www.cisco.com, and click **Register**.

Step 1 In the navigation panel, click **Configure > Security > Web Filter Configuration > Edit Content Filter > Category Server Registration**.

Step 2 In the Category Server Registration screen, click **Edit**.

Step 3 In the Trend tab, enter the IP address, HTTP and HTTPS port numbers, the retransmission count, and the timeout values.

Step 4 Click **Certificate**.

Step 5 In the Certificate tab, click **Download Certificate**, and provide your CCO login credentials.

Step 6 In the download page, enter the IP address of the router that you are configuring, and click **Submit**.

Step 7 In the login dialog that is displayed, enter the login ID and password for the router.

When the certificate has been downloaded, the router displays a web page indicating that the process is complete. The web page advises you to use the link on the page to save the running configuration to startup configuration.

Step 8 Click the link, and reenter the login credentials to save the running configuration to startup configuration.

Step 9 Click **Registration**, and in the Registration tab, click **Swift Registration**.

Step 10 Provide your CCO login credentials.

Step 11 Enter the Product Authorization Key and click **Submit**.

When the Swift Registration server responds, the router has registered with the server.

Category Server Registration Screen Reference

This section describes the following help topics:

- Category Server Registration
- Edit Category Server
- Edit Dialog: Trend Tab
- Edit Dialog: Registration Tab
- Edit Dialog: Certificate Tab

Category Server Registration

In this screen, view the details of the Trend Micro server that the router is registered to use, and display dialogs that allow you to enter the server information, register with the server, and obtain a certificate for authentication.

Note The router must use an advanced security Cisco IOS Release 12.4 (19) image for this screen and its dialog boxes to be displayed.

How to get to this screen

In the navigation panel, click **Configure > Security > Web Filter Configuration > Edit Content Filter > Category Server Registration**.

Related Links

- Edit Dialog: Trend Tab
- Edit Dialog: Registration Tab
- Edit Dialog: Certificate Tab
- Using the Edit Content Filter Screens

Field Reference

Table 40-18 Category Server Registration

Element	Description
Edit	To enter information for a Trend Micro server and register with the server, click **Edit** and provide the information in the displayed dialogs.

Item Name and Item Value	These columns contain the configuration parameters and values for the Trend Micro server. For example, server details might be the following:
	`Trend Server` `global-param-map`
	`Server IP Address` `192.168.7.5`
	`HTTP Port` `80`
	`HTTPS Port` `443`
	`Retransmission Count` `5`
	`Time Out` `10`

Edit Category Server

In this screen edit the information for a category server.

This screen contains multiple tabs. The following parts describe each tab:

- Edit Dialog: Trend Tab
- Edit Dialog: Registration Tab
- Edit Dialog: Certificate Tab

Edit Dialog: Trend Tab

In this tab, provide the name, IP address, port numbers, and transmission settings for a Trend Micro server.

How to get to this tab

In the navigation panel, click **Configure > Security > Web Filter Configuration > Edit Content Filter > Category Server Registration > Edit > Trend.**

Related Links

- Category Server Registration
- Edit Dialog: Registration Tab
- Edit Dialog: Certificate Tab
- Using the Edit Content Filter Screens

Field Reference

Table 40-19 Trend Tab

Element	Description
Server IP Address	Enter the server IP address.
HTTP Port	Enter the HTTP port number to use. The default is 80.
HTTPS Port	Enter the HTTPS port number to use. The default is 443.
Retransmission Count	Enter the number of times that the Cisco IOS Content Filtering service is to retransmit the request when a response does not arrive for the request. The default value is 2.
Timeout	Enter the number of seconds that the Cisco IOS Content Filtering service is to wait for a response from the server. The default is 5.

Edit Dialog: Registration Tab

In this tab, contact the Swift registration server to register with the Trend Micro server.

How to get to this tab

In the navigation panel, click **Configure > Security > Web Filter Configuration > Edit Content Filter > Category Server Registration > Edit > Registration**.

Related Links

- Edit Dialog: Trend Tab
- Edit Dialog: Certificate Tab

Field Reference

Table 40-20 Registration Tab

Element	Description
Swift Registration	To register with the Trend Micro server, ensure that you have entered the correct information in the Trend tab, and click **Swift Registration**.
Status	This field displays the status of the registration attempt. This field displays these values: • Registration is pending • Registration succeeded • Registration failed If registration fails or does not complete after several minutes, test connectivity between the router and the IP address that you entered in the Trend tab, and ensure that the IP address in the Trend tab is correct.

Edit Dialog: Certificate Tab

In this tab, download the certificate that the Cisco IOS Content Filtering service needs to authenticate itself with the Trend Micro server.

How to get to this tab

In the navigation panel, click **Configure > Security > Web Filter Configuration > Edit Content Filter > Category Server Registration > Edit > Certificate**.

Related Links

- Edit Dialog: Trend Tab
- Edit Dialog: Registration Tab

Field Reference

Table 40-21 Certificate Tab

Element	Description
Download Certificate	Click this link to download the certificate to the router.
Status	This field displays the certificate status. This field can display: • Certificate is not present • Download in progress • Certificate is present.

Filtering By URL Category

Content filtering servers assign categories to domain names. You can permit or deny responses to URL requests based on the category assigned to the domain name in the request.

To filter by URL category, complete the following steps:

Step 1 In the navigation panel, click **Configure > Security > Web Filter Configuration > Edit Content Filter**.

Step 2 If you have not registered with a Trend Micro server, complete the procedure in Registering With a Category Server. If you have registered, go to Step 3.

Step 3 Click **Category Filtering**.

Step 4 In the Category Filtering screen, check the content categories that you want to block. All categories that are not checked are allowed. See Content Filter Wizard and Edit Screen: Category Selection for more information.

Step 5 When you have finished checking categories, click **Apply Changes** to send the information to the router. To remove all check marks that you have made before clicking Apply Changes, click **Discard Changes**. All check boxes are cleared.

URL Category Screen Reference

This section describes the following screens:

- Content Filter Wizard and Edit Screen: Category Selection

Filtering By URL Reputation

Content filtering servers assign reputations to domain names. You can permit or deny responses to URL requests based on the reputation assigned to the domain name in the request.

To filter by URL reputation, complete the following steps:

Step 1 In the navigation panel, click **Configure > Security > Web Filter Configuration > Edit Content Filter**.

Step 2 If you have not registered with a Trend Micro server, complete the procedure in Registering With a Category Server. If you have registered, go to the next step.

Step 3 Click **Security Categories**.

Step 4 In the Reputation Filtering screen, check the content categories that you want to block. All those categories that are not checked are allowed. See Content Filter Wizard and Edit Screen: Reputation Selection for more information.

Step 5 When you have finished checking categories, click **Apply Changes** to send the information to the router. To remove all check marks that you have made before clicking Apply Changes, click **Discard Changes**. All check boxes are cleared.

URL Reputation Screen Reference

This section describes the following screens:

- Content Filter Wizard and Edit Screen: Reputation Selection

Configuring the Router To Use Websense or Secure Computing Servers

If there are Websense or Secure Computing URL filter servers on the network, you can configure the router to use them. When the router uses these types of URL filter servers, you can filter responses to URL requests by the category and the reputation that the server assigns to the domain name in the URL.

To configure the router to use Websense or Secure Computing servers, complete these steps:

Step 1 In the navigation panel, click **Configure > Security > Web Filter Configuration > Edit Content Filter**.

Step 2 Click Server Filtering. The Server Filtering screen is displayed.

Step 3 In the Server Filtering screen, click **Add**, and choose either **Secure Computing** or **Websense** from the context menu.

Step 4 In the displayed dialog, enter the information for the URL filter server, and click **OK**. See Add Secure Computing or Websense Server for more information on this dialog.

Step 5 To add the information for more servers, click **Add**, choose the same type of server, and enter the information in the displayed dialog.

Step 6 In the Server Filtering screen, review the information that you added.

URL Filter Server Screen Reference

This section describes the following screens:

- Server Filtering
- Add Secure Computing or Websense Server

Server Filtering

In this screen, view the details of the configured content filter servers, and displays dialogs that enable you to add new servers or edit existing server configurations.

How to get to this screen

In the navigation panel, click **Configure > Security > Web Filter Configuration > Edit Content Filter > Server Filtering**.

Related Links

- Add Secure Computing or Websense Server
- Using the Edit Content Filter Screens

Field Reference

Table 40-22 Server Filtering List

Element	Description
Vendor Name	This column displays the vendor names of the filtering servers. The possible values are Secure Computing and Websense. However, all servers must be from the same vendor. The same value appears for each row in this column.
IP Address/Hostname	This column displays the IP address or hostnames of the configured servers.
Direction	This column displays either inside, or outside.
Port Number	This column displays the port number that is to be used when contacting the server.
Retransmission Count	This column displays the number of times that the router attempts to contact the server before stopping attempts.
Retransmission Timeout	Enter the number of seconds that the router should wait before attempting to retransmit packets to the server. The default value is 6.

Add Secure Computing or Websense Server

In this screen, enter the information for a Secure Computing or Websense server.

How to get to this screen

In the navigation panel, click **Configure > Security > Web Filter Configuration > Edit Content Filter > Server Filtering > Add Websense Server** or **Add Secure Computing Server**.

Related Links

- Server Filtering

Field Reference

Table 40-23 Add Secure Computing or Websense Server

Element	Description
Vendor Name	This field is prepopulated, and is not editable.
IP Address/Hostname	Enter the IP address or hostname of the server. If you enter a hostname, there must be a reachable DNS server that is able to resolve the hostname to the correct IP address.
Direction	Choose either inside or outside.
Port Number	Enter the port number that is to be used when contacting the server. the default port number is 4005.
Retransmission Count	Enter the number of times that the router should attempt to contact the server before stopping attempts. The default value is 2.
Retransmission Timeout	Enter the number of seconds that the router should wait before attempting to retransmit packets to the server. The default value is 6.

Configuring Content Filtering Components

See the following topics as appropriate:

- Configuring or Editing URL Filter Policy Maps
- Configuring URL Filter Class Maps
- Configuring or Editing URL Filter Parameter Maps

Configuring or Editing URL Filter Policy Maps

A policy map consists of one or more class maps. Class maps, in turn consist of one or more parameter maps. If you have not created any of the components that you need for the policy map, the dialogs enable you to do so as you create or edit the policy map.

Step 1 In the navigation panel, click **Configure > Security > Web Filter Configuration > Content Filtering Components**.

Step 2 Click **Policy Map > Content Filter**.

Step 3 In the displayed dialog, name and describe the policy map, and use the Add and Edit buttons to provide the necessary class maps and parameter maps for the policy map.

Step 4 When you have finished working in each dialog, click **OK** to close the dialog and return to the parent screen.

Step 5 In the policy map screen, review the details of the policy map that you have created or edited. If you need to make any changes, choose the policy map entry in the list, click **Edit**, and make the changes you need.

Related Topics

- Policy Map Text Description
- URL Filter Policy Map List
- Add or Edit URL Filter Policy Map Entry

URL Filter Policy Map Screen Reference

This section describes the following screens:

- Policy Map Text Description
- URL Filter Policy Map List
- Add or Edit URL Filter Policy Map Entry

Policy Map Text Description

In this screen, review the description of policy maps.

How to get to this screen

In the navigation panel, click **Configure > Security > Web Filter Configuration > Content Filtering Components > Policy Map**.

Related Links

- Configuring or Editing URL Filter Policy Maps

URL Filter Policy Map List

In this screen, review all configured URL filtering policy maps, and display dialogs that enable you to create and edit URL filtering policy maps.

How to get to this screen

In the navigation panel, click **Configure > Security > Web Filter Configuration > Content Filtering Components > Policy Map > Content Filter**.

Related Links

- Configuring or Editing URL Filter Policy Maps
- Add or Edit URL Filter Policy Map Entry

Field Reference

Table 40-24 URL Filter Policy Map List

Element	Description
Content Filter Policy Map	
Policy Map Name	This column contains the names of the configured policy maps. To view the details of a policy map, select the policy map name, and view details in the Details of Policy Map area.
Used By	This column contains the names of the zones associated with the policy map.
Details of Policy Map	

Table 40-24 URL Filter Policy Map List

Element	Description
Match Class Name	This column contains the names of the class maps associated with the policy map.
Action	This column lists the action that is taken when a matching domain name is encountered. The value `server-specified-action` indicates that the action taken is specified by the Content Filtering server.
Log	This column can contain the following values: • true—a log entry is created when the router encounters a matching URL. • false—no log entry is created when the router encounters a matching URL.

Add or Edit URL Filter Policy Map Entry

In this screen, add or edit a URL filtering policy map. From this screen, you can display additional dialogs that enable you to create class maps for the policy map, and parameter maps.

How to get to this screen

In the navigation panel, click **Configure > Security > Web Filter Configuration > Content Filtering Components > Policy Map > Content Filter > Add** or **Edit**.

Related Links

- Configuring or Editing URL Filter Policy Maps

Field Reference

Table 40-25 Add URL Filter Policy Map

Element	Description
Policy Name	In this field, enter a name for the policy map. If you are editing a policy map, this field cannot be edited.
Description	Enter a description of the policy map.

Table 40-25 Add URL Filter Policy Map (continued)

Element	Description
Select Parameter Type	In this field, choose the type of class map to add to the policy map. You can choose the following: • None—Create a class map for local filtering. • websense—Create a class map for Websense content filtering. • n2h2—Create a class map for N2H2 content filtering. • trend—Create a class map for Trend Micro category filtering. • local—Create a class map for local filtering. **Note** If you choose websense, n2h2, or trend, additional class maps that use content filtering servers must be of the same type. For example, if you choose websense and create a websense class map, you can create a local filtering class map, but you cannot create a trend class map for the same policy map.
Select Parameter Name	The parameter name is automatically chosen based on the chosen parameter type.
Class Map List Area	
Class Map	This column contains the name of the class map.
Action	This column can contain one of the following values: • Allow—Allow the URL. • Reset—Reset the connection between the user browser and the web server. Allow and Reset are available for local filtering. Reset is available for Trend, Websense, and N2H2 filtering.
Log	This column can contain one of the following values: • True—Log matches against the class map. • False—Do not log matches against the class map. Log is available for local and server-based filtering.
Add	To create a new class map, click **Add** and create the class map in the displayed dialogs.

Table 40-25 Add URL Filter Policy Map (continued)

Element	Description
Edit	To edit an existing class map, click **Edit** and create the class map in the displayed dialogs.
Delete	To remove a class map from the policy map, choose the class map, and click **Delete**.
Move Up	To move a class map up the list, so that URLs are evaluated against the contents of the class map before being evaluated against the contents of other class maps for the policy map, choose the class map, and click **Move Up**.
Move Down	To move a class map down the list, so that URLs are evaluated against the contents of the class map after being evaluated against the contents of other class maps for the policy map, choose the class map, and click **Move Down**.

Add Action

In this screen, display additional dialogs to create a class map, and associate an action with the traffic defined in the class map.

How to get to this screen

In the navigation panel, click **Configure > Security > Web Filter Configuration > Content Filtering Components > Policy Map > Content Filter > Add** or **Edit > Add** or **Edit**.

Related Links

- Configuring or Editing URL Filter Policy Maps
- Add or Edit URL Filter Policy Map Entry
- Add or Edit URL Filter Local Class Map Entry
- Add or Edit Websense Class Map Entry
- Add or Edit N2H2 Class Map Entry
- Add Trend Rule

Field Reference

Table 40-26 URL Filter Policy Map Entry

Element	Description
Class Map	If you are creating a class map, click the context button to the right of the field, and choose the type of class map that you want to enter. When you enter the necessary information in the class map dialogs, the name that you entered is displayed in this field. If you are editing a class map, this field contain the name of the class map and is not editable.
Context button	Click the Context button to display dialog boxes to create a class map for local filtering, or a class map for a Content Filtering server. The button options are the following: • URLF-Local—Create a class map for local filtering. This option is always available. • URLF-Websense—Create a class map for filtering by a Websense server. This option is available when websense is chosen in the Add or Edit URL Filter Policy Map Entry Parameter Type field. • URLF-N2H2—Create a class map for filtering by an N2H2 server. This option is available when n2h2 is chosen in the Add or Edit URL Filter Policy Map Entry Parameter Type field. • URLF-Trend—Create a class map for filtering by a Trend server. This option is available when trend is chosen in the Add or Edit URL Filter Policy Map Entry Parameter Type field.
Log	To create a log entry when traffic matching the class map arrives, check **Log**.
Action	Choose what the router is to do with traffic that matches the class map. • Allow—Allows the traffic to pass. • Reset—Blocks the traffic and resets the connection at both ends.

Configuring URL Filter Class Maps

The Cisco IOS content filtering service filters URL requests on the basis of match criteria in class maps. To enable local URL filtering, you must specify at least one class map each for trusted domains, untrusted domains, and blocked keywords. The match criteria for these class maps are specified in a parameter map, which must be configured before the class map is configured.

Step 1 In the navigation panel, click **Configure > Security > Web Filter Configuration > Content Filtering Components**.

Step 2 Click **Class Map**. The tree expands to display the types of parameter maps that you can configure.

Step 3 Choose the type of class map that you want to configure, for example, Websense.

Step 4 In the list screen for that class map type, click **Add** to create a new class map, or choose an existing class map and click **Edit** to modify it.

Step 5 Enter the information for the class map in the displayed dialog.

Step 6 If the dialog provides Add or Edit buttons to enable you to create and modify subordinate entries for the class map, use those buttons to display the dialogs for those entries.

Step 7 When you have finished working in each dialog, click **OK** to close the dialog and return to the parent screen.

Step 8 In the class map screen, review the details of the class map that you have created or edited. If you need to make any changes, choose the class map entry in the list, click **Edit**, and make the changes you need.

Related Topics

- Class Map Text Description
- Content Filter Local Class Map List
- Add or Edit URL Filter Local Class Map Entry
- Add Local Rule
- URL Filter Websense Class Map List
- Add or Edit Websense Class Map Entry

- Content Filter N2H2 Class Map List
- Add or Edit N2H2 Class Map Entry
- Content Filter Trend Class Map List
- Add Trend Rule

URL Filter Class Map Screen Reference

This section describes the following screens:

- Class Map Text Description
- Content Filter Local Class Map List
- Add or Edit URL Filter Local Class Map Entry
- Add Local Rule
- URL Filter Websense Class Map List
- Add or Edit Websense Class Map Entry
- Content Filter N2H2 Class Map List
- Add or Edit N2H2 Class Map Entry
- Content Filter Trend Class Map List
- Add Trend Rule

Class Map Text Description

In this screen, review the description of class maps.

How to get to this screen

In the navigation panel, click **Configure > Security > Web Filter Configuration > Content Filtering Components > Class Map**.

Related Links

- Configuring URL Filter Class Maps

Content Filter Local Class Map List

In this screen, review configured local class maps, and display dialogs to create and edit local class maps. Local class maps are those class maps created to perform local filtering.

How to get to this screen

In the navigation panel, click **Configure > Security > Web Filter Configuration > Content Filtering Components > Class Map > URLF-Local.**

Related Links

- Configuring URL Filter Class Maps
- Add or Edit URL Filter Local Class Map Entry

Field Reference

Table 40-27 Local Class Map List

Element	Description
Content Filter Local Class Map	
Add	To create a class map, click **Add**, and enter the class map information in the displayed dialogs.
Edit	To edit an existing class map, click **Edit**, and update the class map information in the displayed dialogs.
Delete	To remove a class map configuration, choose the class map, and click **Delete**.

Class Map Name and Used By	These columns display the names of the configured class maps and the names of the policy maps to which they are associated. If you configured local class maps for trusted domains, untrusted domains, and keywords to block, a list might contain the following names:
	`untrusted-domain-class urlfltr-pol`
	`trusted-domain-class urlfltr-pol`
	`keyword-class urlfltr-pol`

Used By	This column displays the policy maps that use the class map.
Details of Class Map	

Table 40-27 Local Class Map List (continued)

Element	Description
Item Name And Item Value	These columns contain configuration parameters and values for the selected class map. For example, parameter map details might be the following: `Server Domain trusted-domain-param`

Add or Edit URL Filter Local Class Map Entry

In this screen, create or edit a local class map. Local class maps define the traffic that the router will inspect and act on without sending a lookup request to a content filter server.

How to get to this screen

In the navigation panel, click **Configure > Security > Web Filter Configuration > Content Filtering Components > Class Map > URLF-Local > Add**.

Related Links

- Configuring URL Filter Class Maps
- Content Filter Local Class Map List
- Add Local Rule

Field Reference

Table 40-28 Local Class Map

Element	Description
Class Map Name	In this field, enter or edit the class map name. It can be helpful to create descriptive names for the class map, such as local-cmap.
Description	Enter a description for the class map.
Match Criteria Area	

Table 40-28 Local Class Map (continued)

Element	Description
Match	This column contains one of the following values: • Server-Domain—The class map entry matches a server-domain parameter map. • URL-Keyword—The class map entry matches a URL-keyword parameter map.
Value	This field contains the name of the parameter map whose contents must be matched. Example parameter map names are untrusted-domain-param, and blocked-keyword-param.
Add	To add an entry for the class map, click **Add** and create the entry in the displayed dialogs.
Edit	To edit an entry for the class map, choose the entry, and click **Edit**. Then, edit the information in the displayed dialogs.
Delete	To remove an entry for the class map, select the entry and click **Delete**.
Move Up	To move a class map entry up the list so that it is evaluated before other entries in the class map, select the entry and click **Move Up**.
Move Down	To move a class map entry down the list so that it is evaluated after other entries in the class map, select the entry and click **Move Down**.

Add Local Rule

In this screen, choose a local server-domain parameter map or URL-keyword parameter map. The parameter map must already be created.

How to get to this screen

In the navigation panel, click **Configure > Security > Web Filter Configuration > Content Filtering Components > Class Map > URLF-Local > Add > Add.**

Related Links

- Configuring URL Filter Class Maps
- Add or Edit URL Filter Local Class Map Entry
- Content Filter Glob Parameter Map List
- Add or Edit Regular Expression

Field Reference

Table 40-29 Local Rule

Element	Description
Match Criteria	Specify the criteria for a server-domain name value or for a URL keyword value.
Enter Value	Choose the name of the parameter map from this list. If there are no parameter maps, click **Parameter Map > URLF-Glob > Add**, and create a glob parameter map that you need to use.

URL Filter Websense Class Map List

In this screen, review configured Websense class maps, and display dialogs to create and edit Websense class maps.

How to get to this screen

In the navigation panel, click **Configure > Security > Web Filter Configuration > Content Filtering Components > Class Map > URLF-Websense**.

Related Links

- Configuring URL Filter Class Maps

Field Reference

Table 40-30 Websense Class Map List

Element	Description
Content Filter Websense Class Map	
Add	To create a class map, click **Add**, and enter the class map information in the displayed dialogs.
Edit	To edit an existing class map, click **Edit**, and update the class map information in the displayed dialogs.
Delete	To remove a class map configuration, choose the class map, and click **Delete**.
Class Map Name	This column displays the names of the configured class maps.
Used By	This column displays the policy maps that use the class map.
Details of Websense Class Map	
Item Name And Item Value	These columns contain configuration parameters and values for the selected class map. For example, parameter map details might be the following: `Allow Server Response true` The class map accepts responses from any Websense server.

Add or Edit Websense Class Map Entry

In this screen, create or edit a Websense class map.

How to get to this screen

In the navigation panel, click **Configure > Security > Web Filter Configuration > Content Filtering Components > Class Map > URLF-Websense > Add** or **Edit**.

Related Links

- Configuring URL Filter Class Maps

Field Reference

Table 40-31 Websense Class Map

Element	Description
Class Map Name	In this field, enter a class map name, or click the context button and choose the name of an existing class.
Description	In this field, enter a description for the class map.
Match Criteria	
Allow Server Response	To allow a response from any configured server, check **Any**.

Content Filter N2H2 Class Map List

In this screen, review configured N2H2 class maps, and display dialogs that enable you to create and edit class maps.

How to get to this screen

In the navigation panel, click **Configure > Security > Web Filter Configuration > Content Filtering Components > Class Map > URLF-N2H2**.

Related Links

- Configuring URL Filter Class Maps
- Add or Edit N2H2 Class Map Entry

Field Reference

Table 40-32 N2H2 Class Map List

Element	Description
Content Filter N2H2 Class Map	
Add	To create a class map, click **Add**, and enter the class map information in the displayed dialogs.
Edit	To edit an existing class map, click **Edit**, and update the class map information in the displayed dialogs.
Delete	To remove a class map configuration, choose the class map, and click **Delete**.
Class Map Name	This column lists the names of the configured class maps.
Used By	This column displays the policy maps that use each class map.
Details of N2H2 Class Map	
Item Name And Item Value	These columns contain configuration parameters and values for the selected class map. For example, parameter map details might be the following: `Allow Server Response true` The class map accepts responses from any Websense server.

Add or Edit N2H2 Class Map Entry

In this screen,

How to get to this screen

In the navigation panel, click **Configure > Security > Web Filter Configuration > Content Filtering Components > Class Map > URLF-N2H2 > Add** or **Edit.**

Related Links

- Configuring URL Filter Class Maps

Field Reference

Table 40-33 N2H2 Class Map

Element	Description
Class Map Name	In this field, enter a class map name, or click the context button and choose the name of an existing class.
Description	In this field, enter a description for the class map.
Match Criteria	
Allow Server Response	To allow a response from any configured server, check **Any**.

Content Filter Trend Class Map List

In this screen, review configured Trend class maps, and display dialogs to create and edit Trend class maps. Trend class maps specify the traffic that the router is to block based on category and reputation ratings on the Trend Micro server.

How to get to this screen

In the navigation panel, click **Configure > Security > Web Filter Configuration > Content Filtering Components > Class Map > URLF-Trend**.

Related Links

- Configuring URL Filter Class Maps
- Add or Edit Trend Class Map Entry

Field Reference

Table 40-34 Trend Class Map List

Element	Description
Class Map List Area	
Add	To create a class map, click **Add**, and enter the class map information in the displayed dialogs.
Edit	To edit an existing class map, click **Edit**, and update the class map information in the displayed dialogs.

Table 40-34 Trend Class Map List (continued)

Element	Description
Delete	To remove a class map configuration, choose the class map, and click **Delete**.
Details of Class Map	

Item Name and Item Value	These columns contain the configuration parameters and values for the selected class map. For example, class map details might be the following:
	`Category Abortion,Activist-Groups,`
	`Reputation ADWARE,HACKING,`
	The class map will drop traffic that is categorized as abortion or activist-groups-related, and traffic that has been given the ADWARE or HACKING reputation on the Trend Micro server.

Add or Edit Trend Class Map Entry

In this screen, create or edit a Trend class map. Trend class maps specify which traffic will be blocked, based on Trend-defined categories and reputations assigned to domain names.

How to get to this screen

In the navigation panel, click **Configure > Security > Web Filter Configuration > Content Filtering Components > Class Map > URLF-Trend > Add** or **Edit.**

Related Links

- Content Filter Trend Parameter Map List
- Add Trend Rule

Table 40-35 Trend Class Map

Element	Description
Class Map Name	In this field enter a name for the class map.
Description	In this field, enter a description for the class map.
Match Criteria	

Table 40-35 Trend Class Map

Element	Description
Match	This column lists the type of match criteria. There are two types: • Category—Match against Trend Micro-defined categories. The router sends a lookup request to the Trend Micro server. • Reputation—Match against Trend Micro-defined reputations.
Value	This column contains the category or reputation values against which the match is to be made. Example categories are Abortion, and Activist-Groups. Example reputations are ADWARE, and HACKING. If the lookup requests returns one of the categories or reputations specified in the class map, the traffic is blocked.
Add	To create a new class map entry, click **Add** and create the entry in the displayed dialogs.
Edit	To edit an existing class map, click **Edit** and create the entry in the displayed dialogs.
Delete	To remove an entry from the class map, choose the entry, and click **Delete**.
Move Up	To move an entry up the list, so that URLs are evaluated against the entry before being evaluated against other class map entries, choose the entry, and click **Move Up**.
Move Down	To move an entry down the list, so that URLs are evaluated against other entries before being evaluated against this one, choose the entry, and click **Move Down**.

Add Trend Rule

In this screen, create or edit a Trend category or reputation entry.

How to get to this screen

In the navigation panel, click **Configure > Security > Web Filter Configuration > Content Filtering Components > Class Map > URLF-Trend > Add** or **Edit > Add** or **Edit.**

Related Links

- Configuring URL Filter Class Maps
- Content Filter Trend Class Map List

Field Reference

Table 40-36 Trend Rule

Element	Description
Match Criteria	Choose one of the following: • Category—Match against a Trend Micro-defined category. • Reputation—Match against a Trend Micro-defined reputation.
Enter Value	If you chose Category, this list contains the Trend Micro-defined categories. Choose a category from this list. Traffic that matches this category will be blocked. If you chose Reputation, this list contains the Trend Micro-defined reputations. Choose a reputation from this list. Traffic that matches this reputation will be blocked.

Configuring or Editing URL Filter Parameter Maps

Complete the following steps to configure a URL filter parameter map:

Step 1 In the navigation panel, click **Configure > Security > Web Filter Configuration > Content Filtering Components**.

Step 2 Click **Parameter Map**. The tree expands to display the types of parameter maps that you can configure.

Step 3 Choose the type of parameter map that you want to configure, for example, Websense.

Step 4 In the list screen for that parameter map type, click **Add** to create a new parameter map, or choose an existing parameter map and click **Edit** to modify it.

Step 5 Enter the information for the parameter map in the displayed dialog.

Step 6 If the dialog provides Add or Edit buttons to enable you to create and modify subordinate entries for the parameter map, use those buttons to display the dialogs for those entries.

Step 7 When you have finished working in each dialog, click **OK** to close the dialog and return to the parent screen.

Step 8 In the parameter map screen, review the details of the parameter map that you have created or edited. If you need to make any changes, choose the parameter map entry in the list, click **Edit**, and make the changes you need.

Related Topics

- URL Filter Parameter Map Screen Reference

URL Filter Parameter Map Screen Reference

This section describes the following screens:

- Parameter Map Text Description
- Content Filtering Parameter Maps
- Add Content Filtering: General Tab
- Add Content Filtering: Content Filter Servers Tab

- Add Content Filtering: URL List Tab
- Content Filter Local Parameter Map List
- Add or Edit URL Filtering Local Parameter Map
- Content Filter Websense Parameter Map List
- Add or Edit Websense Parameter Map
- Content Filter N2H2 Parameter Map List
- Add or Edit N2H2 Parameter Map
- Content Filter Trend Global Parameter Map List
- Add or Edit Trend Global Parameter Map
- Content Filter Trend Parameter Map List
- Add or Edit Trend Parameter Map
- Content Filter Glob Parameter Map List
- Add or Edit Regular Expression

Parameter Map Text Description

In this screen, review the description of parameter maps.

How to get to this screen

In the navigation panel, click **Configure > Security > Web Filter Configuration > Content Filtering Components > Parameter Map**.

Content Filtering Parameter Maps

In this screen, view the configured content filter parameter maps, details about each parameter map, and display dialogs that enable you to create and edit parameter maps.

The parameter maps that are listed in this screen also appear when you go to Configure > Security > C3PL > Parameter Maps > URL Filtering.

How to get to this screen

In the navigation panel, click **Configure > Security > Web Filter Configuration > Content Filtering Components > Parameter Map > URLF-Parameter**.

Field Reference

Table 40-37 Parameter Map List

Element	Description
Content Filtering Parameter Maps	
Content Filter Name	This column lists the names of the content filter parameter maps. To view the details of a particular parameter map, select the parameter map name.
Used By	This column displays the class maps that use the parameter map.
Details of Parameter Map	

Item Name And Item Value	These columns contain selected configuration parameters and values for the selected parameter map. For example, parameter map details might be the following:
	`Content Filter Alert On`
	`Allow Mode Off`
	`Audit Trail Off`
	`Message Logging Off`
	`Source Interface GigabitEthernet 0/0`
	The values in the display are taken from the values entered in the General tab.

Add Content Filtering: General Tab

In this screen, specify what the router is to do when it cannot contact the content filter server, make settings for logging, audit trail, and alerts, cache and buffer capacity, and choose the interface the router will use to communicate with the server.

How to get to this screen

In the navigation panel, click **Configure > Security > Web Filter Configuration > Content Filtering Components > Parameter Map > URLF-Parameter > General.**

Related Links

- Content Filtering Parameter Maps
- Add Content Filtering: Content Filter Servers Tab
- Add Content Filtering: URL List Tab

Field Reference

Table 40-38 General Tab

Element	Description
Content Filter Name	Enter a name that will convey how this content filter is configured or used. For example, if you specify a source interface of Fast Ethernet 1, you might enter the name **fa1-parmap**. If the filter uses a Websense URL filter server at IP address 192.128.54.23, you might enter **websense23-parmap** as the name.
Allow Mode	To enable the router to enter allow mode when the router cannot connect to any of the URL filtering servers in the server list, check **Allow Mode**. When the router is in Allow mode, all HTTP requests are allowed to pass if the router cannot connect to any server in the URL filter server list. Allow mode is disabled by default
Content Filter Alert	To enable the router to log content filtering alert messages, check **Content Filter Alert**. Content filtering alert messages report events such as a URL filtering server going down, or an HTTP request containing a URL that is too long for a lookup request. This option is disabled by default.

Table 40-38 General Tab (continued)

Element	Description
Audit Trail	To enable the router to maintain an audit trail in the log, check **Audit Trail**. The router will record URL request status messages that indicate whether an HTTP request has been permitted or denied and other audit trail messages. This option is disabled by default.
Content Filter Server Log	To enable the router to record system messages that pertain to the URL filter server in the log, check **Content Filter Server Log**. This option is disabled by default.
Cache Size	To set the maximum size of the cache that stores the most recently-requested IP addresses and their respective authorization status, enter the number of bytes for the cache size in this field. The default size of this cache is 5000 bytes. The range is from 0 to 2147483647. The cache is cleared every 12 hours.
Maximum Buffered HTTP Requests	To set the maximum number of outstanding HTTP requests that the router can buffer enter the number of requests in this field. By default, the router buffers up to 1000 requests. You can specify from 1 to 2147483647 requests.
Maximum Buffered HTTP Responses	To set the number of HTTP responses from the URL filtering server that the router can buffer, enter the number of responses to buffer in this field. After this number is reached, the router drops additional responses. The default value is 200. You can set a value from 0 to 20000.
Source Interface	From this list, choose the interface from which the router is to receive data from the content filter server.
Reset Settings	To return the settings in this screen to their default values, click **Reset Settings**.

Add Content Filtering: Content Filter Servers Tab

In this screen, enter and edit information for content filter servers on your network.

How to get to this screen

In the navigation panel, click **Configure > Security > Web Filter Configuration > Content Filtering Components > Parameter Map > URLF-Parameter > Content Filter Servers.**

Related Links

- Content Filtering Parameter Maps
- Add Content Filtering: General Tab
- Add Content Filtering: URL List Tab

Field Reference

Table 40-39 Content Filter Servers Tab

Element	Description
Server List	
No.	This field is read only. The number indicates the order of the server in the list.
Server Name or IP Address	Enter the IP address or the hostname for the server. If you enter a hostname, the router must have a connection to a DNS server in order to resolve the hostname to an IP address.
Server Type	This field indicates the type of content filter server. Values are the following: • Websense • n2h2 • Secure computing
Add	To add a server to the list, click Add, and enter server information in the displayed dialog.
Edit	To edit a server entry in the list, choose the entry, click **Edit**, and update the information in the displayed dialog.
Delete	To remove a server from the list, choose the server entry, and click **Delete**.

Add Content Filtering: URL List Tab

In this screen, create and maintain a local URL list that will be stored on the router.

How to get to this screen

In the navigation panel, click **Configure > Security > Web Filter Configuration > Content Filtering Components > Parameter Map > URLF-Parameter > URL List.**

Related Links

- Content Filtering Parameter Maps
- Add Content Filtering: General Tab
- Add Content Filtering: Content Filter Servers Tab
- Add Local URL

Field Reference

Table 40-40 URL List Tab

Element	Description
Add	To add a domain name to the URL list, click **Add** and enter the domain name in the displayed dialog.
Edit	To edit a domain name to the URL list, choose the domain name, click **Edit** and update the domain name in the displayed dialog.
Delete	To remove a domain name from the URL list, choose the domain name, and click **Delete**.
Delete All	To remove all domain names from the URL list, click **Delete All**.
Import URL List	To import an URL list from the PC, click **Import URL List**, and browse for the URL list file. The URL list that you select must have a .txt or .CSV extension. When you save a URL list to the PC, the list is given a .CSV extension.
Export URL List	To export the URL list in this screen to the PC, click **Export URL List**, and browse for the URL list file.
Domain Name	The field contains a full or partial domain name.
Action	This field contains the action that has been applied to the domain. The actions are the following: • Permit • Deny

Content Filter Local Parameter Map List

In this screen, review the local parameter maps, and display dialogs that enable you to create and edit local parameter maps.

How to get to this screen

In the navigation panel, click **Configure > Security > Web Filter Configuration > Content Filtering Components > Parameter Map > URLF-Local**.

Related Links

- Add or Edit URL Filtering Local Parameter Map

Field Reference

Table 40-41 Local Parameter Map List

Element	Description
Content Filter Local Parameter Map	
Parameter Map Name	This column contains the names of the configured local parameter maps.
Used By	This column displays the class maps that use the parameter map.
Details of Local Parameter Map	

Item Name and Item Value	These columns contain the configuration parameters and values for the selected parameter map. For example, parameter map details might be the following:
	`Content Filter Alert Yes`
	`Allow Mode No`
	`Block Page This page not allowed`

Add or Edit URL Filtering Local Parameter Map

In this screen, provide the information for a local URL filtering parameter map.

How to get to this screen

In the navigation panel, click **Configure > Security > Web Filter Configuration > Content Filtering Components > Parameter Map > URLF-Local > Add** or **Edit.**

Related Links

- Content Filter Local Parameter Map List

Field Reference

Table 40-42 Local Parameter Map

Element	Description
Content Filter	In this field enter a name for the parameter map.

Table 40-42 Local Parameter Map (continued)

Element	Description
Content Filter Alert	To enable the router to log content filtering alert messages, check **Content Filter Alert**. Content filtering alert messages report events such as a URL filtering server going down, or an HTTP request containing a URL that is too long for a lookup request. This option is disabled by default.
Allow Mode	To enable the router to enter allow mode when the router cannot connect to any of the URL filtering servers in the server list, check **Allow Mode**. When the router is in Allow mode, all HTTP requests are allowed to pass if the router cannot connect to any server in the URL filter server list. Allow mode is disabled by default
Block Page	Optional Field. Enter the message that is to be displayed to users when the server blocks a requested page. For example, you might enter the message "This page not allowed."

Content Filter Websense Parameter Map List

In this screen, review configured Websense parameter maps, and display dialogs that enable you to create and edit parameter maps.

How to get to this screen

In the navigation panel, click **Configure > Security > Web Filter Configuration > Content Filtering Components > Parameter Map > URLF-Websense.**

Related Links

- Add or Edit Websense Parameter Map

Field Reference

Table 40-43 Websense Parameter Map List

Element	Description
Content Filter Websense Parameter Map	
Parameter Map Name	This column lists the names of the configured parameter maps.
Used By	This column displays the class maps that use the parameter map.

Table 40-43 Websense Parameter Map List (continued)

Element	Description
Details of Websense Parameter Map	

Item Name And Item Value	These columns contain the configuration parameters and values for the selected parameter map. For example, parameter map details might be the following:
	`Content Filter WS-pmap1`
	`Allow Mode false`
	`Content Filter Alert true`
	`Content Filter Server Log true`
	`Truncate true*`
	`Cache Size 5000`
	`Cache Entry Lifetime 24`
	`Maximum Buffered HTTP Requests 1000`
	`Maximum Buffered HTTP Responses 200`
	`Source Interface GigabitEthernet 0/0`
	* The Truncate setting is added automatically. URLs are truncated at the end of the domain name.

Add or Edit Websense Parameter Map

In this screen, create or edit a Websense parameter map.

How to get to this screen

In the navigation panel, click **Configure > Security > Web Filter Configuration > Content Filtering Components > Parameter Map > URLF-Websense.> Add** or **Edit**.

Related Links

- Content Filter Websense Parameter Map List

Field Reference

Table 40-44 Websense Parameter Map

Element	Description
Content Filter	Enter a name for this parameter map.

Table 40-44 Websense Parameter Map (continued)

Element	Description
Allow Mode	To enable the router to enter allow mode when the router cannot connect to any of the URL filtering servers in the server list, check **Allow Mode**. When the router is in Allow mode, all HTTP requests are allowed to pass if the router cannot connect to any server in the URL filter server list. Allow mode is disabled by default
Content Filter Alert	To enable the router to log content filtering alert messages, check **Content Filter Alert**. Content filtering alert messages report events such as a URL filtering server going down, or an HTTP request containing a URL that is too long for a lookup request. This option is disabled by default.
Content Filter Server Log	To enable the router to record system messages that pertain to the URL filter server in the log, check **Content Filter Server Log**. This option is disabled by default.
Cache Size	To set the maximum size of the cache that stores the most recently-requested IP addresses and their respective authorization status, enter the number of bytes for the cache size in this field. The default size of this cache is 5000 bytes. The range is from 0 bytes to 2147483647. The cache is cleared every 12 hours.
Cache Entry Lifetime	Enter the number of seconds that a record can remain in the cache.
Maximum Buffered HTTP Requests	You can set the maximum number of outstanding HTTP requests that the router can buffer. By default, the router buffers up to 1000 requests. You can specify from 1 to 2147483647 requests.
Maximum Buffered HTTP Responses	You can set the number of HTTP responses from the URL filtering server that the router can buffer. After this number is reached, the router drops additional responses. The default value is 200. You can set a value from 0 to 20000.
Source Interface	From this list, choose the interface from which the router is to receive data from the content filter server.
Reset Settings	To return the settings in this screen to their default values, click **Reset Settings**.

Content Filter N2H2 Parameter Map List

In this screen, review the N2H2 parameter maps, and display dialogs that enable you to create and edit N2H2 parameter maps.

How to get to this screen

In the navigation panel, click **Configure > Security > Web Filter Configuration > Content Filtering Components > Parameter Map > URLF-N2H2**.

Related Links

- Add or Edit N2H2 Parameter Map

Field Reference

Table 40-45 N2H2 Parameter Map List

Element	Description
Content Filter N2H2 Parameter Map	
Parameter Map Name	This column lists the names of the configured parameter maps.
Used By	This column displays the class maps that use the parameter map.
Add	To create a new parameter map, click **Add** and enter the information for the parameter map in the displayed dialog.
Edit	To edit an existing parameter map, select the parameter map, click **Edit** and modify the information for the parameter map in the displayed dialog.
Delete	To remove a parameter map, select the parameter map, and click **Delete**.
Details of Parameter Map	

Item Name and Item Value	These columns contain the configuration parameters and values for the selected parameter map. For example, parameter map details might be the following:
	`Content Filter N2H2-pmap1`
	`Allow Mode false`
	`Content Filter Alert true`
	`Content Filter Server Log true`
	`Truncate true*`
	`Cache Size 5000`
	`Cache Entry Lifetime 24`
	`Maximum Buffered HTTP Requests 1000`
	`Maximum Buffered HTTP Responses 200`
	`Source Interface GigabitEthernet 0/0`
	* The Truncate setting is added automatically. URLs are truncated at the end of the domain name.

Add or Edit N2H2 Parameter Map

In this screen, create or modify an N2H2 parameter map.

How to get to this screen

In the navigation panel, click **Configure > Security > Web Filter Configuration > Content Filtering Components > Parameter Map > URLF-N2H2 > Add or Edit**.

Related Links

- Configuring or Editing URL Filter Parameter Maps
- Content Filter N2H2 Parameter Map List

Field Reference

Table 40-46 N2H2 Parameter Map

Element	Description
Content Filter	Enter a name for this parameter map.
Allow Mode	To enable the router to enter Allow mode when the router cannot connect to any of the URL filtering servers in the server list, check **Allow Mode**. When the router is in Allow mode, all HTTP requests are allowed to pass if the router cannot connect to any server in the URL filter server list. Allow mode is disabled by default.
Content Filter Alert	To enable the router to log content filtering alert messages, check **Content Filter Alert**. Content filtering alert messages report events such as a URL filtering server going down, or an HTTP request containing a URL that is too long for a lookup request. This option is disabled by default.
Content Filter Server Log	To enable the router to record system messages that pertain to the URL filter server in the log, check **Content Filter Server Log**. This option is disabled by default.
Cache Size	To set the maximum size of the cache that stores the most recently-requested IP addresses and their respective authorization status, enter the number of bytes for the cache size in this field. The default size of this cache is 5000 bytes. The range is from 0 to 2147483647. The cache is cleared every 12 hours.

Table 40-46 N2H2 Parameter Map (continued)

Element	Description
Cache Entry Lifetime	Enter the number of hours that a record can remain in the cache. The default is 24.
Maximum Buffered HTTP Requests	You can set the maximum number of outstanding HTTP requests that the router can buffer. By default, the router buffers up to 1000 requests. You can specify from 1 to 2147483647.
Maximum Buffered HTTP Responses	You can set the number of HTTP responses from the URL filtering server that the router can buffer. After this number is reached, the router drops additional responses. The default value is 200. You can set a value from 0 to 20000.
Source Interface	From this list, choose the interface from which the router is to receive data from the content filter server.
Reset Settings	To return the settings in this screen to their default values, click **Reset Settings**.

Content Filter Trend Global Parameter Map List

In this screen, review the global Trend Micro parameter map and display dialogs to create and edit the global parameter map.

Note Only one global parameter map can be configured.

How to get to this screen

In the navigation panel, click **Configure > Security > Web Filter Configuration > Content Filtering Components > Parameter Map > URLF-TrendGlobal**.

Related Links

- Configuring or Editing URL Filter Parameter Maps
- Add or Edit Trend Global Parameter Map

Field Reference

Table 40-47 Trend Global Parameter Map List

Element	Description
Parameter Map Name	This column lists the names of the configured parameter maps.
Used By	This column displays the class maps that use the parameter map.
Add	To create a new parameter map, click **Add** and enter the information for the parameter map in the displayed dialog.
Edit	To edit an existing parameter map, select the parameter map, click **Edit** and modify the information for the parameter map in the displayed dialog.
Delete	To remove a parameter map, select the parameter map, and click **Delete**.
Details of Parameter Map	

Item Name and Item Value	These columns contain the configuration parameters and values for the selected parameter map. For example, parameter map details might be the following:
	`Server IP Address 192.168.5.4`
	`HTTP Port 80`
	`HTTPS Port 443`
	`Retransmission Count 5`
	`Timeout 10`
	`Cache Size Maximum Memory 256`
	`Cache Entry Lifetime 24`

Add or Edit Trend Global Parameter Map

In this screen, create or edit the Trend Micro global parameter map. The global parameter map specifies the IP address of the server, port numbers, transmission settings, and cache capacities.

How to get to this screen

In the navigation panel, click **Configure > Security > Web Filter Configuration > Content Filtering Components > Parameter Map > URLF-TrendGlobal > Add** or **Edit.**

Related Links

- Configuring or Editing URL Filter Parameter Maps
- Add or Edit Trend Global Parameter Map

Field Reference

Table 40-48 Trend Global Parameter Map

Element	Description
Server IP Address	Enter the IP address of the server.
HTTP Port	Enter the port number to use for HTTP communication. The default port number is 80.
HTTPS Port	Enter the port number to use for HTTPS communication. The default port number is 443.
Retransmission Count	Enter the number of times that the Cisco IOS Content Filtering service should send a request to the server when no response is received.
Timeout	Enter the number of seconds that the Cisco IOS Content Filtering Service is to wait for a response from the server.
Cache Size Maximum Memory	Enter the size, in kilobytes, of the cache that holds responses from the server. The default value is 256.
Cache Entry Lifetime	Enter the number of hours that a server response is to be held in the cache. The default is 24 hours. Holding responses in the cache reduces the number of times that the Cisco IOS Content Filtering service must contact the server.

Content Filter Trend Parameter Map List

In this screen, review configured Trend parameter maps, and display dialogs to create and edit parameter maps.

How to get to this screen

In the navigation panel, click **Configure > Security > Web Filter Configuration > Content Filtering Components > Parameter Map > URLF-Trend**.

Related Links

- Configuring or Editing URL Filter Parameter Maps
- Add or Edit Trend Global Parameter Map

Field Reference

Table 40-49 Trend Parameter Map List

Element	Description
Add	To create a new parameter map, click **Add** and enter the information for the parameter map in the displayed dialog.
Edit	To edit an existing parameter map, select the parameter map, click **Edit** and modify the information for the parameter map in the displayed dialog.
Delete	To remove a parameter map, select the parameter map, and click **Delete**.
Parameter Map Name	This column contains the names of the configured parameter maps.
Used By	This column contains the names of the class maps that use the parameter map.
Details of Trend Global Parameter Map	

Item Name and Item Value	These columns contain the configuration parameters and values for the selected parameter map. For example, parameter map details might be the following:
	`Allow Mode false`
	`Truncate true*`
	`Block Page This page not allowed`
	`Max Requests 1000`
	`Max Resp PAK 200`
	* The Truncate setting is added automatically. URLs are truncated at the end of the domain name.

Add or Edit Trend Parameter Map

In this screen, create a new Trend parameter map, or edit an existing one.

How to get to this screen

In the navigation panel, click **Configure > Security > Web Filter Configuration > Content Filtering Components > Parameter Map > URLF-Trend > Add** or **Edit**.

Related Links

- Configuring or Editing URL Filter Parameter Maps
- Content Filter Trend Global Parameter Map List

Field Reference

Table 40-50 Trend Parameter Map

Element	Description
URL Filter Name	In this field, enter a name for the URL filter.
Allow Mode	To enable the router to enter Allow mode when the router cannot connect to any of the URL filtering servers in the server list, check **Allow Mode**. When the router is in Allow mode, all HTTP requests are allowed to pass if the router cannot connect to any server in the URL filter server list. Allow mode is disabled by default.
Message and URL radio buttons	Contains two radio buttons: • Message—This option is selected by default. If you choose the **Message** radio button, enter the message that you want displayed when the content filter blocks a requested page. For example, enter "This page is not allowed." • URL—If you choose the **URL** radio button, enter the URL of a specific server to which you want to redirect the router when the content filter blocks a requested web address.
Maximum Requests	Optional field. The value you enter in this field specifies the maximum number of pending URL requests. The range is from 1 to 2147483647. The default is 1000.
Maximum Resp-PAK	Optional field. The value you enter in this field specifies the number of HTTP responses that can be buffered. The range is from 0 and 20000. The default is 200.

Content Filter Glob Parameter Map List

In this screen, review configured glob parameter maps, and display dialogs that enable you to create and edit glob parameter maps. URL filtering glob parameter maps are used to specify keywords that, when found in domain names, can be used to block them.

How to get to this screen

In the navigation panel, click **Configure > Security > Web Filter Configuration > Content Filtering Components > Parameter Map > URLF-Glob**.

Related Links

- Configuring or Editing URL Filter Parameter Maps
- Content Filter Glob Parameter Map List

Field Reference

Table 40-51 Glob Parameter Map List

Element	Description
URL Filtering Glob Parameter Maps	
URL Filtering Glob Parameter Name	This column lists the user-specified or system generated names of glob parameter maps. If a keyword list has been created using the Create Content Filter wizard or the Keyword Blocking screen, a system-generated name is used, and the list appears in this screen.
Used By	This column displays the class maps that use the parameter map.
Add	To create a new parameter map, click **Add** and enter the information for the parameter map in the displayed dialog.
Edit	To edit an existing parameter map, select the parameter map, click **Edit** and modify the information for the parameter map in the displayed dialog.
Delete	To remove a parameter map, select the parameter map, and click **Delete**.
Details of Parameter Map	

Item Name And Item Value	These columns contain the configuration parameters and values for the selected parameter map. For example, parameter map details might be the following:
	`1 adult`
	`2 broker*`
	`3 cards`
	`4 firearm`

Add or Edit Regular Expression

In this screen, create or edit a regular expression list.

How to get to this screen

In the navigation panel, click **Configure > Security > Web Filter Configuration > Content Filtering Components > Parameter Map > URLF-Glob > Add** or **Edit**.

Related Links

- Content Filter Glob Parameter Map List

Field Reference

Table 40-52 Glob Parameter Map

Element	Description
Name	In this field, enter the name of a parameter map. If you are editing a parameter map, this field is read only.
Pattern List	
Number	This column contains an automatically-assigned number given to the pattern. This number simply indicates the order of the pattern in the list. It cannot be edited.
Pattern	This column lists the text of each pattern.
Add	To create a new pattern, click **Add** and enter the pattern in the displayed dialog.
Edit	To edit an existing pattern, select the pattern, click **Edit** and modify the pattern in the displayed dialog.
Delete	To remove a pattern, select the pattern, and click **Delete**.
Copy Pattern	To copy a pattern from another parameter map into the list, click **Copy Pattern**. Then, click the parameter map that contains the pattern that you want to copy, choose the pattern, and click **OK**. The pattern is copied into the list.

Add or Edit Pattern

In this screen, create or edit a pattern for inclusion in a pattern list.

How to get to this screen

In the navigation panel, click **Configure > Security > Web Filter Configuration > Content Filtering Components > Parameter Map > URLF-Glob > Add** or **Edit > Add** or **Edit.**

Related Links

- Add or Edit Regular Expression

Field Reference

Table 40-53 Add Pattern

Element	Description
Pattern	In this field enter the pattern that you want to include in a pattern list. You can include the wildcard character so that patterns based on the text that you enter are found. For example, if you enter the text broker*, the word brokerage will also be a match.

Additional Information

This section contains the following parts:

- Content Filtering is Not Available

Content Filtering is Not Available

This screen is displayed when the Content Filtering feature is not available. This feature may not be available because the Cisco IOS image on the router does not support Content Filtering, or because necessary parts of the router configuration, such as a firewall configuration, are not present.

CHAPTER 41

Cisco IOS IPS

The Cisco IOS Intrusion Prevention System (Cisco IOS IPS) allows you to manage intrusion prevention on routers that use Cisco IOS Release 12.3(8)T4 or later releases. Cisco IOS IPS lets you monitor and prevent intrusions by comparing traffic against signatures of known threats and blocking the traffic when a threat is detected.

Cisco CP lets you control the application of Cisco IOS IPS on interfaces, import and edit signature definition files (SDF) from Cisco.com, and configure the action that Cisco IOS IPS is to take if a threat is detected.

IPS Tabs

Use the tabs at the top of the IPS window to go to the area where you need to work.

- Create IPS—Click to go to the IPS Rule wizard to create a new Cisco IOS IPS rule.
- Edit IPS—Click to edit Cisco IOS IPS rules and apply or remove them from interfaces.
- Security Dashboard—Click to view the Top Threats table and deploy signatures associated with those threats.
- IPS Migration—If the router runs a Cisco IOS image of release 12.4(11)T or later, you can migrate Cisco IOS IPS configurations created using earlier versions of the Cisco IOS.

IPS Rules

A Cisco IOS IPS rule specifies an interface, the type and direction of traffic that it is to examine, and the location of the signature definition file (SDF) that the router uses.

Create IPS

In this window you can download the Cisco IOS IPS License and launch the IPS Rule wizard.

Note The Cisco IOS IPS license is available on Cisco routers running Cisco IOS Release 15.0 and Cisco IOS Release 15.0M. If you do not activate the license, installation of advanced signature packages will fail. Other signature packages can be installed without the license.

The Activate License link is displayed if the Cisco IOS IPS License is not installed on your router. Click **Activate License** to install the license**.**

The IPS Rule wizard prompts you for the following information:

- The interface on which to apply the rule
- The traffic on which to apply Cisco IOS IPS (inbound, outbound, or both)
- The location of the signature definition file (SDF)

For Cisco IOS 12.4(11) or later images, you are also prompted for the following information:

- Where you want to store files that contain changes to the Cisco IOS IPS configuration. A file that stores this type of information is referred to as a delta file.
- The public key to use to access the information in the delta files.
- The signature category. The basic signature category is appropriate for routers with less than 128 Mb of flash memory. The advanced signature category is appropriate for routers with more than 128 Mb of flash memory.

The use case scenario illustrates a configuration in which a Cisco IOS IPS rule is used. After you create the Cisco IOS IPS rule and deliver the configuration to the router, you can modify the rule by clicking the **Edit IPS** tab.

To configure the IPS rule specifications, click the **Launch IPS Rule Wizard** button.

For more information on Cisco IOS IPS, see:

http://www.cisco.com/en/US/products/ps6634/prod_white_papers_list.html

Create IPS: Welcome

This window provides a summary of the tasks to perform when you complete the IPS Rule wizard.

Click **Next** to begin configuring a Cisco IOS IPS rule.

Create IPS: Select Interfaces

Choose the interfaces on which you want to apply the Cisco IOS IPS rule by specifying whether the rule is to be applied to inbound traffic or outbound traffic. If you check both the inbound and the outbound boxes, the rule applies to traffic flowing in both directions.

For example: the following settings apply Cisco IOS IPS to inbound traffic on the BRI 0 interface, and both inbound and outbound traffic on the FastEthernet 0 interface.

Interface Name	Inbound	Outbound
BRI 0	Check	—
FastEthernet 0	Check	Check

Create IPS: SDF Location

Note The Create IPS: SDF Location page is displayed on Cisco routers that are running Cisco IOS Release 12.4(9)T and earlier releases.

Cisco IOS IPS examines traffic by comparing it against signatures contained in a signature definition file (SDF). The SDF can be located in router flash memory or on a remote system that the router can reach. You can specify multiple SDF locations so that if the router is not able to contact the first location, it can attempt to contact other locations until it obtains an SDF.

Use the **Add**, **Delete**, **Move Up**, and **Move Down** buttons to add, remove, and order a list of SDF locations that the router can attempt to contact to obtain an SDF. The router starts at the first entry, and works down the list until it obtains an SDF.

Cisco IOS images that support Cisco IOS IPS contain built-in signatures. If you check the box at the bottom of the window, the router will use the built-in signatures only if it cannot obtain an SDF from any location in the list.

Create IPS: Signature File

The Cisco IOS IPS signature file contains the default signature information present in each update to the file on Cisco.com. Any changes made to this configuration are saved in a delta file. For security, the delta file must be digitally signed. Specify the location of the signature file and provide the name and text of the public key that will be used to sign the delta file in this window.

This help topic describes the Signature File window that is displayed when the router runs Cisco IOS 12.4(11)T and later releases.

Specify the signature file you want to use with IOS IPS

If the signature file is already present on the PC, router flash memory, or on a remote system, click **Specify the signature file you want to use with IOS IPS** to display a dialog in which you can specify the signature file location.

Get the latest signature file from CCO and save to PC

Click **Get the latest signature file from CCO and save to PC** if the signature file is not yet present on the PC or in router flash memory. Click **Browse** to specify where to save the signature file, and then click **Download** to begin downloading the file. Cisco CP downloads the signature file to the location that you specify.

Note If you did not activate the IOS IPS License, as described in Create IPS, page 41-2, the installation of advanced signature packages will fail. Other signature packages can be installed without the license. The IOS IPS license is available on Cisco routers running Cisco IOS Release 15.0 and Cisco IOS Release 15.0M.

Configure Public Key

Each change to the signature configuration is saved in the delta file. This file must be digitally signed with a public key. You can obtain a key from Cisco.com and paste the information in the Name and Key fields.

Note If you have already added a public key to the configuration using the Cisco IOS CLI, you must still provide a public key in this screen. After you have completed the Cisco IOS IPS Rule Wizard, you can go to **Edit IPS > Global Settings**. In the Global Settings screen, you can click **Edit** in the Edit IPS Prerequisites area, and then click **Public Key** to display the Public Key dialog. In that dialog, you can delete public keys that you do not need.

Follow these steps to place the public-key information in the Name and Key fields.

Step 1 Go to the following link to obtain the public key:

http://www.cisco.com/pcgi-bin/tablebuild.pl/ios-v5sigup

Step 2 Download the key to your PC.

Step 3 Copy the text after the phrase “named-key” into the Name field. For example, if the line of text including the name is the following:

```
named-key realm-cisco.pub signature
```

copy `realm-cisco.pub` to the Name field.

Step 4 Copy the text between the phrase **`key-string`**, and the word **`quit`** into the Key field. For example:

```
30820122 300D0609 2A864886 F70D0101 01050003 82010F00 3082010A 02820101
00C19E93 A8AF124A D6CC7A24 5097A975 206BE3A2 06FBA13F 6F12CB5B 4E441F16
17E630D5 C02AC252 912BE27F 37FDD9C8 11FC7AF7 DCDD81D9 43CDABC3 6007D128
B199ABCB D34ED0F9 085FADC1 359C189E F30AF10A C0EFB624 7E0764BF 3E53053E
5B2146A9 D7A5EDE3 0298AF03 DED7A5B8 9479039D 20F30663 9AC64B93 C0112A35
FE3F0C87 89BCB7BB 994AE74C FA9E481D F65875D6 85EAF974 6D9CC8E3 F0B08B85
```

```
50437722 FFBE85B9 5E4189FF CC189CB9 69C46F9C A84DFBA5 7A0AF99E AD768C36
006CF498 079F88F8 A3B3FB1F 9FB7B3CB 5539E1D1 9693CCBB 551F78D2 892356AE
2F56D826 8918EF3C 80CA4F4D 87BFCA3B BFF668E9 689782A5 CF31CB6E B4B094D3
F3020301 0001
```

Create IPS: Configuration File Location and Category

Specify a location for storing the signature information that the Cisco IOS IPS will use. This information consists of the signature file and the delta file that is created when changes are made to the signature information.

This help topic describes the Configuration File Location window that is displayed when the router runs Cisco IOS 12.4(11)T and later releases.

Config Location

Click the button to the right of the Config Location field to display a dialog box that allows you to specify a location. After you enter information in that dialog box, Cisco CP displays the path to the location in this field.

Choose Category

Because router memory and resource constraints may prevent the use of all the available signatures, there are two categories of signatures—**basic** and **advanced**. In the Choose Category field, choose the category that will allow the Cisco IOS IPS to function efficiently on the router. The basic category is appropriate for routers with less than 128 MB of available flash memory. The advanced category is appropriate for routers with more than 128 MB of available flash memory.

Add or Edit a Config Location

Specify a location for storing the signature information and the delta file that the Cisco IOS IPS will use.

Specify config location on this router

To specify a location on the router, click the button to the right of the Directory Name field and choose the directory in which you want to store the configuration information.

Note If the router has a LEFS-based file system, you cannot create a directory in router memory. In that case, **flash:** is used as the config location.

Specify config location using URL

To specify a location on a remote system, specify the protocol and path of the URL needed to reach the location. For example, if you want to specify the URL http://172.27.108.5/ips-cfg, enter 172.27.108.5/ips-cfg.

Note Do not include the protocol in the path that you enter. Cisco CP adds the protocol automatically. If you enter the protocol, Cisco CP displays an error message.

In the No. of Retries and Timeout fields**,** specify how many times the router is to attempt to contact the remote system, and how long the router is to wait for a response before stopping the contacting attempts.

Directory Selection

Click the folder in which you want to store configuration information. If you want to create a new folder, click **New Folder**, provide a name for it in the dialog displayed, select it, and click **OK**.

Signature File

Specify the location of the signature file that the Cisco IOS IPS will use.

Note If you did not activate the IOS IPS License, as given in Create IPS, page 41-2, installation of advanced signature packages will fail. Other signature packages can be installed without the license. The IOS IPS license is available on Cisco routers running Cisco IOS Release 15.0 and Cisco IOS Release 15.0M.

Specify Signature File on Flash

If the signature file is located on router flash memory, click the button to the right of the field. Cisco CP displays the signature file names of the correct format.

Specify Signature File using URL

If the signature file is located on a remote system, select the protocol to be used, and enter the path to the file. For example, if the signature file IOS-S259-CLI.pkg is located at 10.10.10.5, and the FTP protocol will be used, select **ftp** as the protocol, and enter

```
10.10.10.5/IOS-S259-CLI.pkg
```

Note Do not include the protocol in the path that you enter. Cisco CP adds the protocol automatically. If you enter the protocol, Cisco CP displays an error message. Additionally, when you use an URL, you must specify a filename that conforms to the IOS-Snnn-CLI.pkg file naming convention, such as the file used in the previous example.

Specify Signature File on PC

If the signature file is located on the PC, click **Browse**, navigate to the folder containing the file, and select the filename. You must choose an Cisco CP-specific package of the format sigv5-SDM-S*xxx*.zip; for example, sigv5-SDM-S260.zip.

Create IPS: Summary

The following is an example of a Cisco IOS IPS summary display on a router running a Cisco IOS release earlier than 121.4(11)T.

```
Selected Interface: FastEthernet 0/1

IPS Scanning Direction: Both

Signature Definition File Location: flash//sdmips.sdf

Built-in enabled: yes
```

In this example, Cisco IOS IPS is enabled on the FastEthernet 0/1 interface, and both inbound and outbound traffic is scanned. The SDF is named sdmips.sdf and is located in router flash memory. The router is configured to use the signature definitions built in to the Cisco IOS image that the router uses.

Create IPS: Summary

The Summary window displays the information that you have entered so that you can review it before delivering the changes to the router.

This help topic describes the Summary window that is displayed when the router runs Cisco IOS 12.4(11)T and later releases. A sample Summary window display follows.

In this example, the Cisco IOS IPS policy is applied to the FastEthernet 0/0 and the FastEthernet 0/1 interfaces. The signature file is located on the PC. The config location is on router flash memory, in a directory named configloc.

```
IPS rule will be applied to the outgoing traffic on the following interfaces.
     FastEthernet0/1
IPS rule will be applied to the incoming traffic on the following interfaces.
     FastEthernet0/0
Signature File location:
     C:\SDM-Test-folder\sigv5-SDM-S260.zip
Public Key:
       30819F30 0D06092A 864886F7 0D010101 05000381 8D003081 89028181 00B8BE84
  33251FA8 F79E393B B2341A13 CAFFC5E6 D5B3645E 7618398A EFB0AC74 11705BEA
  93A96425 CF579F1C EA6A5F29 310F7A09 46737447 27D13206 F47658C7 885E9732
  CAD15023 619FCE8A D3A2BCD1 0ADA4D88 3CBD93DB 265E317E 73BE085E AD5B1A95
  59D8438D 5377CB6A AC5D5EDC 04993A74 53C3A058 8F2A8642 F7803424 9B020301 0001

Config Location
     flash:/configloc/
Selected category of signatures:
     advanced
```

In this example, the Cisco IOS IPS policy is applied to the FastEthernet 0/0 and the FastEthernet 0/1 interfaces. The signature file is located on the PC. The config location is on router flash memory, in a directory named configloc.

Edit IPS

In this window you can view the Cisco IOS IPS buttons for configuring and managing Cisco IOS IPS policies, security messages, signatures, and more.

IPS Policies Button

Click the IPS Policies button display the Edit IPS window. You can enable or disable Cisco IOS IPS on an interface and view information about how Cisco IOS IPS is applied. If you enable Cisco IOS IPS on an interface, you can specify which traffic to examine for intrusion.

Global Settings Button

Click the Global Settings button to display the Edit IPS: Global Settings window. You can make settings that affect the overall operation of Cisco IOS IPS.

Download Button

Click the Download button to download a signature package from Cisco.com to your PC and then send it to the router. You can either download the latest signature package, or you can specify the package from a list of available packages. See Edit IPS: Download.

Auto Update Button

Click the Auto Update button to configure the router to automatically download the IPS signature package from a specified local server at periodic intervals. See Edit IPS: Auto Update.

SEAP Configuration Button

Click the SEAP Configuration button for advanced filtering and overrides. Signature Event Action Processing (SEAP) gives you greater control over IOS IPS by providing advanced filtering and overrides. This button appears if the Cisco IOS image on the router is version 12.4(11)T or later.

SDEE Messages Button

Click the SDEE Messages button to display the Edit IPS: SDEE Messages window, where you can review SDEE messages and filter them to display only error, status, or alert messages. Secure Device Event Exchange (SDEE) messages report on the progress of Cisco IOS IPS initialization and operation.

Signatures Button

Click the Signatures button to display the Edit IPS: Signatures window where you can manage signatures on the router.

NM CIDS Button

Click the NM CIDS button to manage the IDS module. This button is visible if a Cisco Intrusion Detection System network module is installed in the router.

Edit IPS: IPS Policies

This window displays the Cisco IOS IPS status of all router interfaces, and allows you to enable and disable Cisco IOS IPS on interfaces.

Interfaces

Use this list to filter the interfaces shown in the interface list area. Choose one of the following:

- All interfaces—All interfaces on the router.
- IPS interfaces—Interfaces on which Cisco IOS IPS has been enabled.

Enable Button

Click the Enable button to enable Cisco IOS IPS on the specified interface. You can specify the traffic directions to which Cisco IOS IPS is to be applied, and the ACLs used to define the type of traffic you want to examine. See Enable or Edit IPS on an Interface for more information.

Edit Button

Click the Edit button to edit the Cisco IOS IPS characteristics applied to the specified interface.

Disable Button

Click the Disable button to disable Cisco IOS IPS on the specified interface. A context menu shows you the traffic directions on which Cisco IOS IPS has been applied, and you can choose the direction on which you want to disable Cisco IOS IPS. If you disable Cisco IOS IPS on an interface to which it has been applied, Cisco CP dissociates any Cisco IOS IPS rules from that interface.

Disable All Button

Click the Disable All button to disable Cisco IOS IPS on all interfaces on which it has been enabled. If you disable Cisco IOS IPS on an interface to which it has been applied, Cisco CP dissociates any Cisco IOS IPS rules from that interface.

Interface Name

The name of the interface. For example: Serial0/0, or FE0/1.

IP

This column can contain the following types of IP addresses:

- Configured IP address of the interface.
- DHCP client—The interface receives an IP address from a Dynamic Host Configuration Protocol (DHCP) server.
- Negotiated—The interface receives an IP address through negotiation with the remote device.
- Unnumbered—The router uses one of a pool of IP addresses supplied by your service provider for your router and for the devices on your LAN.
- Not applicable—The interface type cannot be assigned an IP address.

Inbound IPS/Outbound IPS

The Inbound and Outbound columns show whether IPS is enabled or disabled:

- Enabled—Cisco IOS IPS is enabled for this traffic direction.
- Disabled—Cisco IOS IPS is disabled for this traffic direction.

VFR Status

Virtual Fragment Reassembly (VFR) status. The possible values are:

- On—VFR is enabled.
- Off—VFR is disabled.

Cisco IOS IPS cannot identify the contents of IP fragments, nor can it gather port information from the fragment to match it with a signature. Therefore, fragments can pass through the network without being examined or without dynamic access control list (ACL) creation.

VFR enables the Cisco IOS Firewall to create the appropriate dynamic ACLs, thereby protecting the network from various fragmentation attacks.

Description

The Description column displays a description of the connection, if added.

IPS Filter Details

If no filter is applied to traffic, this area contains no entries. If a filter is applied, the name or number of the ACL is shown in parentheses.

Inbound and Outbound Filter Buttons

Click to view the entries of the filter applied to inbound or outbound traffic.

Field Descriptions

Action—Whether the traffic is permitted or denied.

 Permit source traffic.

 Deny source traffic.

Source—Network or host address, or any host or network.

Destination—Network or host address, or any host or network.

Service—Type of service filtered: IP, TCP, UDP, IGMP, or ICMP.

Log—Whether or not denied traffic is logged.

Attributes—Options configured using the CLI.

Description—Any description provided.

Enable or Edit IPS on an Interface

Use this window to choose the interfaces on which you want to enable intrusion detection, and to specify the IPS filters for examining traffic.

Both, Inbound, and Outbound Buttons

Use the Both, Inbound, or Outbound buttons to specify whether you are going to enable Cisco IOS IPS on both inbound and outbound traffic, only inbound traffic, or only outbound traffic.

Inbound Filter

[Optional] Enter the name or number of the access rule that specifies the inbound traffic to be examined. The ACL name that you specify appears in the IPS filter Details area next to the Inbound Filter button when the interface with which it is associated is chosen. If you need to browse for the access rule or create a new one, click the **...** button.

Outbound Filter

[Optional] Enter the name or number of the access rule that specifies the outbound traffic to be examined. The ACL name that you specify appears in the IPS filter Details area next to the Outbound Filter button when the interface with which it is associated is chosen. If you need to browse for the access rule or create a new one, click the **...** button.

... Button

Use this button to specify a filter. Click to display a menu with the following options:

- Select an existing rule. See Select a Rule for more information.
- Create a new rule and select. See Add or Edit a Rule for more information.
- None (clear rule association). Use this option to remove a filter from a traffic direction to which it has been applied.

Enable fragment checking for this interface

(Enabled by default). Check the checkbox if you want the Cisco IOS firewall to check for IP fragments on this interface. See VFR Status for more information.

Enable fragment checking on other interfaces

If fragment checking is enabled for outbound traffic, the router must examine the inbound traffic that arrives on the interfaces that send outbound traffic to the interface being configured. Specify these interfaces below.

If the Inbound radio button is chosen, this area does not appear.

Specify Signature File

The Specify Signature File box contains information about the SDF version that the router is using, and enables you to update the SDF to a more recent version. To specify a new SDF, click the **...** button next to the Signature File field and specify a new file in the displayed dialog.

Edit IPS: Global Settings

This window allows you to view and configure global settings for Cisco IPS. This help topic describes the information that you may see if the running Cisco IOS image is earlier than Cisco IOS Release 12.4(11)T.

Global Settings Table

This table in the Global Settings window displays the current global settings and their values. Click **Edit** to change any of these values.

Table 41-1 Global Settings Table

Item Name	Item Value
Syslog	If enabled, then notifications are sent to the syslog server specified in System Properties.
SDEE	Security Device Event Exchange. If enabled, SDEE events are generated.
SDEE Events	Number of SDEE events to store in the router buffer.
SDEE Subscription	Number of concurrent SDEE subscriptions.
Engine Options	The engine options are: • Fail Closed—By default, while the Cisco IOS compiles a new signature for a particular engine, it allows packets to pass through without scanning for the corresponding engine. When enabled, this option makes the Cisco IOS drop packets during the compilation process. • Use Built-in Signatures (as backup)—If Cisco IOS IPS does not find signatures or fails to load them from the specified locations, it can use the Cisco IOS built-in signatures to enable Cisco IOS IPS. This option is enabled by default. • Deny Action on IPS Interface—We recommend this when the router is performing load balancing. When enabled, this option causes Cisco IOS IPS to enable ACLs on Cisco IOS IPS interfaces instead of enabling them on the interfaces from which attack traffic came.
Shun Events	This option uses the Shun Time parameter. Shun Time is the amount of time that shun actions are to be in effect. A shun action occurs if a host or network is added to an ACL to deny traffic from that host or network.

Table 41-1 Global Settings Table

Item Name	Item Value
Syslog	If enabled, then notifications are sent to the syslog server specified in System Properties.
SDEE	Security Device Event Exchange. If enabled, SDEE events are generated.
SDEE Events	Number of SDEE events to store in the router buffer.
SDEE Subscription	Number of concurrent SDEE subscriptions.
Engine Options	The engine options are: • Fail Closed—By default, while the Cisco IOS compiles a new signature for a particular engine, it allows packets to pass through without scanning for the corresponding engine. When enabled, this option makes the Cisco IOS drop packets during the compilation process. • Use Built-in Signatures (as backup)—If Cisco IOS IPS does not find signatures or fails to load them from the specified locations, it can use the Cisco IOS built-in signatures to enable Cisco IOS IPS. This option is enabled by default. • Deny Action on IPS Interface—We recommend this when the router is performing load balancing. When enabled, this option causes Cisco IOS IPS to enable ACLs on Cisco IOS IPS interfaces instead of enabling them on the interfaces from which attack traffic came.
Shun Events	This option uses the Shun Time parameter. Shun Time is the amount of time that shun actions are to be in effect. A shun action occurs if a host or network is added to an ACL to deny traffic from that host or network.

Configured SDF Locations

A signature location is a URL that provides a path to an SDF. To find an SDF, the router attempts to contact the first location in the list. If it fails, it tries each subsequent location in turn until it finds an SDF.

Add Button

Click to add a URL to the list.

Edit Button

Click to edit a specified location.

Delete Button

Click to delete a specified location.

Move Up an d Move Down Buttons

Use to change the order of preference for the URLs in the list.

Reload Signatures

Click to recompile signatures in all signature engines. During the time that signatures are being recompiled in a signature engine, the Cisco IOS software cannot use the signatures of that engine to scan packets.

Edit Global Settings

The Edit settings that affect the overall operation of Cisco IOS IPS in this window, in the Syslog and SDEE and Global Engine tabs, are displayed.

Enable Syslog Notification (Syslog and SDEE Tab)

Check this check box to enable the router to send alarm, event, and error messages to a syslog server. A syslog server must be identified in System Properties for this notification method to work.

SDEE (Syslog and SDEE Tab)

Enter the number of concurrent SDEE subscriptions in the **Number of concurrent SDEE subscriptions** field. The range is 1-3. An SDEE subscription is a live feed of SDEE events.

In the **Maximum number of SDEE alerts to store** field, enter the maximum number of SDEE alerts that you want the router to store. The range is 10–2000. Storing more alerts uses more router memory.

In the **Maximum number of SDEE messages to store** field, enter the maximum number of SDEE messages that you want the router to store, in the range of 10–500. Storing more messages uses more router memory.

Enable Engine Fail Closed (Global Engine Tab)

By default, while the Cisco IOS software compiles a new signature for a particular engine, it allows packets to pass through without scanning for the corresponding engine. Enable this option to make the Cisco IOS software drop packets during the compilation process.

Use Built-in Signatures (as backup) (Global Engine Tab)

If Cisco IOS IPS does not find or fails to load signatures from the specified locations, it can use the Cisco IOS built-in signatures to enable Cisco IOS IPS. This option is enabled by default.

Enable Deny Action on IPS interface (Global Engine Tab)

This option is applicable if signature actions are configured to "denyAttackerInline" or "denyFlowInline." By default, Cisco IOS IPS applies ACLs to the interfaces from which attack traffic came, and not to Cisco IOS IPS interfaces. Enabling this option causes Cisco IOS IPS to apply the ACLs directly to the Cisco IOS IPS interfaces, and not to the interfaces that originally received the attack traffic. If the router is not performing load balancing, do not enable this setting. If the router is performing load balancing, we recommend that you enable this setting.

Timeout (Global Engine Tab)

This option lets you set the number of minutes that shun actions are to be in effect. The range is i0–65535. The default value is 30 minutes. A shun action occurs if a host or network is added to an ACL to deny traffic from that host or network.

Add or Edit a Signature Location

Specify the location from which Cisco IOS IPS should load an SDF. To specify multiple SDF locations, open this dialog again and enter the information for another SDF.

Specify SDF on this router

Specify the part of router memory in which the SDF is located by using the Location drop-down menu. For example, the menu could have the entries *disk0*, *usbflash1*, and *flash*. Choose the filename by clicking the down arrow next to the File Name field or enter the filename in the File Name field.

Specify SDF using URL

If the SDF is located on a remote system, you can specify the URL where it resides.

Protocol

Choose the protocol the router should use to obtain the SDF, such as *http* or *https*.

URL

Enter the URL in the following form:

path-to-signature-file

Note The protocol you chose from the Protocol menu appears to the right of the URL field. Do *not* reenter the protocol in the URL field.

The following URL is provided as an example of the format. It is *not* a valid URL to a signature file, and it includes the protocol to show the full URL:

`https://172.16.122.204/mysigs/vsensor.sdf`

Autosave

Check this option if you want the router to automatically save the SDF if the router crashes. This eliminates the need for you to reconfigure Cisco IOS IPS with this SDF when the router comes back up.

Edit IPS: SDEE Messages

This window lists the SDEE messages received by the router. SDEE messages are generated when there are changes to Cisco IOS IPS configuration.

SDEE Messages

Choose the SDEE message type to display:

- All—SDEE error, status, and alert messages are shown.
- Error—Only SDEE error messages are shown.
- Status—Only SDEE status messages are shown.
- Alerts—Only SDEE alert messages are shown.

View By

Choose the SDEE message field to search.

Criteria

Enter the search string.

Go Button

Click to initiate the search on the string entered in the Criteria field.

Type

Types are Error, Status, and Alerts. Click SDEE Message Text to see possible SDEE messages.

Time

Time message was received.

Description

Available description.

Refresh Button

Click to check for new SDEE messages.

Close Button

Click to close the SDEE Messages window.

SDEE Message Text

This topic lists possible SDEE messages.

IDS Status Messages

Error Message

```
ENGINE_BUILDING: %s - %d signatures - %d of %d engines
```

Explanation Triggered when Cisco IOS IPS begins building the signature microengine (SME).

Error Message

```
ENGINE_BUILD_SKIPPED: %s - there are no new signature
definitions for this engine
```

Explanation Triggered when there are no signature definitions or no changes to the existing signature definitions of an Intrusion Detection System SME.

Error Message

```
ENGINE_READY: %s - %d ms - packets for this engine will be
scanned
```

Explanation Triggered when an IDS SME is built and ready to scan packets.

Error Message

```
SDF_LOAD_SUCCESS: SDF loaded successfully from %s
```

Explanation Triggered when an SDF file is loaded successfully from a given location.

Error Message

```
BUILTIN_SIGS: %s to load builtin signatures
```

Explanation Triggered when the router resorts to loading the builtin signatures.

IDS Error Messages

Error Message

`ENGINE_BUILD_FAILED: %s - %d ms - engine build failed - %s`

Explanation Triggered when Cisco IOS IPS fails to build one of the engines after an SDF file is loaded. One message is sent for each failed engine. This means that the Cisco IOS IPS engine failed to import signatures for the specified engine in the message. Insufficient memory is the most probable cause of this problem. If this happens, the new imported signature that belongs to this engine is discarded by Cisco IOS IPS.

Error Message

`SDF_PARSE_FAILED: %s at Line %d Col %d Byte %d Len %d`

Explanation Triggered when an SDF file does not parse correctly.

Error Message

`SDF_LOAD_FAILED: failed to %s SDF from %s`

Explanation Triggered when an SDF file fails to load for some reason.

Error Message

`DISABLED: %s - IDS disabled`

Explanation IDS has been disabled. The message should indicate the cause.

Error Message

`SYSERROR: Unexpected error (%s) at line %d func %s() file %s`

Explanation Triggered when an unexpected internal system error occurs.

Edit IPS: Global Settings

Several Cisco IOS IPS configuration options are available with Cisco IOS 12.4(11)T and later images. These are described in this help topic. Screen controls and configuration options available prior to Cisco IOS 12.4(11)T, such as the Syslog and SDEE global settings are described in Edit IPS: Global Settings.

This help topic describes the Global Settings window that is displayed when the router runs Cisco IOS Release 12.4(11)T and later releases.

Engine Options

The engine options available with Cisco IOS Release 12.4(11)T and later releases are the following:

- Fail Closed—By default, while the Cisco IOS compiles a new signature for a particular engine, it allows packets to pass through without scanning for the corresponding engine. When enabled, this option makes the Cisco IOS drop packets during the compilation process.
- Deny Action on IPS Interface—We recommend this option when the router is performing load balancing. When enabled, this option causes Cisco IOS IPS to enable ACLs on Cisco IOS IPS interfaces instead of enabling them on the interfaces from which attack traffic came.

Edit IPS Prerequisites Table

This table displays the information about how the router is provisioned for Cisco IOS IPS. Click **Edit** to change any of these values. The sample data in the following table indicated that the config location is the directory configloc in flash memory, that the router is using the basic category of signatures, and that a public key has been configured to allow the router to access the information in the configloc directory.

Table 41-2 Edit IPS Prerequisites Table

Item Name	Item Value
Config Location	flash:/configloc/
Selected Category	basic
Public Key	Configured

Edit Global Settings Dialog Box

The Edit Global Settings dialog box contains a Syslog and SDEE tab, and a Global Engine tab. Click the link below for the information that you want to see:

- Syslog and SDEE Tab
- Global Engine Tab

Note If Signature Event Action Processing (SEAP) is configured, the tab is displayed. See Edit IPS: SEAP Configuration, page 41-35.

Syslog and SDEE Tab

The Syslog and SDEE dialog box is displayed when the router uses Cisco IOS Release 12.4(11)T or a later image. The Syslog and SDEE dialog box allows you to configure syslog notification and parameters for SDEE subscriptions, events, and messages.

Enable Syslog Notification

Check this check box to enable the router to send alarm, event, and error messages to a syslog server. A syslog server must be identified in System Properties for this notification method to work.

SDEE

Enter the number of concurrent SDEE subscriptions, in the range of 1–3, in the Number of concurrent SDEE subscriptions field. An SDEE subscription is a live feed of SDEE events.

In the Maximum number of SDEE alerts to store field, enter the maximum number of SDEE alerts that you want the router to store, in the range of 10–2000. Storing more alerts uses more router memory.

In the Maximum number of SDEE messages to store field, enter the maximum number of SDEE messages that you want the router to store, in the range of 10–500. Storing more messages uses more router memory.

Global Engine Tab

The Global Engine dialog displayed when the router uses a Cisco IOS 12.4(11)T or later image allows you to configure the settings described in the following sections.

Enable Engine Fail Closed

By default, while the Cisco IOS software compiles a new signature for a particular engine, it allows packets to pass through without scanning for the corresponding engine. Enable this option to make the Cisco IOS software drop packets during the compilation process.

Enable Deny Action on IPS interface

This option is applicable if signature actions are configured to "denyAttackerInline" or "denyFlowInline." By default, Cisco IOS IPS applies ACLs to the interfaces from which attack traffic came, and not to Cisco IOS IPS interfaces. Enabling this option causes Cisco IOS IPS to apply the ACLs directly to the Cisco IOS IPS interfaces, and not to the interfaces that originally received the attack traffic. If the router is not performing load balancing, do not enable this setting. If the router is performing load balancing, we recommend that you enable this setting.

Edit IPS Prerequisites Dialog Box

The Edit IPS Prerequisites dialog box contains tabs for the following categories:

- Config Location Tab
- Category Selection Tab
- Public Key Tab

Config Location Tab

If a config location has been configured on the router, you can edit it. If none has been configured, you can click Add and configure one. The Add button is disabled if a config location is already configured. The Edit button is disabled when no config location has been configured. See Create IPS: Configuration File Location and Category for more information.

Category Selection Tab

If you specify a signature category, Cisco CP configures the router with a subset of signatures appropriate for a specific amount of router memory. You can also remove an existing category configuration to remove category constraints when selecting signatures.

Configure Category

Click **Configure Category** and choose either **basic** or **advanced**. The basic category is appropriate for routers with less than 128 MB of available flash memory. The advanced category is appropriate for routers with more than 128 MB of available flash memory.

Delete Category

To remove the category configuration, click **Delete Category Configuration**.

Public Key Tab

This dialog displays the public keys configured for Cisco IOS IPS. You can add keys or delete keys from this dialog. To add a key, click **Add** and configure the key in the dialog displayed.

To remove a key, select the key name and click **Delete**.

Add Public Key

You can copy the name of the key and the key itself from:

http://www.cisco.com/pcgi-bin/tablebuild.pl/ios-v5sigup

Copy the key name and paste it into the Name field in this dialog. Then copy the key from the same location and paste it into the Key field. For detailed instructions that explain exactly which parts of the text to copy and paste, see Configure Public Key.

Edit IPS: Download

The Download IPS Signature Package feature allows you to download a signature package from Cisco.com to your PC and then send it to the router. You can either download the latest signature package or you can specify a package from a list of available packages.

Note The Download IPS Signature Package feature is supported on Cisco routers that are running Cisco IOS Release 12.4(11)T2 and later.

Note If you did not activate the Cisco IOS IPS License, as described in Create IPS, page 41-2, installation of advanced signature packages will fail. Other signature packages can be installed without the license. The Cisco IOS IPS license is available on Cisco routers running Cisco IOS Release 15.0 and Cisco IOS Release 15.0M.

This section contains the following topics:

- Downloading Signature Package from Cisco.com, page 41-29
- Downloading the Signature Package from Cisco.com Reference, page 41-31

Downloading Signature Package from Cisco.com

Procedure

Use this procedure to download a signature package from Cisco.com to your PC and then send it to the router. You can either download the latest signature package or you can specify the package that you want from a list of available packages.

Step 1 Enable IPS on the router.

Step 2 Specify a location in which to save the signature information. The signature information consists of the signature file and the delta file that is created when changes are made to the signature file.

Note If Steps 1 and 2 are not configured, you will see a warning message.

Step 3 From the Select Community Member drop-down list, choose the router to configure.

Step 4 Choose **Configure > Security > Intrusion Prevention**. The Intrusion Prevention System (IPS) page opens.

Step 5 From the Intrusion Prevention System (IPS) page, click the **Edit IPS** tab.

Step 6 Click the **Download** button. The Download Signature Package from Cisco.com page opens. See Downloading the Signature Package from Cisco.com Reference, page 41-31.

Step 7 To download the latest signature package, do the following:

a. Click the **Get the Latest Signature Package** radio button.

b. Click the **Browse** button (located next to the Download To field) to navigate to the directory in your PC where you want to save the signature package.

c. Click **Download**. The Cisco.com Credentials dialog box opens.

d. Enter your Cisco.com username and password, and then click **OK**. The signature package is downloaded to your PC, and a confirmation dialog box opens.

e. Click **Yes** in the confirmation dialog box to send the signature package from your PC to the router.

Step 8 To choose from a list of available signature packages, do the following:

a. Click the **List the Available Files to Download** radio button.

b. Click the **Refresh** button. The Cisco.com Credentials dialog box opens.

c. Enter your Cisco.com username and password, and then click **OK**.

d. From the List of Signature Packages drop-down list, choose the signature package that you want.

e. Click **Browse** to navigate to the directory in your PC where you want to save the signature package.

f. Click **Download**. The signature package downloads to your PC, and a confirmation dialog box opens.

g. Click **Yes** in the confirmation dialog box to send the signature package from your PC to the router.

Related Topics

- Edit IPS: Download, page 41-29
- Download the Signature Package from Cisco.com Page, page 41-31

Downloading the Signature Package from Cisco.com Reference

This section describes the pages you can use when working with the IPS Signature Download feature and includes the following topic:

- Download the Signature Package from Cisco.com Page, page 41-31

Download the Signature Package from Cisco.com Page

Use the Download Signature Package from Cisco.com Page to download the signature package from Cisco.com to your PC and then send it to the router.

How to Get to This Dialog Box

1. Choose **Configure > Security > Intrusion Prevention**. The Intrusion Prevention System (IPS) page opens.
2. From the Intrusion Prevention System (IPS) page, click the **Edit IPS** tab, and then click the **Download** button.

Related Topics

- Edit IPS: Download, page 41-29
- Downloading Signature Package from Cisco.com, page 41-29

Field Reference

Table 41-3 Download the Signature Package from Cisco.com Page

Element	Description
Get the Latest Signature Package radio button	Click this radio button to download the latest signature package from Cisco.com to your PC.
List the Available Files to Download radio button	Click this radio button to display a list of available signature packages.
Signature Package in Use	Displays the version of the signature package that the router is currently using.

Table 41-3 Download the Signature Package from Cisco.com Page

Element	Description
List of Signature Packages	Choose the signature package that you want from the drop-down list. **Note** The field is active only when you click the **List the Available Files to Download** radio button.
Refresh button	Click this button to browse the list of available signature packages.
Browse button	Click this button to navigate to the directory in your PC where you want to save the signature package.
Download To	Displays the directory on your PC where the signature package will be saved.
Download button	Click this button to open the Cisco.com credentials dialog box. After the Cisco.com credentials are verified, the signature package is saved on your PC. Click **Yes** in the confirmation dialog box to send the signature package from your PC to the router.

Edit IPS: Auto Update

The Auto Update IPS Signature Package feature allows you to configure the router to automatically download the IPS signature package from a specified local server at periodic intervals.

Note The Auto Update IPS Signature Package from Local Server feature is supported on Cisco routers that are running Cisco IOS Release 12.4(11)T2 and later.

This section contains the following topics:

- Automatically Updating IPS Signature Package from a Local Server, page 41-33
- Automatically Update IPS Signature Package Reference, page 41-34

Automatically Updating IPS Signature Package from a Local Server

Procedure

Use this procedure to configure the router to automatically download the IPS signature package from a specified local server at periodic intervals.

Step 1 Enable IPS on the router.

Step 2 Specify a location in which to save the signature information. This signature information consists of the signature file and the delta file that is created when changes are made to the signature file.

Note If Steps 1 and 2 are not configured, you will see a warning message.

Step 3 Configure the encryption key for password encryption.

Note If the encryption key is not configured, the Enter Encryption Key dialog box opens, and you can add the encryption key information.

Step 4 From the Select Community Member drop-down list, choose the router to configure.

Step 5 Choose **Configure > Security > Intrusion Prevention**. The Intrusion Prevention System (IPS) page opens.

Step 6 From the Intrusion Prevention System (IPS) page, click the **Edit IPS** tab.

Step 7 Click the **Auto Update** button. The Automatically Update IPS Signature Package page opens.

Step 8 From the Automatically Update IPS Signature Package page, choose the **Local Server** radio button.

Step 9 In the Login Information for Local Server pane, do the following:

a. Enter the username and password to log into the local server.

b. Enter the URL of the local server from which the signature package is downloaded.

Step 10 In the Set Up Recurring Update pane, specify the day(s) of the month and the time, and the day(s) of the week to update the signature package from the local server to the router.

Step 11 Click **Apply Changes**.

Related Topics

- Edit IPS: Auto Update, page 41-32
- Automatically Update IPS Signature Package Page, page 41-34

Automatically Update IPS Signature Package Reference

This section describes the pages and dialog boxes that you can use when working with the IPS Signature Auto Update feature and includes the following topic:

- Automatically Update IPS Signature Package Page, page 41-34

Automatically Update IPS Signature Package Page

Use the Automatically Update IPS Signature Package page to configure the router to automatically download the IPS signature package from a local server at periodic intervals.

How to Get to This Page

1. Choose **Configure > Security > Intrusion Prevention**. The Intrusion Prevention System (IPS) page opens.
2. From the Intrusion Prevention System (IPS) page, click the **Edit IPS** tab, and then click the **Auto Update** button.

Related Topics

- Automatically Updating IPS Signature Package from a Local Server, page 41-33
- Edit IPS: Auto Update, page 41-32

Field Reference

Table 41-4 Automatically Update IPS Signature Package Page

Element	Description
Login Information for Local Server pane	
Username	Enter the username required to log into the local server.
Password	Enter the password for the username.

Table 41-4 Automatically Update IPS Signature Package Page (continued)

Element	Description
URL	Enter the URL of the local server from which the signature package is downloaded.
Set Up Recurring Update pane—Specify the schedule for automatically updating the signature package from the local server to the router.	
Monthly	Specify the day(s) of the month and the time to update the signature package from the local server to the router.
Weekly	Specify the day(s) of the week to update the signature package from Cisco.com to the router.
Apply Changes button	Click this button to configure the router with the information you added.
Discard Changes button	Click this button to remove the information you added.

Edit IPS: SEAP Configuration

Cisco IOS IPS available with Cisco IOS release 12.4(11)T or later implements Signature Event Action Processing (SEAP). This window describes SEAP features that you can configure. To begin configuration, click on one of the buttons under the SEAP Configuration button.

You can configure SEAP settings for Cisco IOS IPS when the router runs Cisco IOS 12.4(11)T and later releases.

Edit IPS: SEAP Configuration: Target Value Rating

The target value rating (TVR) is a user-defined value that represents the user's perceived value of the target host. This allows the user to increase the risk of an event associated with a critical system and to de-emphasize the risk of an event on a low-value target.

Use the buttons to the right of the Target Value Rating and Target IP Address columns to add, remove, and edit target entries. Click **Select All** to highlight all target value ratings automatically. Click **Add** to display a dialog in which you can create a new TVR entry. Click **Edit** to change the IP address information for an entry.

Target Value Rating Column

Targets can be rated as High, Low, Medium, Mission Critical, or No Value. After a target entry has been created, the rating cannot be changed. If you need to change the rating, you must delete the target entry and recreate it using the rating that you want.

Target IP Address Column

The target IP address can be a single IP address or a range of IP addresses. The following example shows two entries. One is a single IP address entry and the other is an address range.

Target Value Rating	Target IP Address
High	192.168.33.2
Medium	10.10.3.1-10.10.3.55

Apply Changes

When you have entered the information that you want in the Target Value Rating window, click **Apply Changes**. The **Apply Changes** button is disabled when there are no changes to send to the router.

Discard Changes

To clear information that you have entered in the Target Value Rating window but have not sent to the router, click **Discard Changes**. The Discard Changes button is disabled when there are no changes made that are awaiting delivery to the router.

Add Target Value Rating

To add a TVR entry, choose the target value rating and enter a Target IP Address or range of IP addresses.

Target Value Rating

Targets can be rated as High, Low, Medium, Mission Critical, or No Value. Once a rating has been used for one target entry, it cannot be used for additional entries. Therefore, enter into the same entry all the targets that you want to give the same rating.

Target IP Addresses

You can enter a single target IP address or a range of addresses, as shown in the examples that follow:

```
192.168.22.33
10.10.11.4-10.10.11.55
```

The IP addresses that you enter are displayed in the Target Value Rating window.

Edit IPS: SEAP Configuration: Event Action Overrides

Event action overrides allow you to change the actions associated with an event based on the Risk Rating (RR) of that event. You do this by assigning an RR range for each event action. If an event occurs and its RR falls within the range that you defined, the action is added to the event. Event action overrides are a way to add event actions globally without having to configure each signature individually.

Use Event Action Overrides

Check the Use Event Action Overrides box to enable Cisco IOS IPS to use event action overrides. You can add and edit event action overrides whether or not they are enabled on the router.

Select All

The Select All button works with the Enable, Disable, and Delete buttons. If you want to enable or disable all event action overrides, click **Select All** and then click **Enable** or **Disable**. To remove all event action overrides, click **Select All** and then click **Delete**.

Add and Edit Buttons

Click **Add** to display a dialog in which you can enter the information for an event action override. Choose an event action override, and click **Edit** to change the information for an event action override.

Delete

Click **Delete** to remove the event action overrides that you selected, or to remove all event action overrides if you clicked **Select All**.

Enable and Disable

The Enable and Disable buttons allow you to enable or disable event action overrides. Choose one event action override, or click **Select All** to enable or disable all event action overrides.

Apply Changes

When you have entered the information that you want in the Event Action Overrides window, click **Apply Changes**. The **Apply Changes** button is disabled when there are no changes to send to the router.

Discard Changes

If you want to clear information that you have entered in the Event Action Overrides window but have not sent to the router, click **Discard Changes**. The **Discard Changes** button is disabled when there are no changes awaiting delivery to the router.

Add or Edit an Event Action Override

To add an event action override, choose the event action, enable or disable it, and specify the RR range. If you are editing, you cannot change the event action.

Event Action

Choose one of the following event actions:

- Deny Attacker Inline—Does not transmit this packet and future packets from the attacker address for a specified period of time (inline only).
- Deny Connection Inline—Does not transmit this packet and future packets on the TCP Flow (inline only)
- Deny Packet Inline—Does not transmit this packet.
- Produce Alert—Writes an <evIdsAlert> to the log.
- Reset TCP Connection—Sends TCP resets to hijack and terminate the TCP flow.

Enabled

Click **Yes** to enable the event action override, or **No** to disable it. You can also enable and disable event action overrides in the Event Action Override window.

Risk Rating

Enter the lower bound of the RR range in the Min box, and the upper bound of the range in the Max box. When the RR value of an event falls within the range that you specify, Cisco IOS IPS adds the override specified by the Event Action. For example, if Deny Connection Inline is assigned a RR range of 90-100, and an event with an RR of 95 occurs, Cisco IOS IPS responds by denying the connection inline.

Edit IPS: SEAP Configuration: Event Action Filters

Event action filters let Cisco IOS IPS perform individual actions in response to an event without requiring it to perform all actions or remove the entire event. Filters work by removing actions from an event. A filter that removes all actions from an event effectively consumes the event. Event action filters are processed as an ordered list. You can move filters up or down in the list to have the router process one filter before it processes other filters.

The Event Action Filters window displays the configured event action filters, and allows you to reorder the filters list so that Cisco IOS IPS processes the filters in the order that you want.

Use Event Action Filters

Check **Use Event Action Filters** to enable the use of event action filters. You can add, edit, and remove event action filters, and rearrange the list to specify the order that the router processes the filters whether or not event action filtering is enabled.

Event Action Filter List Area

For a description of the columns in the Event Action Filter List area, see Add or Edit an Event Action Filter.

Event Action Filter List Buttons

The Event Action Filter List buttons allow you to create, edit, and remove event action filters, and to place each event action filter in the order you want it to be in the list. The buttons are described in the following sections.

Select All

The **Select All** button works with the **Enable**, **Disable**, and **Delete** buttons. To enable or disable all event action filters, click **Select All**, and then click **Enable** or **Disable**. To remove all event action filters, click **Select All**, and then click **Delete**.

Add

Click the **Add** button to add an event action filter to the end of the list. A dialog box is displayed that enables you to enter the data for the filter.

Insert Before

To insert a new event action filter before an existing one, select the existing filter entry and click **Insert Before**. A dialog box is displayed that enables you to enter the data for the filter.

Insert After

To insert a new event action filter after an existing one, select the existing filter entry and click **Insert Before**. A dialog is displayed that enables you to enter the data for the filter.

Move Up

Choose an event action filter and click the **Move Up** button to move the filter up in the list.

Move Down

Choose an event action filter and click the **Move Down** button to move the filter down in the list.

Edit

Click the **Edit** button to edit an event action filter you have chosen.

Enable

Click the **Enable** button to enable an event action filter you have chosen. To enable all event action filters, click **Select All** first, and then click **Enable**.

Disable

Click the **Disable** button to disable an event action filter you have chosen. To disable all event action filters, click **Select All** first, and then click **Disable**.

Delete

Click the **Delete** button to delete an event action filter you have chosen. If you want to delete all event action filters, click **Select All** first, and then click **Delete**.

Apply Changes

When you have entered the information that you want in this window, click **Apply Changes**. The Apply Changes button is disabled when there are no changes to send to the router.

Discard Changes

To clear information that you have entered in this window but have not sent to the router, click **Discard Changes**. The Discard Changes button is disabled when there are no changes awaiting delivery to the router.

Add or Edit an Event Action Filter

The following information describes the fields in the Add and the Edit Event Action Filter dialogs.

Name

Cisco CP provides event action filter names beginning with Q00000, incrementing the numerical portion of the name by 1 each time you add an event action filter. You can also enter a name that you choose. If you are editing an event action filter, the Name field is read-only.

Enabled

Click **Yes** to enable the event action filter, or click **No** to disable it. You can also enable and disable event action filters in the Event Action Filter window.

Signature ID

For Signature ID, enter a range of signature IDs from 900 to 65535, or enter a single ID in that range. If you enter a range, use a dash (-) to separate the upper and lower bounds of the range. For example, enter 988-5000.

Subsignature ID

For Subsignature ID, enter a range of subsignature IDs from 0 to 255, or enter a single subsignature ID in that range. If you enter a range, use a dash (-) to separate the upper and lower bounds of the range. For example, enter 70-200.

Attacker Address

For Attacker Address, enter a range of addresses from 0.0.0.0 to 255.255.255.255, or enter a single address in that range. If you enter a range, use a dash (-) to separate the upper and lower bounds of the range. For example, enter 192.168.7.0-192.168.50.0.

Attacker Port

For Attacker Port, enter a range of port numbers from 0 to 65535, or enter a single port number in that range. If you enter a range, use a dash (-) to separate the upper and lower bounds of the range. For example, enter 988-5000.

Victim Address

For Victim Address, enter a range of addresses from 0.0.0.0 to 255.255.255.255, or enter a single address in that range. If you enter a range, use a dash (-) to separate the upper and lower bounds of the range. For example, enter 192.168.7.0-192.168.50.0.

Victim Port

For Victim Port, enter a range of port numbers from 0 to 65535, or enter a single port number in that range. If you enter a range, use a dash (-) to separate the upper and lower bounds of the range. For example, enter 988-5000.

Risk Rating

For Risk Rating, enter an RR range between 0 and 100.

Actions to Subtract

Click any actions that you want to subtract from matching events. To subtract more than one action from matching events, hold down the **Ctrl** key and choose additional events. All the events that you choose for this filter will be listed in the Event Action Filters window.

Stop on Match

If you want the Cisco IOS IPS to stop when an event matches this event action filter, click **Yes**. If you want the Cisco IOS IPS to evaluate matching events against the other remaining filters, click **No**.

Comments

You can add comments to describe the purpose of this filter. This field is optional.

Edit IPS: Signatures

Note The Edit IPS: Signatures page is displayed on Cisco routers that are running Cisco IOS Release 12.4(11)T and earlier releases.

Cisco IOS IPS prevents intrusion by comparing traffic against the signatures of known attacks. Cisco IOS images that support Cisco IOS IPS have built-in signatures that can be used, and you can also have Cisco IOS IPS import signatures for the router to use when examining traffic. Imported signatures are stored in a signature definition file (SDF).

This window lets you view the configured Cisco IOS IPS signatures on the router. You can add customized signatures, or import signatures from SDFs downloaded from Cisco.com. You can also edit, delete, enable, and disable signatures.

Cisco IOS IPS is shipped with an SDF that contains signatures that your router can accommodate. To learn more about the SDF shipped with Cisco IOS IPS, and how to have Cisco IOS IPS use it, click IPS-Supplied Signature Definition Files.

Signature Tree

The signature tree enables you to filter the signature list on the right according to the type of signature that you want to view. First choose the branch for the general type of signature that you want to display. The signature list displays the configured signatures for the type that you chose. If a plus (+) sign appears to the left of the branch, there are subcategories that you can use to refine the filter. Click the + sign to expand the branch and then choose the signature subcategory that you want to display. If the signature list is empty, there are no configured signatures available for that type.

For example:

- To display all attack signatures, click the **Attack** branch folder.
- To see the subcategories that you can use to filter the display of attack signatures, click the + sign next to the Attack folder.
- To see Denial of Service (DoS) signatures, click the **DoS** folder.

Import Button

Click to import a signature definition file from the PC or from the router. When you have specified the file, Cisco IOS IPS displays the signatures available in the file, and you can choose the ones that you want to import to the router. For more information about how to choose the signatures to import, see Import Signatures.

Note You can only import signatures from the router if the router has a DOS-based file system.

SDFs are available from:

http://www.cisco.com/cgi-bin/tablebuild.pl/ios-sigup

Note You need a CCO user name and password to access the above URL.

Cisco maintains an alert center that provides information on emerging threats. See Cisco Security Center for more information.

View By and Criteria List

The View By and Criteria drop-down lists enable you to filter the display according to the types of signatures that you want to view. First choose the criteria in the View By drop-down list, then choose the value for that criteria in the Criteria drop-down list.

For example, If you choose **Engine** in View By, Criteria changes to Engine, and you can choose among the available engines, such as **Atomic.ICMP** and **Service.DNS**.

If you choose **Sig ID**, or **Sig Name**, you must enter a value in the criteria field.

Total [*n*] New [*n*] Deleted [*n*]

This text gives you the count of new signatures and deleted signatures.

Select All

Click to choose all signatures in the list.

Add

Click **Add** if you want to do any of the following:

- **Add New**—This option allows you to add a new signature, and provide signature parameters in the displayed dialog.
- **Clone**—This option is enabled if a signature is specified that does not belong to a hardcoded engine. It is disabled if the signature uses one of the Cisco IOS hardcoded engines.

Edit

Click to edit the parameters of the specified signature.

Delete

Click **Delete** to mark the specified signature for deletion from the list. To view signatures you have deleted, click **Details**. For more information on the status and handling of these signatures, see Signatures marked for deletion.

Note You can display and monitor TrendMicro OPACL signatures, but you cannot edit, delete, enable, or disable them. If a TrendMicro OPACL signature is specified, the **Edit**, **Delete**, **Enable,** and **Disable** buttons are disabled. The Cisco Incident Control Server assumes control of these signatures.

Enable

Click **Enable** to enable the specified signature. An enabled signature is designated with a green checkmark. A signature, which was disabled and then enabled, has a yellow Wait icon in the ! column indicating that the change must be applied to the router.

Disable

Click **Disable** to disable the specified signature. A signature that is disabled is designated with a red icon. If the signature is disabled during the current session, a yellow Wait icon appears in the ! column indicating that the change must be applied to the router.

Summary or Details Button

Click to display or hide the signatures marked for deletion.

Signature List

Displays the signatures retrieved from the router, and any signatures added from an SDF.

Note Signatures that are set to import and are identical to deployed signatures are not imported and do not appear in the signature list.

The signature list can be filtered using the selection controls.

Enabled	Enabled signatures are indicated with a green icon. If enabled, the actions specified when the signature is detected is carried out. Disabled signatures are indicated with a red icon. If disabled, the actions are disabled and are not be carried out.
Alert (!)	This column may contain the yellow Wait icon.  This icon indicates new signatures that have not been delivered to the router or modified signatures that have not been delivered to the router.
Sig ID	Numerical signature ID. For example, the sigID for ICMP Echo Reply is 2000.
SubSig ID	Subsignature ID.
Name	Name of the signature. For example, ICMP Echo Reply.
Action	Action to take when the signature is detected.

Filter	ACL associated with the corresponding signature.
Severity	Severity level of the event. Severity levels are informational, low, medium, and high.
Engine	Engine to which the signature belongs.

Right-click Context Menu

If you right-click a signature, Cisco CP displays a context menu with the following options:

- Actions—Click to choose the actions to be taken when the signature is matched. See Assign Actions for more information.
- Set Severity to—Click to set the severity level of a signature to: high, medium, low, or informational.
- Restore Defaults—Click to restore the default values of the signature.
- Remove Filter—Click to remove a filter applied to the signature.
- NSDB help (need CCO account)—Click to display help on the Network Security Data Base (NSDB).

Signatures marked for deletion

This area is visible when the **Details** button is clicked. It lists the signatures that you deleted from the Signature List, and signatures that are marked for deletion because imported signatures are set to replace signatures already configured on the router. See How to Import Signatures for more information.

Signatures marked for deletion remain active in the Cisco IOS IPS configuration until you click **Apply Changes**. If you exit the Signatures window and disable Cisco IOS IPS, the marked signatures will be deleted if Cisco IOS IPS is re-enabled.

Undelete All Button

Click to restore all signatures in the signatures marked deleted list.

Undelete Button

Click to restore specified signatures marked for deletion. When clicked the signatures are unmarked, and returned to the list of active signatures.

Apply Changes Button

Click to deliver newly imported signatures, signature edits, and newly enabled or disabled signatures to the router. When the changes are applied, the yellow Wait icon is removed from the ! column. These changes are saved to your router flash memory in the file sdmips.sdf. This file is created automatically the first time you click **Apply Changes**.

Note If you are attempting to import signatures, and these signatures are all identical to deployed signatures, the **Apply Changes** button is disabled.

Discard Changes Button

Click to discard accumulated changes.

Note If you are attempting to import signatures, and these signatures are all identical to deployed signatures, the **Discard Changes** button is disabled.

Victim Port

For Victim Port, enter a range of port numbers from 0 to 65535, or enter a single port number in that range. If you enter a range, use a dash (-) to separate the upper and lower bounds of the range. For example, enter 988-5000.

Risk Rating

For Risk Rating, enter an RR range between 0 and 100.

Actions to Subtract

Click any actions that you want to subtract from matching events. To subtract more than one action from matching events, hold down the **Ctrl** key when you choose additional events. All the events that you choose for this filter will be listed in the Event Action Filters window.

Stop on Match

If you want the Cisco IOS IPS to stop when an event matches this event action filter, click **Yes**. If you want the Cisco IOS IPS to evaluate matching events against the other remaining filters, click **No**.

Comments

You can add comments to describe the purpose of this filter. This field is optional.

Edit IPS: Signatures

Cisco IOS IPS prevents intrusion by comparing traffic against the signatures of known attacks. Cisco IOS images that support Cisco IOS IPS have built-in signatures that Cisco IOS IPS can use, and you can also have Cisco IOS IPS import signatures for the router to use when examining traffic. Imported signatures are stored in a signature definition file (SDF).

This help topic describes the Signatures window displayed when the router runs Cisco IOS 12.4(11)T and later releases.

The Signatures window lets you view the configured Cisco IOS IPS signatures on the router. You can add customized signatures, or import signatures from SDFs downloaded from Cisco.com. You can also edit, enable, disable, retire, and unretire signatures.

Signature Tree

The signature tree enables you to filter the signature list on the right according to the type of signature that you want to view. First choose the branch for the general type of signature that you want to display. The signature list displays the configured signatures for the type that you chose. If a plus (+) sign appears to the left of the branch, there are subcategories that you can use to refine the filter. Click the + sign to expand the branch and then choose the signature subcategory that you want to display. If the signature list is empty, there are no configured signatures available for that type.

For example: If you want to display all attack signatures, click the **Attack** branch folder. If you want to see the subcategories that you can use to filter the display of attack signatures, click the + sign next to the Attack folder. If you want to see Denial of Service (DoS) signatures, click the **DoS** folder.

Import Button

Click to import a signature definition file from the PC or from the router. When you have specified the file, Cisco IOS IPS displays the signatures available in the file, and you can choose the ones that you want to import to the router. For more information about how to choose the signatures to import, see Import Signatures.

Note You can only import signatures from the router if the router has a DOS-based file system.

SDFs are available from:

http://www.cisco.com/cgi-bin/tablebuild.pl/ios-sigup

Note You need a CCO user name and password to access the above URL.

Cisco maintains an alert center that provides information on emerging threats. See Cisco Security Center for more information.

View By and Criteria List

The View By and Criteria drop-down list enable you to filter the display according to the types of signatures that you want to view. First choose the criteria in the View By drop-down list, then choose the value for that criteria in the Criteria drop-down list.

For example: If you choose Engine in View By, Criteria changes to Engine, and you can choose among the available engines, such as Atomic.ICMP and Service.DNS.

If you choose Sig ID, or Sig Name, you must enter a value in the criteria field.

Total [*n*]

This text gives you the total number of signatures on the router.

Compiled [*n*]

This text gives you the total number of compiled signatures on the router.

Select All

Click to choose all signatures in the list.

Disable

Click **Disable** to disable the specified signature. A signature that is disabled is designated with a red icon. If the signature is disabled during the current session, a yellow Wait icon appears in the ! column indicating that the change must be applied to the router.

Retire

Click **Retire** to prevent a signature from being compiled for scanning.

Unretire

Click **Unretire** to allow the signature to be compiled for scanning.

Signature List

Displays the signatures retrieved from the router, and any signatures added from an SDF.

Note Signatures that are set to import and are identical to deployed signatures are not imported and do not appear in the signature list.

The signature list can be filtered using the selection controls.

Enabled	Enabled signatures are indicated with a green icon. If enabled, the actions specified when the signature is detected is carried out. Disabled signatures are indicated with a red icon. If disabled, the actions are disabled and are not be carried out.
Alert (!)	This column may contain the yellow Wait icon.  This icon indicates new signatures that have not been delivered to the router or modified signatures that have not been delivered to the router.
Sig ID	Numerical signature ID. For example: the sigID for ICMP Echo Reply is 2000.
SubSig ID	Subsignature ID.
Name	Name of the signature. For example: ICMP Echo Reply.
Action	Action to take when the signature is detected.
Severity	Severity level of the event. Severity levels are informational, low, medium, and high
Fidelity Rating	The fidelity rating of the signature.
Retired	A value of true or false. True if signature has been retired. False if not. Retired signatures are not compiled.
Engine	Engine to which the signature belongs.

Right-click Context Menu

If you right-click a signature, Cisco CP displays a context menu with the following options:

- Actions—Click to choose the actions to be taken when the signature is matched. See Assign Actions for more information.
- Fidelity Rating—Click to enter a fidelity rating for the signature.
- Set Severity to—Click to set the severity level of a signature to: high, medium, low, or informational.
- Restore Defaults—Click to restore the signature's default values.

- NSDB help (need CCO account)—Click to display help on the Network Security Data Base (NSDB).

Apply Changes

Click **Apply Changes** to deliver newly imported signatures, signature edits, and newly enabled or disabled signatures to the router. When the changes are applied, the yellow Wait icon is removed from the ! column. These changes are saved to your router flash memory in the file sdmips.sdf. This file is created automatically the first time you click **Apply Changes**.

Note If you are attempting to import signatures, and these signatures are all identical to deployed signatures, then the **Apply Changes** button is disabled.

Discard Changes

Click **Discard Changes** to discard accumulated changes.

Note If you are attempting to import signatures, and these signatures are all identical to deployed signatures, then the **Discard Changes** button is disabled.

Edit Signature

Use the fields in Edit Signature dialog to edit the selected signature. The changes that you make are stored in a delta file that is saved to router flash memory. The elements of signatures are described in the following sections.

This help topic describes the Edit Signatures window displayed when the router runs Cisco IOS 12.4(11)T and later releases.

Signature ID

The unique numerical value assigned to this signature. This value allows the Cisco IOS IPS to identify a particular signature.

Subsignature ID

The unique numerical value assigned to this subsignature. A subsignature ID is used to identify a more granular version of a broad signature.

Alert Severity

Choose one of the following to categorize the severity of the alert: High, Medium, Low, or Informational.

Sig Fidelity Rating

The signature fidelity rating is a value set by the author of the signature to quantify the confidence that the signature will produce true positives. This value is set before a signature is deployed and can be adjusted when signature performance data is available.

Promiscuous Delta

The promiscuous delta is a factor that is subtracted from the Risk Rating (RR) of an event when the router is operating in promiscuous mode. The Promiscuous Delta is subtracted from the RR every time an alert is triggered when the system is deployed in promiscuous mode.

Note Even though the promiscuous delta can be reconfigured on a signature basis, it is not recommended that you change any of the predefined promiscuous-delta settings.

Sig Description

The signature description includes the signature name and release, any alert notes available from the Cisco Security Center, user comments, and other information.

Engine

The signature engine associated with this signature. One commonly-used engine is named Atomic IP.

The Engine box contains fields that allow you to tune a wide variety of signature parameters. For example, you can specify the action to be taken if this signature is matched and an event is generated, you can specify the layer 4 protocol to inspect for events matching this signature, and you can specify IP parameters, such as header length and type of service.

Event Counter

The controls in the Event Counter box allow you to specify the parameters described in the following sections.

Event Count

The number of times an event must occur before an alert is generated.

Event Count Key

The type of information to use to count an event as occurring. For example, if you choose **both attacker and victim addresses and ports**, each time you have these 4 pieces of information for an event, the count increments by 1. If you choose **attacker address**, only that piece of information is needed.

Event Interval

The number of seconds between events being sent to the log. If you select **Yes**, an additional field is displayed allowing you to enter the number of seconds.

Alert Frequency

The purpose of the alert frequency parameter is to reduce the volume of the alerts written to the log,

Summary Mode

There are four modes: Fire All, Fire Once, Summarize, and Global Summarize. The summary mode is changed dynamically to adapt to the current alert volume. For example, you can configure the signature to Fire All, but after a certain threshold is reached, it starts summarizing.

Summary Key

The Summary Key has the type of information to use to determine when to summarize. For example, if you choose **both attacker and victim addresses and ports**, each time you have these 4 pieces of information for an event, summarization occurs. If you choose **attacker address**, only that piece of information is needed.

Specify Global Summary Threshold

You can specify numerical thresholds to use for determining when to summarize events to the log. If you choose **Yes**, you can specify a global summary threshold, and a summary interval.

Status

You can specify whether the signature should be enabled, disabled, or retired in the Status box. Additionally, the Status box can display the signatures that you have obsoleted.

File Selection

This window allows you to load a file from your router. Only DOSFS file systems can be viewed in this window.

The left side of window displays an expandible tree representing the directory system on your Cisco router flash memory and on USB devices connected to that router.

The right side of the window displays a list of the names of the files and directories found in the directory that is specified in the left side of the window. It also shows the size of each file in bytes, and the date and time each file and directory was last modified.

You can choose a file to load in the list on the right side of the window. Below the list of files is a Filename field containing the full path of the specified file.

Note If you are choosing a configuration file to provision your router, the file must be a CCCD file or have a .cfg extension.

Name

Click **Name** to order the files and directories alphabetically based on name. Clicking **Name** again will reverse the order.

Size

Click **Size** to order the files and directories by size. Directories always have a size of zero bytes, even if they are not empty. Clicking **Size** again will reverse the order.

Time Modified

Click **Time Modified** to order the files and directories based on modification date and time. Clicking **Time Modified** again reverses the order.

Assign Actions

This window contains the actions that can be taken upon a signature match. Available actions depend on the signature, but the most common actions are listed below:

- **alarm**—Generate an alarm message. Same as **produce-verbose-alert**.
- **deny-attacker-inline**—Create an ACL that denies all traffic from the IP address considered to be the source of the attack by the Cisco IOS IPS system. Same as **denyAttackerInline**.
- **deny-connection-inline**—Drop the packet and all future packets on this TCP flow. Same as **produce-alert** and **denyFlowInline**.
- **deny-packet-inline**—Do not transmit this packet (inline only). Same as **drop**.
- **denyAttackerInline**—Create an ACL that denies all traffic from the IP address considered to be the source of the attack by the Cisco IOS IPS system. Same as **deny-attacker-inline**.
- **denyFlowInline**—Create an ACL that denies all traffic from the IP address that is considered the source of the attack belonging to the 5-tuple (src ip, src port, dst ip, dst port and l4 protocol). denyFlowInline is more granular than denyAttackerInline. Same as **produce-alert** and **deny-connection-inline**.
- **drop**—Drop the offending packet. Same as **deny-packet-inline**.

- **produce-alert**—Generate an alert. Same as **denyFlowInline** and **deny-connection-inline**.
- **produce-verbose-alert**—Generate an alert which includes an encoded dump of the offending packet. Same as **alarm**.
- **reset**—Reset the connection and drop the offending packet. Same as **reset-tcp-connection**.
- **reset-tcp-connection**—Send TCP RESETS to terminate the TCP flow. Same as **reset**.

Import Signatures

Use the Import IPS window to import signatures from an SDF or other file on your PC. The information in this window tells you which signatures are available from the SDF, and which of them are already deployed on your router.

How to Import Signatures

To import signatures, follow these steps:

Step 1 Use the signature tree, View By drop-down list, and Criteria List drop-down list to display the signatures you want to import.

In the signature list, uncheck the **Import** check box for the signatures that you *do not* want to import. If you want to uncheck the **Import** check box for all of the signatures, click the **Unselect All** button, which changes to the **Select All** button

Step 2 Check the check box **Do not import signatures that are defined as disabled** if you want to avoid importing signatures that may degrade router performance when used.

Step 3 Click the **Merge** button to merge the imported signatures with the signatures that are already configured on the router, or the **Replace** button to replace the already configured signatures.

See Merge Button and Replace Button for more information.

Step 4 Click the **Apply Changes** button in the Edit IPS window to deploy the imported signatures.

You can make changes to the imported signatures before deploying them. Signatures that set to import and are identical to deployed signatures will not be imported. If all imported signatures are identical to deployed signatures, then the **Apply Changes** button is disabled.

Signature Tree

For a description of the signature tree, see Signature Tree. You can use the signature tree in this window to assemble the signatures that you want to import, category by category.

For example: you may want to add signatures from the OS category, and from the Service category. You can do this by choosing the **OS** branch of the tree, and any branch from that part of the tree that you want, such as the UNIX branch or the Windows branch. When the types of signatures that you want to import are displayed, you can make your selections in the signature list area. Then you can choose the **Service** branch, and choose any of the service signatures that you want.

View By and Criteria List

The View By and Criteria list boxes enable you to filter the display according to the types of signatures that you want to view. First choose the criteria in the View By list, then choose the value for that criteria in the list to the right (the criteria list).

For example: If you choose **Engine** in the View By list, the criteria list is labeled Engine, and you can choose among the available engines, such as **Atomic.ICMP**, and **Service.DNS**.

If you choose **Sig ID**, or **Sig Name**, you must enter a value in the criteria list.

Signature List Area

The signature list displays the signatures available in the SDF based on the criteria you chose in the signature tree. The text of signatures already found on the target router is blue.

The signature list area has these columns:

- Sig ID—Unique numerical value assigned to this signature. This value allows Cisco IOS IPS to identify a particular signature.

- Name—Name of the signature. For example: *FTP Improper Address*.
- Severity—High, medium, low, or informational.
- Deployed—Displays *Yes* if the signature is already deployed on the router. Displays *No* if the signature is not deployed on the router.
- Import—Contains a check box for each signature. If you want to import the signature, check this box.

Note All of the signatures imported from an SDF or a zip file with the name IOS-S*xxx*.zip can be displayed in the signature list. When signatures are imported from a zip file with a different name, only the signatures found through the View By and Criteria List drop-down lists are displayed.

Merge Button

Click to merge the signatures that you are importing with the signatures that are already configured on the router.

Replace Button

Click to replace the signatures that are already configured on the router with the signatures that you are importing. Signatures already configured on the router but that are *not* found in the list of signatures being imported are marked for deletion and listed under **Signatures Marked for Deletion** in **Edit IPS > Signatures**. See Signatures marked for deletion for more information.

Add, Edit, or Clone Signature

This window contains fields and values described in the Field Definitions section. The fields vary depending on the signature, so this is not an exhaustive list of all the fields you might see.

Field Definitions

The following fields are in the Add, Edit, and Clone Signature windows.

- **SIGID**—Unique numerical value assigned to this signature. This value allows Cisco IOS IPS to identify a particular signature.

- **SigName**—Name assigned to the signature.
- **SubSig**—Unique numerical value assigned to this subsignature. A subsig ID is used to identify a more granular version of a broad signature.
- **AlarmInterval**—Special Handling for timed events. Use AlarmInterval Y with MinHits X for X alarms in Y second interval.
- **AlarmSeverity**—Severity of the alarm for this signature.
- **AlarmThrottle**—Technique used for triggering alarms.
- **AlarmTraits**—User-defined traits further describing this signature.
- **ChokeThreshold**—Threshold value of alarms-per-interval that triggers autoswitch AlarmThrottle modes. If ChokeThreshold is defined, Cisco IOS IPS automatically switches AlarmThrottle modes if a large volume of alarms is seen in the ThrottleInterval.
- **Enabled**—Identifies whether or not the signature is enabled. A signature must be enabled in order for Cisco IOS IPS to protect against the traffic specified by the signature.
- **EventAction**—Actions Cisco IOS IPS will take if this signature is triggered.
- **FlipAddr**—True if the source and destination addresses, and their associated ports, are swapped in the alarm message. False if no swap occurs (default).
- **MinHits**—Specifies the minimum number of signature hits that must occur before the alarm message is sent. A hit is the appearance of the signature on the address key.
- **SigComment**—Comment or description text for the signature.
- **SigVersion**—Signature version.
- **ThrottleInterval**—Number of seconds defining an Alarm Throttle interval. This is used with the AlarmThrottle parameter to tune special alarm limiters.
- **WantFrag**—True enables inspection of fragmented packets only. False enables inspection of non-fragmented packets only. Choose “undefined” to allow for inspection of both fragmented and non-fragmented packets.

Cisco Security Center

The Cisco Security Center provides information on emerging threats, and links to the Cisco IOS IPS signatures available to protect your network from them. Signature reports and downloads are available at:

http://tools.cisco.com/MySDN/Intelligence/searchSignatures.x

Note You need a CCO user name and password to access the above URL.

IPS-Supplied Signature Definition Files

To ensure that the router has as many signatures available as its memory can accommodate, Cisco CP is shipped with one of the following SDFs:

- 256MB.sdf—If the amount of RAM available is greater than 256 MB. The 256MB.sdf file contains 500 signatures.
- 128MB.sdf—If the amount of RAM available is between 128 MB and 256 MB. The 128MB.sdf file contains 300 signatures.
- attack-drop.sdf—If the amount of available RAM is 127 MB or less. The attack-drop.sdf file contains 82 signatures.

If your router runs Cisco IOS version 12.4(11)T or later, you must use an SDF file that has a name of the format sigv5-SDM-S*xxx*.zip; for example, sigv5-SDM-S260.zip.

Note The router must be running Cisco IOS Release 12.3(14)T or later releases to be able to use all the available signature engines in 256MB.sdf and 128MB.sdf files. If the router uses an earlier release, not all signature engines will be available.

To use an SDF in router memory, determine which SDF has been installed and then configure Cisco IOS IPS to use it. The procedures that follow show you how to do this.

Determine Which SDF File Is in Memory

To determine which SDF file is in router memory, open a Telnet session to the router, and enter the **show flash** command. The output is similar to the following:

```
System flash directory:
File  Length   Name/status
  1   10895320  c1710-k9o3sy-mz.123-8.T.bin
  2   1187840  ips.tar
  3   252103   attack-drop.sdf
  4   1038     home.shtml
  5   1814     sdmconfig-1710.cfg
  6   113152   home.tar
  7   758272   es.tar
  8   818176   common.tar
[14028232 bytes used, 2486836 available, 16515068 total]
16384K bytes of processor board System flash (Read/Write)
```

In this example, the attack-drop.sdf file is in router memory. On some routers, such as routers with a disk file system, use the **dir** command to display the contents of router memory.

Configuring IPS to Use an SDF

To have Cisco IOS IPS use the SDF in router memory, do the following:

Step 1 Click **Global Settings**.

Step 2 In the Configured SDF Locations list, click **Add**.

Step 3 In the dialog box displayed, click **Specify SDF on flash**, and enter the name of the SDF file.

Step 4 Click **OK** to close the dialog box.

Security Dashboard

The Security Dashboard allows you to keep your router updated with signatures for the latest security threats. You must have Cisco IOS IPS configured on your router before you can deploy signatures using the Security Dashboard.

Top Threats Table

The Top Threats table displays the latest top threats from Cisco if the status of the associated signatures indicates that they are available for deployment or are under investigation. Some of the top threats in the table are associated with signatures that can be deployed to your router. The text of signatures already found on your router is blue.

To obtain the latest top threats, click the **Update top threats list** button.

Note You cannot update the top threats by using the Cisco CP **Refresh** button or your browser's Refresh command.

The Top Threats table has the following columns:

- **Device Status** indicates if the signature associated with the threat is already enabled on your router. The following symbol may appear in the Device Status column:

  Signature is already enabled on your router.

  Signature is not available on your router or is available but *not* enabled on your router.

- **Sig ID** is a unique number identifying the signature associated with the threat.
- **SubSig ID** is a unique number identifying the subsignature. If the signature associated with the threat does not have a subsignature, **SubSig ID** is 0.
- **Name** is the name given to the threat.
- **Urgency** indicates if the level of the threat is high (Priority Maintenance) or normal (Standard Maintenance).
- **Threat Status** indicates if the signature associated with the threat is available or if the threat is still under investigation.
- **Deploy** contains check boxes that can be checked if the signature associated with the threat is available to deploy.

Select SDF

Click the **Browse** button and choose the Cisco IOS SDF file to use. The Cisco IOS SDF file must be present on your PC. The format that the filename has depends on the version of Cisco IOS the router is running.

- If the router is running a Cisco IOS image earlier than 12.4(11)T, the SDF must have a name with the format IOS-S*xxx*.zip, where *xxx* is a three-digit number. For example: a Cisco IOS IPS SDF file may be named IOS-S193.zip.
- If the router is running a Cisco IOS image of version 12.4(11)T or later, the SDF must have a name with the format sigv5-SDM-S*xxx*.zip; for example, sigv5-SDM-S260.zip

The location of a Cisco IOS SDF file you choose is shown in the SDF file location field. The SDF file location field is read-only.

After the first time you download a Cisco IOS SDF file, Cisco CP remembers the location of the file. The next time you load the Security Dashboard, Cisco CP will select the latest Cisco IOS SDF file based on the three-digit number in the file's name.

Note The Cisco IOS SDF file with the highest three-digit number in its name is the latest Cisco IOS SDF file.

Deploying Signatures From the Top Threats Table

Before attempting to deploy signatures from the Top Threats table, ensure that you have:

- Configured Cisco IOS IPS on your router
- Downloaded the latest Cisco IOS file to your PC

To deploy signatures from the Top Threats table, follow these steps:

Step 1 Click the **Update top threats list** button to ensure that you have the latest top threats list.

Step 2 In the Deploy column, check the check box for each top-threat signature you want to deploy from the Top Threats table.

Only top threats with the status **Signature available** can be chosen. Available signatures with a red icon in their Applied column are automatically set to deploy.

Step 3 Click the **Browse** button and choose the latest SDF file if you need to ensure that you are using the latest signature file.

You may need to do this if the location of the latest SDF file has changed since it was last set in the Security Dashboard, or if the format of its name is not IOS-S*xxx*.zip, where *xxx* is a three-digit number

Step 4 Click the **Deploy signatures** button to deploy the chosen signatures to your router.

A warning is shown if any of the chosen signatures are not found in the Cisco IOS file. However, all found signatures can still be deployed. After being deployed on your router, the signatures are automatically enabled and added to the router active signatures list.

IPS Migration

If you have an existing the Cisco IOS IPS configuration that you want to migrate to Cisco IOS IPS available in Cisco IOS 12.4(11)T or later releases, you can use the IPS Migration wizard to do the migration.

Note If the router uses a Cisco IOS image of version 12.4(11)T or later, you must migrate a configuration created before this release if you want to use Cisco IOS IPS on your router. If you do not migrate the configuration, the configuration commands will not be changed, but Cisco IOS IPS will not operate.

Click the **Launch IPS Migration Wizard** button to begin the migration process.

Migration Wizard: Welcome

The Migration Wizard welcome window lists the tasks that the wizard helps you to complete. If you do not want to run the IPS migration wizard, click **Cancel**.

The IPS Migration wizard is available when the router runs Cisco IOS 12.4(11)T and later releases.

Migration Wizard: Choose the IOS IPS Backup Signature File

The backup file contains the Cisco IOS IPS information that will be migrated. This may be a Signature Definition File (SDF), such as attack-drop.sdf, or 128MB.sdf. If you made changes to the signature information, such as disabling signatures or changing the attributes of specific signatures, the records of your changes are kept in a separate file. If you used Cisco CP to make changes, Cisco CP saves them in a file named sdmips.sdf, which it saves to router flash memory. If you made changes manually, you may have given the file another name and may have saved a backup copy on your PC.

Click the **...** button next to the backup file field to display a dialog that allows you to browse for this backup file on router flash memory or on your PC.

Signature File

Specify the location of the backup signature file in this dialog.

Specify signature file on flash

If the backup signature file is located on flash memory, click the down arrowhead button next to this field and choose the file.

Specify signature file on the PC

If the backup signature file is located on the PC, click the **Browse** button next to this field and navigate to the file.

Java Heap Size

Cisco CP displays the Java Heap Size window when the Java heap size is too low to support a Cisco CP feature. Complete the following procedure to set the heap size to the value stated in the window.

Step 1 Exit Cisco CP.

Step 2 Click **Start > Control Panel > Java**.

Step 3 Open the Java Applet Runtime Settings dialog box. The location of this dialog box varies by release.

a. Click the **Advanced** tab. Locate the Java Applet Runtime Settings dialog box and proceed to Step 4. If the dialog box is not available from the Advanced tab, click the **Java** tab.

b. Click the **Java** tab. Locate the Java Applet Runtime Settings dialog box. Click the **View** button if necessary to display the dialog box, and proceed to Step 4.

Step 4 In the Java Runtime Parameters column, enter the value stated in the window. For example if the window states that you must use the value `-Xmx256m`, enter that value in the Java Runtime Parameters column. The following table shows sample values.

Product Name	Version	Location	Java Runtime Parameters
JRE	1.5.0_11	C:\Program Files\java\jre1.5.0_11	-Xmx256m

Step 5 Click **OK** in the Java Applet Runtime Settings dialog box.

Step 6 Click **Apply** in the Java Control Panel, and then click **OK**.

Step 7 Restart Cisco CP.

CHAPTER 42

Network Admission Control

Network Admission Control (NAC) protects data networks from computer viruses by assessing the health of client workstations, ensuring that they receive the latest available virus signature updates, and controlling their access to the network.

NAC works with antivirus software to assess the condition of a client, called the client's *posture*, before allowing the client access to the network. NAC ensures that a network client has an up-to-date virus signature set which has not been infected. If the client requires a signature update, NAC directs it to complete the update. If the client has been compromised or if a virus outbreak is occurring on the network, NAC places the client into a quarantined network segment until disinfection is completed.

For more information on NAC, read the following documents:

- Security Solutions for Enterprise: Network Admission Control Introduction. This document can be found at the following link:

  http://www.cisco.com/en/US/netsol/ns466/networking_solutions_package.html

- Network Admission Control (NAC) Framework.This document can be found at the following link:

  http://www.cisco.com/en/US/netsol/ns617/networking_solutions_sub_solution_home.html

Create NAC Tab

You use the Create NAC tab and NAC wizard to create a NAC policy and associate it with an interface. After you create the NAC policy, you can edit it by clicking **Edit NAC** and choosing it in the policy list.

The NAC configuration on the router is only one part of a complete NAC implementation. Click Other Tasks in a NAC Implementation to learn the tasks that must be performed on other devices in order to implement NAC.

Enable AAA Button

Authentication, authorization, and accounting (AAA) must be enabled on the router before you can configure NAC. If AAA is not enabled, click the **Enable AAA** button. If AAA has already been configured on the router, this button is not displayed.

Launch NAC Wizard Button

Click this button to launch the NAC wizard. The wizard divides NAC configuration into a series of screens in which you complete a single configuration task.

How Do I List

If you want to create a configuration that this wizard does not guide you through, click the button next to this list. It lists other types of configurations that you might want to perform. If you want to learn how to create one of the configurations listed, choose the configuration and click **Go**.

Other Tasks in a NAC Implementation

A full NAC implementation includes the following configuration steps:

Step 1 Install and configure the Cisco Trust Agent (CTA) software on network hosts. This provides hosts with a posture agent capable of responding to EAPoUDP queries by the router. See the links after these steps to obtain the CTA software and learn how to install and configure it.

Step 2 Install and configure an AAA authentication EAPoUDP server. This server must be a Cisco Secure Access Control Server (ACS) using the RADIUS protocol. Cisco Secure Access Control Server software version 3.3 is required. See the links after these steps to learn more about installing and configuring ACS.

Step 3 Install and configure the posture validation and remediation server.

If you are a registered Cisco.com user, you can download Cisco Trust Agent (CTA) software from the following link:

http://www.cisco.com/cgi-bin/tablebuild.pl/cta

The document "Administrator Guide for Cisco Trust Agent, Release 2.1, With Bundled Supplicant" at the following link explains how to install and configure CTA software on a host.

http://www.cisco.com/en/US/docs/security/cta/2.1.103.0_supplicant/admin_guide/cta_bundled_with_supplicant.html

The document "Implementing Network Admission Control Phase One Configuration and Deployment" at the following link contains an overview of the configuration process.

http://www.cisco.com/en/US/solutions/collateral/ns340/ns394/ns171/ns466/ns617/net_implementation_white_paper0900aecd80217e26.pdf

Documents at the following link explain how to install and configure Cisco Secure ACS for Windows Servers.

http://www.cisco.com/en/US/docs/net_mgmt/cisco_secure_access_control_server_for_windows/4.2/roadmap/DGuide42.html

Welcome

The NAC wizard enables you to do the following:

- Choose the interface on which NAC is to be enabled—Hosts attempting access to the network through this interface must undergo the NAC validation process.

- Configure NAC Policy Servers—Admission control polices are configured on these servers, and the router contacts them when a network host attempts to access the network. You can specify information for multiple servers. NAC policy servers use the RADIUS protocol.
- Configure a NAC exception list—Hosts such as printers, IP phones, and hosts without NAC posture agents installed may need to bypass the NAC process. Hosts with static IP addresses and other devices can be identified in an exception list, and be handled using an associated exception policy. Hosts can also be identified by their MAC address, or by their device type.
- Configure an agentless host policy—If you want to use a policy residing on a Cisco Secure ACS server to handle hosts without an installed posture agent, you can do so. When the Cisco Secure ACS server receives a packet from an agentless host, it responds by sending the agentless host policy. Configuring an agentless host policy is useful when there are agentless hosts that are dynamically addressed, such as DHCP clients.
- Configuring NAC for remote access—Hosts using Cisco CP to manage the router must be allowed access. The wizard lets you specify IP addresses for remote management so that Cisco CP can modify the NAC ACL to allow the hosts with those addresses access to the router.

Configuring NAC on the router is the last step in a NAC configuration. Before you configure the router with this feature, Complete the steps described in the following link: Other Tasks in a NAC Implementation.

NAC Policy Servers

NAC admission control policies are configured and stored in a policy database residing on RADIUS servers running Cisco Secure ACS version 3.3. The router must validate the credentials of network hosts by communicating with the RADIUS server. Use this window to provide the information the router needs to contact the RADIUS servers. Each RADIUS server that you specify must have Cisco Secure Cisco Access Control Server (ACS) software version 3.3 installed and configured.

Choose the RADIUS client source

Configuring the RADIUS source allows you to specify the source IP address to be sent in RADIUS packets bound for the RADIUS server. If you need more information about an interface, choose the interface and click the **Details** button.

The source IP address in the RADIUS packets sent from the router must be configured as the NAD IP address in the Cisco ACS version 3.3 or later.

If you choose **Router chooses source**, the source IP address in the RADIUS packets will be the address of the interface through which the RADIUS packets exit the router.

If you choose an interface, the source IP address in the RADIUS packets will be the address of the interface that you chose as the RADIUS client source.

Note Cisco IOS software allows a single RADIUS source interface to be configured on the router. If the router already has a configured RADIUS source and you choose a different source, the source IP address placed in the packets sent to the RADIUS server changes to the IP address of the new source, and may not match the NAD IP address configured on the Cisco ACS.

Details Button

If you need a quick snapshot of the information about an interface before choosing it, click **Details**. The screen shows you the IP address and subnet mask, the access rules and inspection rules applied to the interface, the IPSec policy and QoS policy applied, and whether there is an Easy VPN configuration on the interface.

Server IP, Timeout, and Parameters Columns

The Server IP, Timeout, and Parameters columns contain the information that the router uses to contact a RADIUS server. If no RADIUS server information is associated with the chosen interface, these columns are blank.

Use for NAC Check Box

Check this box if you want to use the listed RADIUS server for NAC. The server must have the required admissions control policies configured if NAC is to be able to use the server.

Add, Edit, and Ping Buttons

To provide information for a RADIUS server, click the **Add** button and enter the information in the screen displayed. Choose a row and click **Edit** to modify the information for a RADIUS server. Choose a row and click **Ping** to test the connection between the router and a RADIUS server.

Note When performing a ping test, enter the IP address of the RADIUS source interface in the source field in the ping dialog. If you chose **Router chooses source**, you need not provide any value in the ping dialog source field.

The **Edit** and **Ping** buttons are disabled when no RADIUS server information is available for the chosen interface.

Interface Selection

Choose the interface on which to enable NAC in this window. Choose the interface through which network hosts connect to the network.

Click the **Details** button to display the policies and rules associated with the interface you choose. The window displays the names of the ACLs applied to inbound and to outbound traffic on this interface.

If an inbound ACL is already present on the interface, Cisco CP uses that ACL for NAC by adding appropriate permit statements for EAPoUDP traffic. If the IP address of the interface on which NAC is being applied were 192.55.22.33, a sample permit statement might be the following:

```
access-list 100 permit udp any eq 21862 192.55.22.33
```

The permit statement that Cisco CP adds uses the port number 21862 for the EAPoUDP protocol. If the network hosts run EAPoUDP on a custom port number, you must modify this ACL entry to use the port number that the hosts use.

If no inbound ACL is configured on the interface you specify, you can have Cisco CP apply an ACL to the interface. You can choose a recommended policy, or a policy that simply monitors reported NAC postures.

- **Strict Validation (Recommended)**—Cisco CP applies an ACL that denies all traffic (**deny ip any any**). Admission to the network is determined by the NAC validation process. By default, all traffic is denied except the traffic found to be valid based on the policy configured on the NAC policy server.
- **Monitor NAC Postures**—Cisco CP applies an ACL that permits all traffic (**permit ip any any**). After the NAC validation process, the router may receive policies from the NAC server that deny access to certain hosts. You can use the **Monitor NAC Postures** setting to determine the impact of NAC configuration on the network. After you have done so, you can modify the policies on the NAC policy server, and then reconfigure NAC on the router to use **Strict Validation**, by changing the ACL applied to the interface to **deny ip any any** using the Cisco CP Firewall Policy feature.

NAC Exception List

You can identify hosts that must be allowed to bypass the NAC validation process. Typically, hosts such as printers, IP phones, and hosts without NAC posture agent software installed are added to the exception list.

If there are hosts without static addresses on your network it is recommended that they be entered in the agentless host policy, and not in the NAC exception list. The NAC exception policy may not work properly if host IP addresses change.

If you are using the NAC wizard and you do not need to configure a NAC exception list, you can click **Next** without entering information in this window. As an alternative or as a complement to the NAC exception list, the wizard allows you to configure an agentless host policy in another window.

IP Address/MAC Address/Device Type, Address/Device, and Policy Columns

These columns contain information about a host in the exception list. A host can be identified by its IP address, MAC address, or the type of device it is. If it is identified by an address, the IP address or MAC address is shown in the row along with the name of the policy that governs the host access to the network.

Add, Edit, and Delete Buttons

Build the exception list by clicking **Add** and entering information about a host. You can use the **Add** button as many times as you need to.

Choose a row and click **Edit** to change information about a host. Click **Delete** to remove information about a host from this window. The Edit and Delete buttons are disabled when there is no information in this list.

Add or Edit an Exception List Entry

Add or edit the information in an exception list entry in this window.

Type List

Hosts are chosen by the way they are identified. This list contains the following selections:

- IP Address—Choose this if you want to identify the host by its IP address.
- MAC Address—Choose this if you want to identify the host by its MAC address.
- Cisco IP Phone—Choose this if you want to include the Cisco IP phones on the network in the exception list.

Specify Address Field

If you choose IP Address or MAC Address as the host type, enter the address in this field. If you choose a device type, this field is disabled.

Policy Field

If you know the name of the exception policy, enter it in this field. Click the button with three dots to the right of the Policy field to choose an existing policy or to display a dialog box in which you can create a new policy.

Choose an Exception Policy

Choose the policy that you want to apply to the host. When you choose a policy, the redirect URL specified for the policy appears in a read-only field, and the access rule entries for the policy are displayed.

If no policies are available in the list, click **Cancel** to return to the wizard screen, and then choose the option that allows you to add a policy.

Choose the policy that you want to apply to the excepted host from the list. If there are no policies in the list, click **Cancel** to return to the wizard. Then choose **Create a new policy** and choose it in the Add to the Exception List window.

Redirect URL: URL Field

This read-only field displays the redirect URL associated with the policy that you choose. Hosts to which this policy is applied are redirected to this URL when the attempt to access the network.

Preview of Access Rule

The Action, Source, Destination, and Service columns show the ACL entries in the access rule associated with the policy. These columns are empty if no ACL is configured for this policy.

Add Exception Policy

Create a new exception policy in this window.

To create a new exception policy, enter a name for the policy, and either specify an access rule that defines the IP addresses that hosts in the exception list can access, or enter a redirect URL. The redirect URL should contain remediation information that enables users to update their virus definition files. You must provide either an access rule name or a redirect URL. You can specify both.

Name Field

Enter the name for the policy in this field. Do not use question mark (?) characters or space characters in policy names. Limit each policy name to no more than 256 characters.

Access Rule Field

Enter the name of the access rule that you want to use, or click the button to the right of this field to browse for an access rule or create a new access rule. The access rule must contain permit entries that specify the IP addresses that hosts on the exception list can connect to. The access rule must be a named ACL; numbered ACLs are not supported.

Redirect URL Field

Enter a URL that contains the remediation information for your network. This information might contain instructions for downloading virus definition files.

A remediation URL might look like the following:

```
http://172.23.44.9/update
```

Redirect URLs are usually of the form `http://URL`, or `https://URL`.

Agentless Host Policy

If a policy for agentless hosts exists on the Cisco Secure ACS server, the router can use that policy to handle hosts without installed posture agents. This method of handling agentless hosts can be used as an alternative or as a complement to a NAC exception list. If you are using the NAC wizard and you do not need to configure an agentless host policy, you can click **Next** without entering information in this window.

Authenticate Agentless Hosts Check Box

Check this box to indicate that you want to use the agentless hosts policy on the Cisco Secure ACS server.

Username and Password Fields

Some Cisco IOS software images require that a username and password be supplied along with the request to the Cisco Secure ACS server. If this is required, enter the username and password configured on the Cisco Secure ACS server for this purpose. If the Cisco IOS software image does not require this information, these fields do not appear.

Configuring NAC for Remote Access

Configuring NAC for remote access allows you to modify the ACLs that NAC configuration creates so that they will permit Cisco CP traffic. Specify the hosts that must be able to use Cisco CP to access the router.

Enable Cisco CP Remote Management

Check this box to enable Cisco CP remote management on the named interface.

Host/Network Address Fields

If you want Cisco CP to modify the ACL to allow Cisco CP traffic from a single host, choose **Host Address** and enter the IP address of a host. Choose **Network Address** and enter the address of a network and a subnet mask to allow Cisco CP traffic from hosts on that network. The host or network must be accessible from the interfaces that you specified. Choose **Any** to allow Cisco CP traffic from any host connected to the specified interfaces.

Modify Firewall

Cisco CP checks each ACL applied to the interface specified in this configuration to determine if it blocks any traffic that should be allowed through the firewall so that the feature you are configuring will work.

Each interface is listed, along with the service currently being blocked on that interface, and the ACL that is blocking it. If you want Cisco CP to modify the ACL to allow the traffic listed, check the **Modify** box in the appropriate row. If you want to see the entry that Cisco CP will add to the ACL, click the **Details** button.

In the following table, FastEthernet0/0 has been configured for NAC. This interface is configured with the services shown in the Service column.

Interface	Service	ACL	Action
FastEthernet0/0	RADIUS Server	101 (INBOUND)	[ ] Modify
FastEthernet0/0	DNS	100 (INBOUND)	[ ] Modify
FastEthernet0/0	DHCP	100 (INBOUND)	[ ] Modify
FastEthernet0/0	NTP	101 (INBOUND)	[ ] Modify
FastEthernet0/0	VPN	190 (INBOUND)	[ ] Modify

Details Window

This window displays the entries that Cisco CP will add to ACLs to allow services needed for the service you are configuring. The window might contain an entry like the following:

```
permit tcp host 10.77.158.84 eq www host 10.77.158.1 gt 1024
```

In this case, web traffic whose port number is greater than 1024 is permitted from the host 10.77.158.84 on the local network to the host 10.77.158.1

Summary of the configuration

This window summarizes the information you entered, and allows you to review it in a single window. You can use the Back button to return to any wizard screen to change information. Click **Finish** to deliver the configuration to the router.

Here is an example of a NAC configuration summary:

```
NAC Interface:  FastEthernet0/1.42
Admission Name::  SDM_EOU_3


AAA Client Source Interface: FastEthernet0/1.40
NAC Policy Server 1:   10.77.158.54

Exception List
-------------------------------------------------------------------------
Address/Device     IP Address       (22.22.22.2) newly added
Policy Details:
Policy Name:          P55
       Redirect URL:  http://www.fix.com
        Access Rule:   test11

-------------------------------------------------------------------------


Enabled agentless host policy
Username:  bill
Password:   ******
```

In this example, RADIUS packets will have the IP address of FastEthernet 0/1.40. NAC is enabled on FastEthernet 0/1.42, and the NAC policy that the wizard applied is SDM_EOU_3. One host has been named in the exception list, and its access to the network is controlled by the exception policy P55.

Edit NAC Tab

The Edit NAC tab lists the NAC policies configured on the router and enables you to configure other NAC settings. A NAC policy must be configured for each interface on which posture validation is to be performed.

NAC Timeouts Button

The router and the client use Extensible Authentication Protocol over Unformatted Data Protocol (EAPoUDP) to exchange posture information. Default values for EAPoUDP timeout settings are preconfigured, but you can change the settings. This button is disabled if there is no NAC policy configured on the router.

Agentless Host Policy Button

If a policy for agentless hosts exists on the Cisco Secure ACS server, the router can use that policy to handle hosts without installed posture agents. This method of handling agentless hosts can be used when such hosts do not have static IP addresses. This button is disabled if there is no NAC policy configured on the router.

Add, Edit, and Delete Buttons

These buttons allow you to manage the NAC policy list. Click **Add** to create a new NAC policy. Use the Edit and Delete buttons to modify and remove NAC policies. The Edit and Delete buttons are disabled when no NAC policies have been configured on the router.

Only the Add button is enabled when there is no NAC policy configured on the router. The Add button is disabled when all router interfaces are configured with a NAC policy.

NAC Policies List

The name, the interface to which the NAC policy is applied, and the access rule that defines the policy are included in the list. If you enabled NAC on an interface using the Create NAC wizard, the default NAC policy SDM_EOU_1 appears in this list.

NAC Components

This window provides a brief description of the EAPoUDP components that Cisco CP allows you to configure.

Exception Policies Window

NAC exception policies control the network access of hosts in the exception list. A NAC exception policy consists of a name, an access rule, and/or a redirect URL. The access rule specifies the destinations to which hosts governed by the policy have access. If a redirect URL is specified in the policy, the policy can point web clients to sites that contain information on how to obtain the latest available virus protection.

An example of a NAC policy entry is shown in the following table:

Name	Access Rule	Redirect URL
NACLess	nac-rule	http://172.30.10/update

Access rules associated with NAC policies must be extended ACLs, and must be named. An example of an access rule that might be used in a NAC policy is shown in the following table:

Action	Source	Destination	Service	Log	Attributes
permit	any	172.30.2.10	ip		

This rule permits any host governed by the policy to send IP traffic to the IP address 172.30.2.10.

Add, Edit, and Delete Buttons

Click the **Add** button to create a new exception policy. Use the **Edit** button to modify existing exception policies, and the **Delete** button to remove exception policies. The Edit and Delete buttons are disabled when there are no exception policies in the list.

NAC Timeouts

Configure the timeout values the router is to use for EAPoUDP communication with network hosts. The default, minimum, and maximum values for all settings are shown in the following table.

Value	Default	Minimum	Maximum
Hold Period Timeout	180 seconds	60 seconds	86400 seconds
Retransmission Timeout	3 seconds	1 second	60 seconds
Revalidation Timeout	36000 seconds	300 seconds	86400 seconds
Status Query Timeout	300 seconds	30 seconds	1800 seconds

Interface Selection

Choose the interface to which the NAC timeout settings are to apply.

Hold Period Timeout Field

Enter the number of seconds that the router is to ignore packets from clients that have just failed authentication.

Retransmit Timeout Field

Enter the number of seconds that the router is to wait before retransmitting EAPoUDP messages to clients.

Revalidation Timeout Field

The router periodically queries the posture agent on the client to determine the client's adherence to security policy. Enter the number of seconds that the router should wait between queries.

Status Query Timeout Field

Enter the number of seconds that the router should wait between queries to the posture agent on the host.

Reset to Defaults Button

Click this button to reset all NAC timeouts to their default values.

Configure these timeout values globally Check Box

Click this check box to have these values apply to all interfaces.

Configure a NAC Policy

A NAC policy enables the posture validation process on a router interface, and can be used to specify the types of traffic that are to be exempt from posture validation in the admission control process.

Name Field

Enter a name for the policy.

Select an Interface List

Choose the interface to which you want to apply the NAC policy. Choose an interface that connects network clients to the router.

Admission Rule Field

You can use an access rule to exempt specific traffic from triggering the admission control process. It is not required. Enter the name or the number of the access rule that you want to use for the admission rule. You can also click the button to the right of this field and browse for the access rule, or create a new access rule.

The access rule must contain deny statements that specify the traffic that is to be exempted from the admission control process. No posture validation triggering occurs if the access rule contains only deny statements.

An example of ACL entries for a NAC admission rule follows:

```
deny udp any host 10.10.30.10 eq domain
deny tcp any host 10.10.20.10 eq www
```
permit ip any any

The first deny statement exempts traffic with a destination of port 53 (domain), and the second statement exempts traffic with a destination of port 80 (www). The permit statement ending the ACL ensures that posture validation occurs.

How Do I...

The following topics contain procedures for performing tasks that the Create NAC wizard does not help you to do.

How Do I Configure a NAC Policy Server?

The router must have a connection to a Cisco Secure Access Control Server (ACS) running ACS software. The ACS must be configured to use the RADIUS protocol in order to implement NAC. Documents at the following link explain how to install and configure Cisco Secure ACS for Windows Servers.

http://www.cisco.com/en/US/docs/net_mgmt/cisco_secure_access_control_server_for_windows/4.2/roadmap/DGuide42.html

How Do I Install and Configure a Posture Agent on a Host?

If you are a registered Cisco.com user, you can download Cisco Trust Agent (CTA) software from the following link:

http://www.cisco.com/cgi-bin/tablebuild.pl/cta

The document “Administrator Guide for Cisco Trust Agent, Release 2.1, With Bundled Supplicant” at the following link explains how to install and configure CTA software on a host.

http://www.cisco.com/en/US/docs/security/cta/2.1.103.0_supplicant/admin_guide/cta_bundled_with_supplicant.html

The specific installation procedures required to install third-party posture agent software and the optional remediation server vary depending on the software in use. Consult the vendor documentation for complete details.

CHAPTER 43

Cisco Common Classification Policy Language

Cisco Common Classification Policy Language (C3PL) is a structured replacement for feature-specific configuration commands. C3PL allows you to create traffic policies based on events, conditions, and actions. Cisco Configuration Professional (Cisco CP) uses C3PL to create the policy maps and class maps that the following help topics describe.

Policy Map

Policy maps specify the actions to be taken when traffic matches defined criteria. Traffic types and criteria are defined in class maps associated with a policy map. In order for a router to use the information in a policy map and its associated class maps, the policy map must be associated with a zone pair. See Zone-Based Policy Firewall for more information on configuring zones and zone pairs. See Policy Map Screens for a description of the screens used to configure policy maps.

Policy Map Screens

Use the policy map windows to review, create and edit policy maps for QoS, HTTP, and other types of traffic. The top portion of the window lists the configured policy maps, and the bottom portion displays the details of the highlighted policy map. If you need to edit a policy map or see more detail, click **Edit** to display a dialog that lets you view information and make changes.

This help topic provides a general description for the policy map windows and some sample data.

Add

Click **Add** to display a dialog in which you can configure a policy map.

Edit

Click **Edit** to display a dialog in which you can edit the selected policy map. The **Edit** button is disabled if no policy maps have been configured.

Delete

Click **Delete** to remove the selected policy map.

Policy Map List Area

This area lists the policy maps configured for the particular protocol or feature. Select a policy map to display details in the lower part of the screen. The following example shows two IM policies.

Policy Map Name	Description
im-pmap-g	guest policy
im-pmap-e	employee policy

Details of Policy Map

The details of the selected policy map shows the policy map configuration. The detail shown varies according to the type of policy map.

HTTP, IM, P2P, IMAP, and POP3 display a match class name, action and log column. The following table shows detail for an IM policy map. The router blocks AOL traffic, but allows all other types of IM traffic.

Match Class Name	Action	Log
aol-cmap	Disabled	Disabled
class-default	Enabled	Disabled

Protocol Inspection, SMTP, and SUNRPC policy map detail includes Match Class Name and Action columns.The following table shows detail for a SUNRPC policy map.

Match Class Name	Action
cmap-sunrpc1	Allow
cmap-sunrpc2	None

Add or Edit a QoS Policy Map

Use this information as you add or edit a QoS policy map.

Policy Name and Description

If you are creating a new policy map, enter a name and a description for it in these fields. If you are editing a policy map, these fields are display only.

Class Map, Queuing, Set DSCP, and Drop

These columns summarize the information about each class map in the policy map. The following example entry is for a voice class map:

```
Voice-FastEthernet0/1  LLQ 70%     ef          No
```

This class map uses low latency queuing, and 70% of the bandwidth for this interface. The DSCP value is set to ef, and packets of this type are not dropped.

Click the **Add**, **Edit**, **Delete**, **Move Up**, and **Move Down** buttons to modify the class map information in this list.

Associate a Policy Map to Interface

In this screen, associate a policy map to the chosen interface.

Field Reference

Table 43-1 Associate a Policy Map Fields

Element	Description
QoS Group Name	The name of the QoS group.
Policy Map	Choose the policy map that you want to associate with the interface.
Policy Map details	
Class Map	The Class Map column displays the class maps that the policy map contains.

Queuing	The Queuing column displays the type of queuing used by the class map, and the percentage of bandwidth allocated to the class. For example, the Queuing column might contain the following entries:
	`LLQ - 33%`
	`CBWFQ - 5%`
	`CBWFQ - 5% Remaining`
	`Fair Queue`
	One class map uses Low Latency Queuing (LLQ), two class maps use Class-Based Weighted Fair Queuing (CBWFQ), and one uses Fair Queuing. The percentages show the bandwidth, or remaining bandwidth allocated to these class maps.

Shaping	The Shaping column indicates whether shaping is configured for the class map or not. • Yes—Shaping is configured. • No—Shaping is not configured.
Policing	The Policing column indicates whether policing is configured for the class map or not. • Yes—Policing is configured. • No—Policing is not configured.
Set DSCP	The Set DSCP column lists the DSCP markings used in the class map.
Drop	

Add an Inspection Policy Map

Inspection policy maps specify the action that the router will take for traffic that matches the criteria in the associated class maps. The router can allow the traffic to pass, can drop the traffic and optionally log the event, or can inspect the traffic.

The name and description that you enter will be visible in the Inspect Policy Maps window. The Class Map and Action columns display the class maps associated with this policy map, and the action that the router will take for the traffic that the class map describes. Click **Add** to add a new class map to the list and configure the action. Click **Edit** to modify the settings for a class map. Click the **Move Up**, and **Move Down** buttons to change the order in which the class maps are evaluated.

Layer 7 Policy Map

This window allows you to select a Layer 7 Policy map to use to inspect an application that you have selected. The window displays the policy maps available for that application. Choose a policy map and click **OK**.

Application Inspection

Application inspection policies are applied at Layer 7 of the Open Systems Interconnect (OSI) model, where user applications send and receive messages that allow the applications to offer useful capabilities. Some applications might offer undesired or vulnerable capabilities, so the messages associated with these capabilities must be filtered to limit activities on the application services.

Cisco IOS Software Zone-Policy Firewall offers application inspection and control on the following application services: HTTP, SMTP, POP3, IMAP, SUNRPC, P2P, and IMAP applications. See the following links for more information

- Add an HTTP Inspection Class Map
- Add or Edit an SMTP Class Map
- Add or Edit a POP3 Class Map
- Add or Edit an IMAP Class Map
- Add or Edit a SUNRPC Class Map

- Add or Edit a Point-to-Point Class Map
- Add or Edit an Instant Messaging Class Map

Configure Deep Packet Inspection

Layer 7 (application) inspection augments Layer 4 inspection with the capability to recognize and apply service-specific actions, such as selectively blocking or allowing file search, file transfer, and text chat capabilities. Service-specific capabilities vary by service.

If you are creating a new policy map, enter a name in the **Policy Map Name** field. You can also add a description. Click **Add > New Class Map** to create a new Point-to-Point class map. Add or Edit a Point-to-Point Class Map provides information on how to create this type of class map. Click **Add > class default to add the default class map.**

When the class map appears in the table, specify the action that you want taken when a match is found, and whether you want matches logged. You can specify **<None>**, **Reset**, or **Allow**. In the following example, there are P2P class maps for gnutella and eDonkey.

Match Class Name	Action	Log
gnutellaCMap	Allow	
eDonkeyCMap	Reset	X

Class Maps

Class maps define the traffic that a Zone-Policy Based Firewall (ZPF) selects for policy application. Layer 4 class maps sort the traffic based on the following criteria:

- Access group—A standard, extended, or named Access Control List can filter traffic based on source and destination IP address and on source and destination port.
- Protocol—The Layer 4 protocols (TCP, UDP, and ICMP) and application services such as HTTP, SMTP, DNS, etc. Any well-known or user-defined service known to PAM may be specified.

- Class map—A subordinate class map providing additional match criteria can be nested inside another class map.

Class Maps can apply “match any” or “match all” operators to determine how to apply the match criteria. If “match any” is specified, traffic must meet only one of the match criteria in the class map. If “match all” is specified, traffic must match all of the class map’s criteria to belong to that particular class.

Associate Class Map

To associate a class map with an inspect policy map, complete the following tasks.

Step 1 Specify a class map name by clicking the button to the right of the name field and choosing **Add a Class Map**, **Select a Class Map**, or **class-default**.

Step 2 In the Action box, click **Pass**, **Drop**, or **Inspect**. If you click Drop, you can optionally click **Log** to have the drop event logged. If you click Inspect, click **Advanced Options** to specify the parameter maps, inspection policies, or policing that you want for the traffic in this class.

Step 3 Click **OK** to close this dialog and return to the Add dialog or the Edit Protocol Inspection Policy Map dialog.

Class Map Advanced Options

When you choose the inspect action for traffic, you can specify parameter maps, application inspection, and ZPF policing.

Inspect Parameter Map

Inspect parameter maps specify TCP, DNS, and UDP timeouts and session control parameters. You can select an existing parameter map. If no parameter map is configured, this field is disabled. Click **View** to display the selected parameter map without leaving this dialog.

URL Filtering Parameter Map

URL filtering parameter maps can specify URL filtering servers and local URL lists. You can select an existing parameter map. If no parameter map is configured, this field is disabled. Click **View** to display the selected parameter map without leaving this dialog.

Enable Application Inspection

An application inspection policy specifies the types of data to inspect in packets of a specified application. You can select an existing application inspection policy. If no application inspection policy is configured, this field is disabled. Click **View** to display the selected application inspection policy without leaving this dialog.

Police Rate and Burst

You can limit traffic to a specified police rate and specify a burst value. The police rate can be a value between 8,000 and 2,000,000,000 bits per second. The burst rate can be a value between 1,000 and 512,000,000 bytes.

QoS Class Map

Use this window to display and edit QoS class map information. QoS class maps are used in QoS policy maps to define types of traffic.

Click a class map name to display details about that class map in the Details of Class Map area.

The details of a class map show which protocols are matched to define the traffic. The following example shows details of a voice signaling class map.

```
Details of Class Map:SDMSignal-FastEthernet0/1

    Item Name                          Item Value
Match Protocols                        h323,rtcp
```

H.323 and RTCP are the voice signaling protocols to be matched.

Add or Edit a QoS Class Map

Use this information to help add or edit a QoS class map. If you are adding a new QoS class map, click the button on the right of the field and choose either **Add a Classmap** or **Select a Classmap** from the context menu.

See the information in Action Pane to learn about the Drop, Set DSCP, and Queuing options.

Add or Edit a QoS Class Map

Enter a name and description of the QoS class Map you are creating so that it can be easily identified and used. Click Classification Pane for a description of the Any, All, and Edit buttons in the Classification box.

Select a Class Map

Click the name of the class map that you want to choose, and click **OK**. The class map entry is added to the window from which you invoked this dialog.

Deep Inspection

Deep inspection allows you to create class maps for parameters specific to an application. For example, you can create class maps for the common P2P applications such as eDonkey, gnutella, and kazaa2.

Class Map and Application Service Group Windows

Use the class map windows to review, create, and edit class maps for protocols such as HTTP, SMTP, and POP3. The Class Map area of the window lists the configured class maps, and the bottom part displays the details for the selected class map. To edit a class map or see more detail, click **Edit** to display a dialog that lets you view information and make changes.

Add

Click **Add** to create a new class map of the type you have selected and enter the configuration in the displayed dialog.

Edit

Click **Edit** to change the configuration of the selected class map.

Delete

Click **Delete** to remove the selected class map. Cisco CP may display dialogs if there are dependencies associated with this configuration, such as subordinate class maps or parameter maps that could be used by other class maps.

Class Map Area

This area displays the class maps configured for the protocol that you selected. It contains the names of the configured class maps and other relevant information.

QoS Class Maps

QoS class maps are displayed in a table with a Class Map Name and a Description column. A sample table follows.

Class Map Name	Description
CMAP-DMZ	FTP and HTTP QoS class map
CMAP-3	Test

Inspection, HTTP, SMTP, SUN RPC, IMAP and POP3 Class Maps

These types of class maps have a Class Map Name and a Used By column A sample table for HTTP follows.

Class Map Name	Used By
http-rqst	pmap-5
http-rsp-body	pmap-5

Instant Messaging Service Groups and Peer-to-Peer Application Service Groups

Instant Messaging Service group and peer-to-peer (P2P) application service groups have an additional column because class maps are configured for a specific application, such as the Yahoo! Messenger instant messaging application or the gnutella P2P application. The following table shows sample data for P2P application service groups

Class Map Name	Used By	Class Map Type
cmap-gnutella	pmap-7	gnutella
cmap-edonkey	pmap-7	edonkey
cmap-bittorrent	pmap-7	bittorrent

Details of Class Map

The Details of Class Map area shows the configuration for a particular class map. It has an Item Name and an Item Value column.

Item Name

The name of the configuration setting. For example, an HTTP class map might have settings for Request Header, Port Misuse, and Protocol Violation.

Item Value

The value of the configuration setting. For example, HTTP Request Header setting value might be Length > 500, and the Port Misuse flag might be disabled.

More Information About Class Map Details

For more information about class map details displayed in these windows, click any of the following links:

- Add or Edit a QoS Class Map
- Add or Edit an Inspect Class Map
- Add an HTTP Inspection Class Map
- Add or Edit an Instant Messaging Class Map
- Add or Edit a Point-to-Point Class Map
- Add or Edit an SMTP Class Map

- Add or Edit a SUNRPC Class Map
- Add or Edit an IMAP Class Map
- Add or Edit a POP3 Class Map

Add or Edit an Inspect Class Map

Creating an inspect class map enables you to make a wide variety of traffic available for inspection. Enter a name to identify this class map in the **Class Name** field. You can also enter a description. If you are editing a class map, you cannot change the name. When you have specified the conditions that you want the class to map, click **OK**.

Specifying whether you want the class to match any or all of the conditions

Click **Any** if the class needs to match one or more conditions that you choose. Click **All** if the class must match all the conditions.

Choosing what you want the inspect class map to match

Browse what you want the class map to match in the left column. Click the plus sign (**+**) next to a node to display the child nodes. For example, click **HTTP** to display the child nodes http and https. To choose an item, click it and then click **Add>>**. To remove an item that you have added to the column on the right, click it and then click **<<Remove**.

Changing the match order

If you chose **Any** to match any of the conditions, you may want to change the match order of the items in the right column. To move an item up the list, click it and then click **Up**. To move an item down the list, click it and then click **Down**. The Up button is disabled when you click the item at the top of the list. The Down button is disabled when you click the item at the bottom of the list.

Associate Parameter Map

This dialog displays the parameter maps that you can associate with the class map. Click the **Select** box next to the parameter map you want to associate with the class map.

Add an HTTP Inspection Class Map

HTTP inspection class maps allow you to make a wide variety of HTTP request, response, and request response data available for inspection.

To create an HTTP inspection class map, follow these steps:

Step 1 Enter a class name to identify the class map. You can also enter a description.

Step 2 Click the branch in the HTTP tree that contains the type of data you want to make available for inspection. You can create a class map for HTTP requests, responses, and request-responses.

Step 3 Click the appropriate sub-branch to further specify the type of data you want to include.

Step 4 Configure the class map data in the fields displayed.

Step 5 To specify match conditions, click **Any conditions below** if the class map must match only one or more conditions. Click **All the specified below** if the class map must match all the conditions that you specified.

HTTP Request Header

Enter class map criteria for HTTP request header attributes.

Length Greater Than

Click this box to specify a global request header length that a packet should not exceed, and enter the number of bytes.

Count Greater Than

Click this box to specify a limit to the total number of request header fields that a packet should not exceed, and enter the number of fields.

Regular Expressions

Click this box to specify regular expressions to be matched against. Choose an existing regular expression class map, or create a new one that will match the strings that you are inspecting for. See Add or Edit Regular Expression for more information about creating regular expressions. To examine an existing map without leaving this dialog, choose the map in the **Select an existing map** list, and click **View**.

Field Name and Configuration Options

You can include fields within the header to the inspection criteria and specify length, count, and strings to inspect for. Click **Add** to include a field, and enter criteria in the dialog displayed.

HTTP Request Header Fields

Choose the type of header field from the list, and specify the inspection criteria for it.

Length Greater Than

Click this box to specify a length that this field should not exceed, and enter the number of bytes. For example, you might block a request whose cookie field exceeds 256 bytes, or whose user-agent field exceeds 128 bytes.

Count Greater Than

Click this box to specify the number of times that this field can be repeated in the header, and enter a number. For example you might block a request that has multiple content-length header lines by entering the value 1. This example is an effective measure for preventing session smuggling.

Regular Expressions

Click this box to specify regular expressions to be matched against. Choose an existing regular expression class map, or create a new one that will match the strings that you are inspecting for. See Add or Edit Regular Expression for more

information about creating regular expressions. To examine an existing map without leaving this dialog, choose the map in the **Select an existing map** list, and click **View**.

Match Field

Check this box to match the class map to the field type that you chose.

Other Fields in This Dialog

Depending on which HTTP header field you choose, additional fields may be displayed in this dialog, enabling you to specify additional criteria. For example, if you choose the content-type field, you can inspect for content type mismatches between the request and the response, unknown content types, and protocol violations for the particular content type. If you choose the transfer-encoding field, you can inspect for various types of compression and encoding.

HTTP Request Body

You can inspect an HTTP request body for length and character strings.

Length

Check this box and choose **Greater than (>)** to specify an upper limit to the length of the request body. Choose **Less than (<)** to specify a lower limit.

Regular Expressions

To inspect for strings, click this box. Choose an existing regular expression class map, or create a new regular expression class map that will match the strings you are inspecting for. See Add or Edit Regular Expression for more information on how to create regular expressions. To examine an existing map without leaving this dialog, choose it in the Select an existing map list, and click **View**.

HTTP Request Header Arguments

You can inspect for the length of the arguments sent in a request, and inspect for strings that match regular expressions that you have configured.

Length greater Than

Click this box to specify the number of bytes that the total length of request header arguments should not exceed.

Regular Expressions

Click this box to specify regular expressions to be matched against. Choose an existing regular expression class map, or create a new one that will match the strings you are inspecting for. See Add or Edit Regular Expression for more information on how to create regular expressions. To examine an existing map without leaving this dialog, choose it in the Select an existing map list, and click **View**.

HTTP Method

HTTP methods indicate the purpose of an HTTP request. Choose the HTTP methods in the Method List column that you want to inspect and check the **Select** box next to the method.

Request Port Misuse

HTTP port #80 is sometimes used by IM, P2P, tunneling, and other applications. Check the types of port misuse that you want to inspect for. You can inspect for any type of port misuse, port misuse by IM applications, P2P application port misuse, and misuse by tunneling applications

Request URI

Enter the Universal Resource Identifier (URI) criteria that you want to include in the class map.

Length Greater Than

Click this box to specify a URI length that a packet should not exceed, and enter the number of bytes.

Regular Expressions

Click this box to specify regular expressions to be matched against. Choose an existing regular expression class map, or create a new one that will match the strings you are inspecting for. See Add or Edit Regular Expression for more information on how to create regular expressions. To examine an existing map without leaving this dialog, choose it in the **Select an existing map** list, and click **View**.

Sample Use Case

Configure an HTTP class map to block a request whose URI matches any of the following regular expressions:

".*cmd.exe"

".*sex"

".*gambling"

Response Header

Enter the criteria for HTTP response headers that you want to include in the class map.

Length Greater Than

Click this box to specify a global response header length that a packet should not exceed, and enter the number of bytes.

Count Greater Than

Click this box to specify a limit to the total number of response header fields that a packet should not exceed, and enter the number of fields.

Regular Expressions

Click this box to specify regular expressions to be matched against. Choose an existing regular expression class map, or create a new one that will match the strings you are inspecting for. See Add or Edit Regular Expression for more

information on how to create regular expressions. To examine an existing map without leaving this dialog, choose it in the **Select an existing map** list, and click **View**.

Response Header Fields

Choose the type of header field from the list, and specify the inspection criteria for it.

Length Greater Than

Click this box to specify a field length that a packet should not exceed, and enter the number of bytes.

Count Greater Than

Click this box to specify a limit to the total number of fields of this type that a packet should not exceed, and enter the number of fields.

Regular Expressions

Click this box to specify regular expressions to be matched against. Choose an existing regular expression class map, or create a new one that will match the strings you are inspecting for. See Add or Edit Regular Expression for more information on how to create regular expressions. To examine an existing map without leaving this dialog, choose it in the Select an existing map list, and click **View**.

Other Fields in This Dialog

Depending on which HTTP header field you choose, additional fields may be displayed in this dialog, enabling you to specify additional criteria. For example, if you choose the **content-type** field, you can inspect for content type mismatches between the request and the response, inspect for unknown content types, and inspect for protocol violations for the particular content type. If you choose the **transfer-encoding** field, you can inspect for various types of compression and encoding.

Match Field

Check this box the class map to match the field type that you chose.

HTTP Response Body

Specify the HTTP response body criteria to inspect for.

Java Applets in HTTP Response

Check this box to inspect for Java applets in the HTTP response.

Length

Check this box and choose **Greater than (>)** to specify an upper limit to the response body length. Choose **Less than (<)** to specify a lower limit.

Regular Expressions

Click this box to specify regular expressions to be matched against. Choose an existing regular expression class map, or create a new one that will match the strings you are inspecting for. See Add or Edit Regular Expression for more information on how to create regular expressions. To examine an existing map without leaving this dialog, choose it in the **Select an existing map** list, and click **View**.

HTTP Response Status Line

Click this box and specify regular expressions to be matched against response status lines. Choose an existing regular expression class map, or create a new one that will match the strings you are inspecting for.

Sample Use Case

Configure the router to log an alarm whenever an attempt is made to access a forbidden page. A forbidden page usually contains a 403 status-code and the status line looks like “HTTP/1.0 403 page forbidden\r\n.”

The regular expression for this is the following:

```
[Hh][Tt][Tt][Pp][/][0-9][.][0-9][ \t]+403
```

Logging is specified in the policy map to which the HTTP class map is associated.

See Add or Edit Regular Expression for more information on how to create regular expressions. To examine an existing map without leaving this dialog, choose it in the **Select an existing map** list, and click **View**.

Request/Response Header Criteria

Enter class map criteria for HTTP request/response headers.

Length Greater Than

Click this box to specify a global request/response header length that a packet should not exceed, and enter the number of bytes.

Count Greater Than

Click this box to specify a limit to the total number of request/response header fields that a packet should not exceed, and enter the number of fields.

Regular Expressions

Click this box to specify regular expressions to be matched against. Choose an existing regular expression class map, or create a new one that will match the strings you are inspecting for. See Add or Edit Regular Expression for more information on how to create regular expressions. To examine an existing map without leaving this dialog, choose it in the **Select an existing map** list, and click **View**.

HTTP Request/Response Header Fields

Choose the HTTP Request/Response header field that you want to include in the class map.

Length Greater Than

Click this box to specify a field length that a packet should not exceed, and enter the number of bytes.

Count Greater Than

Click this box to specify a limit to the total number of fields of this type that a packet should not exceed, and enter the number of fields.

Regular Expressions

Click this box to specify regular expressions to be matched against. Choose an existing regular expression class map, or create a new one that will match the strings you are inspecting for. See Add or Edit Regular Expression for more information on how to create regular expressions. To examine an existing map without leaving this dialog, choose it in the **Select an existing map** list, and click **View**.

Other Fields in This Dialog

Depending on which HTTP header field you choose, additional fields may be displayed in this dialog, enabling you to specify additional criteria. For example, if you choose the **content-type** field, you can inspect for content type mismatches between the request and the response, inspect for unknown content types, and inspect for protocol violations for the particular content type. If you choose the **transfer-encoding** field, you can inspect for various types of compression and encoding.

Match Field

Check this box if you want the class map to match the field type that you chose.

Request/Response Body

The router can inspect for request/response body length and specific text strings inside the body of the request/response.

Length

Check this box and choose **Greater than (>)** to specify an upper limit to the request/response body length. Choose **Less than (<)** to specify a lower limit.

Regular Expressions

Click this box to specify regular expressions to be matched against. Choose an existing regular expression class map, or create a new one that will match the strings you are inspecting for. See Add or Edit Regular Expression for more information on how to create regular expressions. To examine an existing map without leaving this dialog, choose it in the **Select an existing map** list, and click **View**.

Request/Response Protocol Violation

To inspect for protocol violations in HTTP request/responses, click **Protocol Violation**.

Add or Edit an IMAP Class Map

Creating a class map for Internet Message Access Protocol (IMAP) inspection can help ensure that users are using secure authentication mechanisms to prevent compromise of user credentials.

Enter a name to identify this class map in the **Class Name** field. You can also enter a description. If you are editing a class map, you cannot change the name.

Click **Login string in clear text** to have the router inspect IMAP traffic for nonsecure logins.

Click **Invalid protocol command** to have the router inspect IMAP traffic for invalid commands.

Add or Edit an SMTP Class Map

Simple Mail Transfer Protocol (SMTP) class maps enable you to limit content length and enforce protocol compliance.

Enter a name to identify this class map in the **Class Name** field. You can also enter a description in the field provided.

In the **Maximum data transfer allowed in a session** field, enter the maximum number of bytes the router should allow for an SMTP session.

Add or Edit a SUNRPC Class Map

SUN Remote Procedure Call (SUNRPC) class maps allow you to specify the number of the program whose traffic you want the router to inspect.

Enter a name to identify this class map in the **Class Name** field. You can also enter a description. If you are editing a class map, you cannot change the name.

Click **Add** in the **Match Program Number** box to add a program number.

Add or Edit an Instant Messaging Class Map

Instant Messaging (IM) class maps allow you to specify the type of instant messaging and whether you want traffic for all IM services inspected, or only traffic for the text chat service.

In the **Class Map Type** field, choose **aol** for America Online, **msnmsgr** for Microsoft Networks Messenger, or choose **ymsgr** for Yahoo! Messenger.

In the Match Criteria box, click **All services**, or click **Text chat services** if you want only text chat traffic to be inspected.

Add or Edit a Point-to-Point Class Map

A P2P class map specifies a P2P application and the match criteria. Only one application can be specified per class map.

Class Name

Enter a new class name to create a new class map. Clicking the button at the right of the field allows you to select existing class maps to edit. You can edit the match criteria for a class map, but you cannot change the class map type.

Class Map Type

You can create a P2P class map for the following types of P2P services:

- eDonkey
- fasttrack
- gnutella
- kazaa2

Match Criteria and Value

Click **Add** to enter match criteria to specify the type of connections to be identified by the traffic class.

You can specify that file transfer connections be identified by the traffic class for fasttrack, gnutella, and kazaa2. For eDonkey, you can specify that file transfer connections, filename requests (search file name), and text chats be identified by the traffic class. The value for the match criteria can be any regular expression. For example, to specify that all file transfer connections be identified, enter *.

Add P2P Rule

Enter match criteria to specify the type of connections that are to be identified by the traffic class. You can specify that file transfer connections be identified by the traffic class for fasttrack, gnutella, and kazaa2. For eDonkey, you can specify that file transfer connections, filename requests (search-file-name), and text chats be identified by the traffic class. The value for the match criteria can be any regular expression. For example, to specify that all file transfer connections be identified, enter *.

Add or Edit a POP3 Class Map

Creating a class map for Post Office Protocol version 3 (POP3) inspection can help ensure that users are using secure authentication mechanisms to prevent compromise of user credentials.

Enter a name to identify this class map in the **Class Name** field. You can also enter a description. If you are editing a class map, you cannot change the name.

Click **Login string in clear text** to have the router inspect POP3 traffic for nonsecure logins.

Click **Invalid protocol command** to have the router inspect POP3 traffic for invalid commands.

Parameter Maps

Parameter Maps specify inspection behavior for Zone-Policy Firewall, for parameters such as denial-of-service protection, session and connection timers, and logging settings, Parameter Maps are also applied with Layer 7 class maps and policy maps to define application-specific behavior, such as HTTP objects, POP3 and IMAP authentication requirements, and other application-specific information.

Parameter Map Windows

The parameter map windows list the configured parameter maps for protocol information, URL filtering, regular expressions, and other types of parameter maps. If a parameter map has been associated with a class map, the class map name appears in the Used By column. The details of the selected parameter map are displayed in the bottom half of the window. You can add, edit, and delete parameter maps. Cisco CP informs you if you attempt to delete a parameter map that is being used by a class map.

For more information about the parameter maps displayed in these windows, click any of the following links:

- Add or Edit a Parameter Map for Protocol Information
- General Settings for URL Filtering
- Add or Edit a URL Filter Server
- Local URL List
- Add or Edit Regular Expression

Add or Edit a Parameter Map for Protocol Information

It may be necessary to identify servers for specific types of applications, such as IM applications so that you can restrict use to a particular activity, such as text chat.

Parameter Map Name

Enter a name that conveys the use of this parameter map. For example, if you are creating a server list for Yahoo! Instant Messenger text chat servers, you can enter the name **ymsgr-pmap**.

Server Details

This area of the screen is a list of server names, server IP addresses, or IP address ranges.

Add or Edit a Server Entry

You can provide the hostname or IP address of an individual server, or a range of IP addresses assigned to a group of servers.

You can enter a hostname in the **Name** field if the router is able to contact a DNS server on the network to resolve the server's IP address. To enter the IP address for one server, enter it in the **Single IP Address** field. If there are several servers that use an IP address range, use the **IP range** field. Enter the lowest IP address in the left-hand field and the highest IP address in the right hand field. For example to enter the range 103.24.5.67 through 99, enter **103.24.5.67** in the left-hand field and **103.24.5.99** in the right-hand field.

Add or Edit Regular Expression

A regular expression matches text strings either literally as an exact string, or by using *metacharacters* so you can match multiple variants of a text string. You can use a regular expression to match the content of certain application traffic; for example, you can match body text inside an HTTP packet.

The regular expressions that you create can be used anywhere in which a regular expression is needed in the Zone-Based Policy Firewall screens. Regular Expression Metacharacters lists regular expression metacharacters and how they are used.

Name

Enter a name to identify the regular expression. If you are editing the regular expression, the name field is read only.

Pattern List

A regular expression can contain multiple patterns. Click **Add** to display a dialog in which you can enter a new regular expression pattern. Each pattern that you create is automatically added to the list. If you need to copy a pattern from another regular expression, click **Copy Pattern**, click the plus (**+**) sign next to regular expression name, click the pattern that you want, and then click **OK**.

Here is an example pattern list.

```
parameter-map type regex ref_regex
pattern "\.delfinproject\.com"
pattern "\.looksmart\.com"
parameter-map type regex host_regex
pattern "secure\.keenvalue\.com"
pattern "\.looksmart\.com"
parameter-map type regex usragnt_regex
```
pattern "Peer Points Manager"

Add a Pattern

The pattern that you enter in this window is added at the bottom of the regular expression parameter map that you are editing. If you need to reorder the patterns in the parameter map, you can do so in the Edit Regular Expression window.

Pattern

Enter the pattern that you want to add to the regular expression.

Guide Button

Click the **Guide** Button to display the Build Regular Expression dialog, which can assist you in constructing a regular expression. If you click **Guide**, any text that you entered in the **Pattern** field appears in the Regular Expression field of the Build Regular Expression dialog.

Build Regular Expression

The Build Regular Expression dialog box lets you construct a regular expression from characters and metacharacters. Fields that insert metacharacters include the metacharacter in parentheses in the field name.

Build Snippet

This area lets you build text snippets of regular text or lets you insert a metacharacter into the Regular Expression field.

- Starts at the beginning of the line (^)—To indicate that the snippet should start at the beginning of a line, use the caret (^) metacharacter. Be sure to insert any snippet with this option at the beginning of the regular expression.
- Specify Character String—Enter a text string manually.
  - Character String—Enter a text string.
  - Escape Special Characters—If you entered any metacharacters in your text string that you want to be used literally, check this box to add the backslash (\) escape character before them. For example, if you enter “example.com,” this option converts it to “example\.com”.
  - Ignore Case—To match uppercase and lowercase characters, this check box automatically adds text to match both uppercase and lowercase characters. For example, “cats” converts to “[cC][aA][tT][sS]”.

Specify Character

This area lets you specify a metacharacter to insert in the regular expression.

- Negate the character—Specifies not to match the character you identify.
- Any character (.)—Inserts the period (.) metacharacter to match any character. For example, “d.g” matches *dog*, *dag*, *dtg*, and any word that contains those characters, such as *doghouse*.
- Character set—Inserts a character set. Text can match any character in the set. Sets include:

  [0-9A-Za-z]

  [0-9]

  [A-Z]

[a-z]

[aeiou]

[\n\f\r\t] (which matches a new line, form feed, return, or a tab)

For example, if you specify [0-9A-Za-z], then this snippet will match any character from A to Z (uppercase or lowercase) or any digit 0 through 9.

- Special character—Inserts a character that requires an escape, including \, ?, *, +, |, ., [, (, or ^. The escape character is the backslash (\), which is automatically entered when you choose this option.
- Whitespace character—Whitespace characters include \n (new line), \f (form feed), \r (carriage return), or \t (tab).
- Three digit octal number—Matches an ASCII character as octal (up to three digits). For example, the character \040 represents a space. The backslash (\) is entered automatically.
- Two digit hexadecimal number—Matches an ASCII character using hexadecimal (exactly two digits). The backslash (\) is entered automatically.
- Specified character—Enter any single character.

Snippet Preview

Display only. Shows the snippet as it will be entered in the regular expression.

- Append Snippet—Adds the snippet to the end of the regular expression.
- Append Snippet as Alternate—Adds the snippet to the end of the regular expression separated by a pipe (|), which matches either expression it separates. For example, **dog|cat** matches dog or cat.
- Insert Snippet at Cursor—Inserts the snippet at the cursor.

Regular Expression

This area includes regular expression text that you can enter manually and build with snippets. You can then select text in the Regular Expression field and apply a quantifier to the selection.

- Selection Occurrences—Select text in the Regular Expression field, click one of the following options, and then click **Apply to Selection**. For example, if the regular expression is “test me,” and you select “me” and apply **One or more times**, then the regular expression changes to “test (me)+”.

  - Zero or one times (?)—A quantifier that indicates that there are 0 or 1 of the previous expression. For example, **lo?se** matches lse or lose.
  - One or more times (+)—A quantifier that indicates that there is at least 1 of the previous expression. For example, **lo+se** matches lose and loose, but not lse.
  - Any number of times (*)—A quantifier that indicates that there are 0, 1 or any number of the previous expression. For example, **lo*se** matches lse, lose, loose, etc.
  - At least—Repeat at least *x* times. For example, **ab(xy){2,}z** matches abxyxyz, abxyxyxyz, etc.
  - Exactly—Repeat exactly *x* times. For example, **ab(xy){3}z** matches abxyxyxyz.
- Apply to Selection—Applies the quantifier to the selection.

Regular Expression Metacharacters

The following table lists the metacharacters that have special meanings.

Character	Description	Notes
.	Dot	Matches any single character. For example, **d.g** matches dog, dag, dtg, and any word that contains those characters, such as doggonnit.
(*exp*)	Subexpression	A subexpression segregates characters from surrounding characters, so that you can use other metacharacters on the subexpression. For example, **d(o|a)g** matches dog and dag, but **do|ag** matches do and ag. A subexpression can also be used with repeat quantifiers to differentiate the characters meant for repetition. For example, **ab(xy){3}z** matches abxyxyxyz.
|	Alternation	Matches either expression it separates. For example, **dog|cat** matches dog or cat.

Character	Description	Notes
?	Question mark	A quantifier that indicates that there are 0 or 1 of the previous expression. For example, **lo?se** matches lse or lose. **Note** You must enter **Ctrl+V** and then the question mark or else the help function is invoked.
*	Asterisk	A quantifier that indicates that there are 0, 1 or any number of the previous expression. For example, **lo*se** matches lse, lose, loose, etc.
+	Plus	A quantifier that indicates that there is at least 1 of the previous expression. For example, **lo+se** matches lose and loose, but not lse.
{*x*}	Repeat quantifier	Repeat exactly *x* times. For example, **ab(xy){3}z** matches abxyxyxyz.
{*x*,}	Minimum repeat quantifier	Repeat at least *x* times. For example, **ab(xy){2,}z** matches abxyxyz, abxyxyxyz, etc.
[*abc*]	Character class	Matches any character in the brackets. For example, **[abc]** matches a, b, or c.
[^*abc*]	Negated character class	Matches a single character that is not contained within the brackets. For example, **[^abc]** matches any character other than a, b, or c. **[^A-Z]** matches any single character that is not an uppercase letter.
[*a*-*c*]	Character range class	Matches any character in the range. **[a-z]** matches any lowercase letter. You can mix characters and ranges: **[abcq-z]** matches a, b, c, q, r, s, t, u, v, w, x, y, z, and so does [**a-cq-z**]. The dash (-) character is literal only if it is the last or the first character within the brackets: **[abc-]** or **[-abc]**.
""	Quotation marks	Preserves trailing or leading spaces in the string. For example, **" test"** preserves the leading space when it looks for a match.
^	Caret	Specifies the beginning of a line.
\	Escape character	When used with a metacharacter, matches a literal character. For example, **\[** matches the left square bracket.

Character	Description	Notes
char	Character	When character is not a metacharacter, matches the literal character.
\r	Carriage return	Matches a carriage return 0x0d.
\n	Newline	Matches a new line 0x0a.
\t	Tab	Matches a tab 0x09.
\f	Formfeed	Matches a form feed 0x0c.
\x*NN*	Escaped hexadecimal number	Matches an ASCII character using hexadecimal (exactly two digits).
NNN	Escaped octal number	Matches an ASCII character as octal (exactly three digits). For example, the character 040 represents a space.

CHAPTER 44

802.1x Authentication

802.1x authentication allows a remote Cisco IOS router to connect authenticated VPN users to a secure network through a VPN tunnel that is up at all times. The Cisco IOS router will authenticate users through a RADIUS server on the secure network.

802.1x authentication is applied to switch ports or Ethernet (routed) ports, but not to both types of interfaces. If 802.1x authentication is applied to an Ethernet port, non-authenticated users can be routed outside the VPN tunnel to the Internet.

802.1x authentication is configured on interfaces by using the LAN wizard. However, before you can enable 802.1x on any interface, AAA must be enabled on your Cisco IOS router. If you attempt to use the LAN wizard before AAA is enabled, a window appears asking if you want to enable AAA. If you choose to enable AAA, then the 802.1x configuration screens will appear as part of the LAN wizard. If you choose to *not* enable AAA, then the 802.1x configuration screens will *not* appear.

LAN Wizard: 802.1x Authentication (Switch Ports)

This window allows you to enable 802.1x authentication on the switch port or ports you selected for configuration using the LAN wizard.

Enable 802.1x Authentication

Check **Enable 802.1x Authentication** to enable 802.1x authentication on the switch port.

Host Mode

Choose **Single** or **Multiple**. Single mode allows only one authenticated client to have access. Multiple mode allows for any number of clients to have access once a single client has been authenticated.

Note Ports on Cisco 85x and Cisco 87x routers can be set only to multiple host mode. Single mode is disabled for these routers.

Guest VLAN

Check **Guest VLAN** to enable a VLAN for clients lacking 802.1x support. If you enable this option, choose a VLAN form the VLAN drop-down list.

Auth-Fail VLAN

Check **Auth-Fail VLAN** to enable a VLAN for clients that fail 802.1x authorization. If you enable this option, choose a VLAN form the VLAN drop-down list.

Periodic Reauthentication

Check **Periodic Reauthentication** to force reauthentication of 802.1x clients on a regular interval. Choose to configure the interval locally, or to allow the RADIUS server to set the interval. If you choose to configure the reauthentication interval locally, enter a value in the range of 1–65535 seconds. The default setting is 3600 seconds.

Advanced Options

Click **Advanced Options** to open a window with additional 802.1x authentication parameters.

Advanced Options

This window allows you to change the default values for a number of 802.1x authentication parameters.

Radius Server Timeout

Enter the time, in seconds, that your Cisco IOS router waits before timing out its connection to the RADIUS server. Values must be in the range of 1–65535 seconds. The default setting is 30 seconds.

Supplicant Reply Timeout

Enter the time, in seconds, that your Cisco IOS router waits for a reply from an 802.1x client before timing out its connection to that client. Values must be in the range of 1–65535 seconds. The default setting is 30 seconds.

Supplicant Retries Timeout

Enter the time, in seconds, that your Cisco IOS router retries an 802.1x client before timing out its connection to that client. Values must be in the range of 1–65535 seconds. The default setting is 30 seconds.

Quiet Period

Enter the time, in seconds, that your Cisco IOS router will wait between the initial connection to a client and when a login request is sent. Values must be in the range of 1–65535 seconds. The default setting is 60 seconds.

Rate Limit Period

Values must be in the range of 1–65535 seconds. However, the default setting is 0 seconds, which turns off **Rate Limit Period**.

Maximum Reauthentication Attempts

Enter the maximum number of times your Cisco IOS router tries to reauthenticate an 802.1x client. Values must be in the range 1–10. The default setting is 2.

Maximum Retries

Enter the maximum number of login requests that can be sent to the client. Values must be in the range 1–10. The default setting is 2.

Reset to Defaults

Click **Reset to Defaults** to reset all advanced options to their default values.

LAN Wizard: RADIUS Servers for 802.1x Authentication

802.1x authentication information is configured and stored in a policy database residing on RADIUS servers running Cisco Secure ACS version 3.3. The router must validate the credentials of 802.1x clients by communicating with a RADIUS server. Use this window to provide the information the router needs to contact one or more RADIUS servers. Each RADIUS server that you specify must have Cisco Secure ACS software version 3.3 installed and configured.

Note All of your Cisco IOS router interfaces enabled with 802.1x authorization will use the RADIUS servers set up in this window. When you configure a new interface, you will see this screen again. Additions or changes to the RADIUS server information, however, do not have to be made.

Choose the RADIUS client source

Configuring the RADIUS source allows you to specify the source IP address to be sent in RADIUS packets bound for the RADIUS server. If you need more information about an interface, choose the interface and click the **Details** button.

The source IP address in the RADIUS packets sent from the router must be configured as the NAD IP address in the Cisco ACS version 3.3 or later.

If you choose **Router chooses source**, the source IP address in the RADIUS packets will be the address of interface through which the RADIUS packets exit the router.

If you choose an interface, the source IP address in the RADIUS packets will be the address of the interface that you chose as the RADIUS client source.

Note Cisco IOS software allows a single RADIUS source interface to be configured on the router. If the router already has a configured RADIUS source and you choose a different source, the source IP address placed in the packets sent to the RADIUS server changes to the IP address of the new source, and may not match the NAD IP address configured on the Cisco ACS.

Details

If you need a quick snapshot of the information about an interface before choosing it, click **Details**. The screen shows you the IP address and subnet mask, the access rules and inspection rules applied to the interface, the IPSec policy and QoS policy applied, and whether there is an Easy VPN configuration on the interface.

Server IP, Timeout, and Parameters Columns

The Server IP, Timeout, and Parameters columns contain the information that the router uses to contact a RADIUS server. If no RADIUS server information is associated with the chosen interface, these columns are blank.

Use for 802.1x Check Box

Check this box if you want to use the listed RADIUS server for 802.1x. The server must have the required 802.1x authorization information configured if 802.1x is used successfully.

Add, Edit, and Ping

To provide information for a RADIUS server, click the **Add** button and enter the information in the screen displayed. Choose a row and click **Edit** to modify the information for a RADIUS server. Choose a row and click **Ping** to test the connection between the router and a RADIUS server.

Note When performing a ping test, enter the IP address of the RADIUS source interface in the source field in the ping dialog. If you chose **Router chooses source**, you need not provide any value in the ping dialog source field.

The **Edit** and **Ping** buttons are disabled when no RADIUS server information is available for the chosen interface.

Edit 802.1x Authentication (Switch Ports)

This window allows you to enable and configure 802.1x authentication parameters.

If a message is displayed indicating that the port is operating in trunk mode instead of the 802.1x authentication parameters, then the switch cannot have 802.1x authentication enabled.

If the 802.1x authentication parameters appear but are disabled, then one of the following is true:

- AAA has not been enabled.

  To enable AAA, go to **Configure > Router > AAA > Overview**. Then click **Enable AAA**.

- AAA has been enabled, but an 802.1x authentication policy has not been configured.

  To configure an 802.1x authentication policy, go to **Configure > Router > AAA > Authentication Policies > 802.1x**.

Enable 802.1x Authentication

Check **Enable 802.1x Authentication** to enable 802.1x authentication on this switch port.

Host Mode

Choose **Single** or **Multiple**. Single mode allows only one authenticated client to have access. Multiple mode allows for any number of clients to have access once a single client has been authenticated.

Note Ports on Cisco 87x routers can be set only to multiple host mode. Single mode is disabled for these routers.

Guest VLAN

Check **Guest VLAN** to enable a VLAN for clients lacking 802.1x support. If you enable this option, choose a VLAN form the VLAN drop-down list.

Auth-Fail VLAN

Check **Auth-Fail VLAN** to enable a VLAN for clients that fail 802.1x authorization. If you enable this option, choose a VLAN form the VLAN drop-down list.

Periodic Reauthentication

Check **Periodic Reauthentication** to force reauthentication of 802.1x clients on a regular interval. Choose to configure the interval locally, or to allow the RADIUS server to set the interval. If you choose to configure the reauthentication interval locally, enter a value in the range of 1–65535 seconds. The default setting is 3600 seconds.

Advanced Options

Click **Advanced Options** to open a window with additional 802.1x authentication parameters.

LAN Wizard: 802.1x Authentication (VLAN or Ethernet)

This window allows you to enable 802.1x authentication on the Ethernet port you selected for configuration using the LAN wizard. For Cisco 87x routers, this window is available for configuring a VLAN with 802.1x authentication.

Note Before configuring 802.1x on VLAN, be sure that 802.1x is *not* configured on any VLAN switch ports. Also be sure that the VLAN is configured for DHCP.

Use 802.1x Authentication to separate trusted and untrusted traffic on the interface

Check **Use 802.1x Authentication to separate trusted and untrusted traffic on the interface** to enable 802.1x authentication.

Exception Lists

Click **Exception Lists** to create or edit an exception list. An exception list exempts certain clients from 802.1x authentication while allowing them to use the VPN tunnel.

Exempt Cisco IP phones from 802.1x authentication

Check **Exempt Cisco IP phones from 802.1x authentication** to exempt Cisco IP phones from 802.1x authentication while allowing them to use the VPN tunnel.

802.1x Exception List

An exception list exempts certain clients from 802.1x authentication while allowing them to use the VPN tunnel. Exempt clients are identified by their MAC addresses.

Add

Click **Add** to open a window where you can add the MAC address of a client. The MAC address must be in the format that matches one of these examples:

- 0030.6eb1.37e4
- 00-30-6e-b1-37-e4

Cisco CP rejects misformatted MAC addresses, except for MAC addresses shorter than the given examples. Shorter MAC addresses will be padded with a “0” (zero) for each missing digit.

Note Cisco CP’s 802.1x feature does not support the CLI option that associates policies with MAC addresses and will not include in the exception list MAC addresses that have a policy associated with them.

Delete

Click **Delete** to remove a chosen client from the exception list.

802.1x Authentication on Layer 3 Interfaces

This window allows you to configure 802.1x authentication on a Layer 3 Interface. It lists Ethernet ports and VLAN interfaces that have or can be configured with 802.1x authentication, allows you to choose a Virtual Template interface for untrusted clients, and create an exception list for clients to bypass 802.1x authentication.

Note If policies have been set using the CLI, they will appear as read-only information in this window. In this case, only enabling or disabling 802.1x is allowed in this window.

Prerequisite Tasks

If a prerequisite task appears in the window, it must be completed before 802.1x authentication can be configured. A message explaining the prerequisite task is displayed, along with a link to the window where the task can be completed.

Enable 802.1x Authentication Globally

Check **Enable 802.1x Authentication Globally** to enable 802.1x authentication on all Ethernet ports.

Interfaces Table

The Interfaces table has the following columns:

Interface—Displays the name of the Ethernet or VLAN interface.

802.1x Authentication—Indicates whether 802.1x authentication is enabled for the Ethernet port.

Edit

Click **Edit** to open a window of editable 802.1x authentication parameters. The parameters are the 802.1x authentication settings for the interface chosen in the Interfaces table.

Untrusted User Policy

Choose a Virtual Template interface from the drop-down list. The chosen Virtual Template interface represents the policy applied to clients that fail 802.1x authentication.

Click the **Details** button to see more information about the chosen Virtual Template interface.

Exception List

For more information about the exception list, see 802.1x Exception List.

Exempt Cisco IP phones from 802.1x authentication

Check **Exempt Cisco IP phones from 802.1x authentication** to exempt Cisco IP phones from 802.1x authentication while allowing them to use the VPN tunnel.

Apply Changes

Click **Apply Changes** for the changes you made to take effect.

Discard Changes

Click **Discard Changes** to erase the unapplied changes you made.

Edit 802.1x Authentication

This window allows you to enable and change the default values for a number of 802.1x authentication parameters.

Enable 802.1x Authentication

Check **Enable 802.1x Authentication** to enable 802.1x authentication on the Ethernet port.

Periodic Reauthentication

Check **Periodic Reauthentication** to force reauthentication of 802.1x clients on a regular interval. Choose to configure the interval locally, or to allow the RADIUS server to set the interval. If you choose to configure the reauthentication interval locally, enter a value in the range of 1–65535 seconds. The default setting is 3600 seconds.

Advanced Options

Click Advanced Options for descriptions of the fields in the Advanced Options box.

How Do I ...

This section contains procedures for tasks that the wizard does not help you complete.

How Do I Configure 802.1x Authentication on More Than One Ethernet Port?

Once you configure 802.1x authentication on an interface, the LAN wizard will no longer display any 802.1x options for Ethernet ports because Cisco CP uses the 802.1x configuration globally.

If you want to edit the 802.1x authentication configuration on an Ethernet port, go to **Configure > Router > AAA > Authentication Policies > 802.1x**. Then choose the authentication policy, and click **Edit**. Edit the policy in the displayed dialog.

CHAPTER 45

Port-to-Application Mapping

Port-to-Application Mapping (PAM) allows you to customize TCP and UDP port numbers for network services and applications. PAM uses this information to support network environments that run services using ports that are different from the registered or well-known ports associated with an application.

The information that PAM maintains enables Context-Based Access Control (CBAC) supported services to run on nonstandard ports. Previously, CBAC was limited to inspecting traffic using only the well-known or registered ports associated with an application. Now, PAM allows network administrators to customize network access control for specific applications and services.

Port-to-Application Mapping Reference

This section contains the following topics:

- Port-to-Application Mappings
- Add or Edit Port Map Entry

Port-to-Application Mappings

This window displays the port-to-application mappings configured on the router and allows you to add, edit and remove PAM entries. Each row in the window displays a PAM entry, and entries are grouped according to type.

Table 45-1 Port-to-Application Mappings

Element	Description
Add, Edit, and Delete	Use these buttons to create, edit, or remove PAM entries. To create an entry that maps a nonstandard port number to a protocol name, click **Add**. To change a user defined entry, click **Edit**. Entries with the value *System Defined* in the Protocol Type column cannot be edited or deleted.
Application Protocol	This column contains the name of the application protocol, and the names of the protocol types. For example, the FTP and the TFTP entries are found under the File Transfer protocol type.
Port Type	This list appears if the router is running a Cisco IOS image that allows you to specify whether this port map entry applies to TCP or to UDP traffic.
Port	This column contains the port number. For example the system-defined entry for HTTP would have the port number 80 in this column. A user-defined entry for HTTP might have the port number 8080 or another custom-defined number in this column.
Protocol Type	A row in this column displays one of the following values: • **System-Defined**—The entry contains a standard, registered mapping between the protocol and protocol number, such as *tftp 69*, or *smtp 25*. System-defined entries cannot be edited or deleted. System-defined entries contain no value in the Access List column because they apply to all hosts on the network. • **User-Defined**—The entry contains a nonstandard mapping between a protocol and protocol number. The entry could be associated with a host IP address identified by the access control list (ACL) whose number is displayed in the Access List column.
Access List	A PAM entry applies to a single host, defined by a standard ACL. This column displays the number of the ACL used to identify the host to which the PAM entry applies. If you want to view the ACL that identifies the host, go to **Configure > Router > ACL > ACL Editor**. Then click the number of the ACL that you saw in this window.
Description	If a description of the PAM entry has been created, the description is displayed in this column.

Add or Edit Port Map Entry

In this screen add or edit port map entries for custom or standard protocols.

Table 45-2 Add or Edit a Port Map Entry

Element	Description
Protocol Field	If you are adding an entry, specify the protocol by clicking the list (**...**) button to the right and choosing a system-defined protocol, or by entering the name of a custom protocol. You cannot enter custom-defined protocol names for which a port mapping already exists. If you are editing an entry, the protocol field is disabled. If you need to change the protocol, delete the PAM entry and re-create it using the protocol information that you need.
Description Field	This field appears if the router is running a Cisco IOS image that allows you to specify whether this port map entry applies to TCP or to UDP traffic. You can optionally enter a description of the port map entry. Descriptions are helpful when you are adding entries for custom protocols or special applications. For example, if you created an entry for a custom database application named “orville” running on host sf-5, you might enter “orville-sf-5.”
Port Type List	This list appears if the router is running a Cisco IOS image that allows you to specify whether this port map entry applies to TCP or to UDP traffic. Choose either **TCP** or **UDP**. The default is TCP.

Table 45-2 Add or Edit a Port Map Entry (continued)

Element	Description
Port Number Field	Enter the port number that you want to map to the protocol that you specified. If the router is running a Cisco IOS image that allows you to specify whether this port map entry applies to TCP or to UDP traffic, you can enter multiple port numbers separated by commas, or port number ranges indicated with a dash. For example, you might enter three noncontiguous port numbers as 310, 313, 318, or you might enter the range 415–419. If the router is not running a Cisco IOS image that allows you to specify whether this port map entry applies to TCP or to UDP traffic, you can enter a single port number.
Host of Service Field	Specify the IP address of the host to which this port mapping is to apply. If you need the same mapping for another host, create a separate PAM entry for that host.

CHAPTER 46

Security Audit

Security Audit is a feature that examines your existing router configurations and then updates your router in order to make your router and network more secure. Security Audit is based on the Cisco IOS AutoSecure feature; it performs checks on and assists in configuration of almost all of the AutoSecure functions. For a complete list of the functions that Security Audit checks for, and for a list of the few AutoSecure features unsupported by Security Audit, see the topic Cisco CP and Cisco IOS AutoSecure.

Security Audit operates in one of two modes—the Security Audit wizard, which lets you choose which potential security-related configuration changes to implement on your router, and One-Step Lockdown, which automatically makes all recommended security-related configuration changes.

Perform Security Audit

This option starts the Security Audit wizard. The Security Audit wizard tests your router configuration to determine if any potential security problems exist in the configuration, and then presents you with a screen that lets you determine which of those security problems you want to fix. Once determined, the Security Audit wizard will make the necessary changes to the router configuration to fix those problems.

To have Cisco CP perform a security audit and then fix the problems it has found:

Step 1 In the Feature bar, select **Configure > Security > Security Audit**.

Step 2 Click **Perform Security Audit**.

The Welcome page of the Security Audit wizard appears.

Step 3 Click **Next>**.

The Security Audit Interface Configuration page appears.

Step 4 The Security Audit wizard needs to know which of your router interfaces connect to your inside network and which connect outside of your network. For each interface listed, check either the **Inside** or **Outside** check box to indicate where the interface connects.

Step 5 Click **Next>**.

The Security Audit wizard tests your router configuration to determine which possible security problems may exist. A screen showing the progress of this action appears, listing all of the configuration options being tested for, and whether or not the current router configuration passes those tests.

If you want to save this report to a file, click **Save Report**.

Step 6 Click **Close**.

The Security Audit Report Card screen appears, showing a list of possible security problems.

Step 7 Check the **Fix it** boxes next to any problems that you want Cisco Configuration Professional (Cisco CP) to fix. For a description of the problem and a list of the Cisco IOS commands that will be added to your configuration, click the problem description to display a help page about that problem.

Step 8 Click **Next>**.

Step 9 The Security Audit wizard may display one or more screens requiring you to enter information to fix certain problems. Enter the information as required and click **Next>** for each of those screens.

Step 10 The Summary page of the wizard shows a list of all the configuration changes that Security Audit will make. Click **Finish** to deliver those changes to your router.

One-Step Lockdown

This option tests you router configuration for any potential security problems and automatically makes any necessary configuration changes to correct any problems found. The conditions checked for and, if needed, corrected are as follows:

- Disable Finger Service

- Disable PAD Service
- Disable TCP Small Servers Service
- Disable UDP Small Servers Service
- Disable IP BOOTP Server Service
- Disable IP Identification Service
- Disable CDP
- Disable IP Source Route
- Enable Password Encryption Service
- Enable TCP Keepalives for Inbound Telnet Sessions
- Enable TCP Keepalives for Outbound Telnet Sessions
- Enable Sequence Numbers and Time Stamps on Debugs
- Enable IP CEF
- Disable IP Gratuitous ARPs
- Set Minimum Password Length to Less Than 6 Characters
- Set Authentication Failure Rate to Less Than 3 Retries
- Set TCP Synwait Time
- Set Banner
- Enable Logging
- Set Enable Secret Password
- Disable SNMP
- Set Scheduler Interval
- Set Scheduler Allocate
- Set Users
- Enable Telnet Settings
- Enable NetFlow Switching
- Disable IP Redirects
- Disable IP Proxy ARP
- Disable IP Directed Broadcast
- Disable MOP Service

- Disable IP Unreachables
- Disable IP Mask Reply
- Disable IP Unreachables on NULL Interface
- Enable Unicast RPF on Outside Interfaces
- Enable Firewall on All of the Outside Interfaces
- Set Access Class on HTTP Server Service
- Set Access Class on VTY Lines
- Enable SSH for Access to the Router

Welcome Page

This screen describes the Security Audit wizard and the changes the wizard will attempt to make to your router configuration.

Interface Selection Page

This screen displays a list of all interfaces and requires you to identify which router interfaces are “outside” interfaces, that is, interfaces that connect to unsecure networks such as the Internet. By identifying which interfaces are outside interfaces, Security Configuration knows on which interfaces to configure firewall security features.

Interface Column

This column lists each of the router interfaces.

Outside Column

This column displays a check box for each interface listed in the Interface column. Check the check box for each interface that connects to a network outside of your network, such as the Internet.

Inside Column

This column displays a check box for each interface listed in the Interface column. Check the check box for each interface that connects directly to your local network and is thus protected from the Internet by your firewall.

Report Card Page

The Report Card popup page displays a list of recommended configuration changes that, if made, make the network more secure. The **Save** button, enabled after all checks are made, lets you save the report card to a file that you can print or email. Clicking **Close** displays a dialog that lists the reported security problems, and that can list security configurations that Cisco CP can undo.

Fix It Page

This page displays the configuration changes recommended in the Report Card page. Use the **Select an Option** list to display the security problems Cisco CP can fix, or the security configurations Cisco CP can undo.

Select an Option: Fix the security problems

The Report Card screen displays a list of recommended configuration changes that will make your router and network more secure. The potential security problems in your router configuration are listed in the left column. To get more information about a potential problem, click the problem. Online help will display a more detailed description of the problem and the recommended configuration changes. To correct all of the potential problems, click **Fix All**, and then click **Next>** to continue. To correct individual security issues, check the **Fix It** check box next to the issue or issues that you want to correct, and then click **Next>** to continue the Security Audit Wizard. The Security Audit will correct the problems you selected, collecting further input from you as necessary, and will then display a list of the new configuration commands that will be added to the router configuration.

Fix All

Click this button to place a check mark next to all of the potential security problems listed on the Report Card screen.

Select an option: Undo Security Configurations

When this option is selected, Cisco CP displays the security configurations that it can undo. To have Cisco CP undo all the security configurations, click **Undo All**. To specify a security configuration that you want to undo, check the **Undo** box next to it. **Click Next>** after you have specified which security configurations to undo. You must select at least one security configuration to undo.

Undo All

Click the button to place a checkmark next to all the security configurations that Cisco CP can undo.

To see which security configurations Cisco CP can undo, click:

Security Configurations Cisco CP Can Undo

I want Cisco CP to fix some problems, but undo other security configurations

If you want Cisco CP to fix some security issues but undo other security configurations that you do not need, you can run the Security Audit wizard once to specify the problems to fix, and then run it again so that you can select the security configurations you want to undo.

Disable Finger Service

Security Audit disables the finger service whenever possible. Finger is used to find out which users are logged into a network device. Although this information is not usually tremendously sensitive, it can sometimes be useful to an attacker.

In addition, the finger service can be used in a specific type of Denial-of-Service (DoS) attack called “Finger of death,” which involves sending a finger request to a specific computer every minute, but never disconnecting.

The configuration that will be delivered to the router to disable the Finger service is as follows:

```
no service finger
```

This fix can be undone. To learn how, click Undoing Security Audit Fixes.

Disable PAD Service

Security Audit disables all packet assembler/disassembler (PAD) commands and connections between PAD devices and access servers whenever possible.

The configuration that will be delivered to the router to disable PAD is as follows:

```
no service pad
```

This fix can be undone. To learn how, click Undoing Security Audit Fixes.

Disable TCP Small Servers Service

Security Audit disables small services whenever possible. By default, Cisco devices running Cisco IOS version 11.3 or earlier offer the "small services": echo, chargen, and discard. (Small services are disabled by default in Cisco IOS software version 12.0 and later.) These services, especially their User Datagram Protocol (UDP) versions, are infrequently used for legitimate purposes, but they can be used to launch DoS and other attacks that would otherwise be prevented by packet filtering.

For example, an attacker might send a Domain Name System (DNS) packet, falsifying the source address to be a DNS server that would otherwise be unreachable, and falsifying the source port to be the DNS service port (port 53). If such a packet were sent to the router's UDP echo port, the result would be the router sending a DNS packet to the server in question. No outgoing access list checks would be applied to this packet, since it would be considered to be locally generated by the router itself.

Although most abuses of the small services can be avoided or made less dangerous by anti-spoofing access lists, the services should almost always be disabled in any router which is part of a firewall or lies in a security-critical part of the network. Since the services are rarely used, the best policy is usually to disable them on all routers of any description.

The configuration that will be delivered to the router to disable TCP small servers is as follows:

```
no service tcp-small-servers
```

This fix can be undone. To learn how, click Undoing Security Audit Fixes.

Disable UDP Small Servers Service

Security Audit disables small services whenever possible. By default, Cisco devices running Cisco IOS version 11.3 or earlier offer the "small services": echo, chargen, and discard. (Small services are disabled by default in Cisco IOS software version 12.0 and later.) These services, especially their UDP versions, are infrequently used for legitimate purposes, but they can be used to launch DoS and other attacks that would otherwise be prevented by packet filtering.

For example, an attacker might send a DNS packet, falsifying the source address to be a DNS server that would otherwise be unreachable, and falsifying the source port to be the DNS service port (port 53). If such a packet were sent to the router's UDP echo port, the result would be the router sending a DNS packet to the server in question. No outgoing access list checks would be applied to this packet, since it would be considered to be locally generated by the router itself.

Although most abuses of the small services can be avoided or made less dangerous by anti-spoofing access lists, the services should almost always be disabled in any router which is part of a firewall or lies in a security-critical part of the network. Since the services are rarely used, the best policy is usually to disable them on all routers of any description.

The configuration that will be delivered to the router to disable UDP small servers is as follows:

```
no service udp-small-servers
```

Disable IP BOOTP Server Service

Security Audit disables the Bootstrap Protocol (BOOTP) service whenever possible. BOOTP allows both routers and computers to automatically configure necessary Internet information from a centrally maintained server upon startup, including downloading Cisco IOS software. As a result, BOOTP can potentially be used by an attacker to download a copy of a router's Cisco IOS software.

In addition, the BOOTP service is vulnerable to DoS attacks; therefore it should be disabled or filtered via a firewall for this reason as well.

The configuration that will be delivered to the router to disable BOOTP is as follows:

```
no ip bootp server
```

This fix can be undone. To learn how, click Undoing Security Audit Fixes.

Disable IP Identification Service

Security Audit disables identification support whenever possible. Identification support allows you to query a TCP port for identification. This feature enables an unsecure protocol to report the identity of a client initiating a TCP connection and a host responding to the connection. With identification support, you can connect a TCP port on a host, issue a simple text string to request information, and receive a simple text-string reply.

It is dangerous to allow any system on a directly connected segment to learn that the router is a Cisco device and to determine the model number and the Cisco IOS software version being run. This information may be used to design attacks against the router.

The configuration that will be delivered to the router to disable the IP identification service is as follows:

```
no ip identd
```

This fix can be undone. To learn how, click Undoing Security Audit Fixes.

Disable CDP

Security Audit disables Cisco Discovery Protocol (CDP) whenever possible. CDP is a proprietary protocol that Cisco routers use to identify each other on a LAN segment. This is dangerous in that it allows any system on a directly connected segment to learn that the router is a Cisco device and to determine the model number and the Cisco IOS software version being run. This information may be used to design attacks against the router.

The configuration that will be delivered to the router to disable CDP is as follows:

```
no cdp run
```

This fix can be undone. To learn how, click Undoing Security Audit Fixes.

Disable IP Source Route

Security Audit disables IP source routing whenever possible. The IP protocol supports source routing options that allow the sender of an IP datagram to control the route that the datagram will take toward its ultimate destination, and generally the route that any reply will take. These options are rarely used for legitimate purposes in networks. Some older IP implementations do not process source-routed packets properly, and it may be possible to crash machines running these implementations by sending them datagrams with source routing options.

Disabling IP source routing will cause a Cisco router to never forward an IP packet that carries a source routing option.

The configuration that will be delivered to the router to disable IP source routing is as follows:

```
no ip source-route
```

This fix can be undone. To learn how, click Undoing Security Audit Fixes.

Enable Password Encryption Service

Security Audit enables password encryption whenever possible. Password encryption directs the Cisco IOS software to encrypt the passwords, Challenge Handshake Authentication Protocol (CHAP) secrets, and similar data that are saved in its configuration file. This is useful for preventing casual observers from reading passwords, for example, when they happen to look at the screen over an administrator's shoulder.

The configuration that will be delivered to the router to enable password encryption is as follows:

```
service password-encryption
```

This fix can be undone. To learn how, click Undoing Security Audit Fixes.

Enable TCP Keepalives for Inbound Telnet Sessions

Security Audit enables TCP keep alive messages for both inbound and outbound Telnet sessions whenever possible. Enabling TCP keep alives causes the router to generate periodic keep alive messages, letting it detect and drop broken Telnet connections.

The configuration that will be delivered to the router to enable TCP keep alives for inbound Telnet sessions is as follows:

```
service tcp-keepalives-in
```

This fix can be undone. To learn how, click Undoing Security Audit Fixes.

Enable TCP Keepalives for Outbound Telnet Sessions

Security Audit enables TCP keep alive messages for both inbound and outbound Telnet sessions whenever possible. Enabling TCP keep alives causes the router to generate periodic keep alive messages, letting it detect and drop broken Telnet connections.

The configuration that will be delivered to the router to enable TCP keep alives for outbound Telnet sessions is as follows:

```
service tcp-keepalives-out
```

This fix can be undone. To learn how, click Undoing Security Audit Fixes.

Enable Sequence Numbers and Time Stamps on Debugs

Security Audit enables sequence numbers and time stamps on all debug and log messages whenever possible. Time stamps on debug and log messages indicate the time and date that the message was generated. Sequence numbers indicate the sequence in which messages that have identical time stamps were generated. Knowing the timing and sequence that messages are generated is an important tool in diagnosing potential attacks.

The configuration that will be delivered to the router to enable time stamps and sequence numbers is as follows:

```
service timestamps debug datetime localtime show-timezone msec
service timestamps log datetime localtime show-timeout msec
```

```
service sequence-numbers
```

Enable IP CEF

Security Audit enables Cisco Express Forwarding (CEF) or Distributed Cisco Express Forwarding (DCEF) whenever possible. Because there is no need to build cache entries when traffic starts arriving at new destinations, CEF behaves more predictably than other modes when presented with large volumes of traffic addressed to many destinations. Routes configured for CEF perform better under SYN attacks than routers using the traditional cache.

The configuration that will be delivered to the router to enable CEF is as follows:

```
ip cef
```

Disable IP Gratuitous ARPs

Security Audit disables IP gratuitous Address Resolution Protocol (ARP) requests whenever possible. A gratuitous ARP is an ARP broadcast in which the source and destination IP addresses are the same. It is used primarily by a host to inform the network about its IP address. A spoofed gratuitous ARP message can cause network mapping information to be stored incorrectly, causing network malfunction.

To disable gratuitous ARPs, the following configuration will be delivered to the router:

```
no ip gratuitous-arps
```

This fix can be undone. To learn how, click Undoing Security Audit Fixes.

Set Minimum Password Length to Less Than 6 Characters

Security Audit configures your router to require a minimum password length of six characters whenever possible. One method attackers use to crack passwords is to try all possible combinations of characters until the password is discovered. Longer passwords have exponentially more possible combinations of characters, making this method of attack much more difficult.

This configuration change will require every password on the router, including the user, enable, secret, console, AUX, tty, and vty passwords, to be at least six characters in length. This configuration change will be made only if the Cisco IOS version running on your router supports the minimum password length feature.

The configuration that will be delivered to the router is as follows:

```
security passwords min-length <6>
```

Set Authentication Failure Rate to Less Than 3 Retries

Security Audit configures your router to lock access after three unsuccessful login attempts whenever possible. One method of cracking passwords, called the "dictionary" attack, is to use software that attempts to log in using every word in a dictionary. This configuration causes access to the router to be locked for a period of 15 seconds after three unsuccessful login attempts, disabling the dictionary method of attack. In addition to locking access to the router, this configuration causes a log message to be generated after three unsuccessful login attempts, warning the administrator of the unsuccessful login attempts.

The configuration that will be delivered to the router to lock router access after three unsuccessful login attempts is as follows:

```
security authentication failure rate <3>
```

Set TCP Synwait Time

Security Audit sets the TCP synwait time to 10 seconds whenever possible. The TCP synwait time is a value that is useful in defeating SYN flooding attacks, a form of Denial-of-Service (DoS) attack. A TCP connection requires a three-phase handshake to initially establish the connection. A connection request is sent by the originator, an acknowledgement is sent by the receiver, and then an acceptance of that acknowledgement is sent by the originator. Once this three-phase handshake is complete, the connection is complete and data transfer can begin. A SYN flooding attack sends repeated connection requests to a host, but never sends the acceptance of acknowledgements that complete the connections, creating increasingly more incomplete connections at the host. Because the buffer for incomplete connections is usually smaller than the buffer for completed

connections, this can overwhelm and disable the host. Setting the TCP synwait time to 10 seconds causes the router to shut down an incomplete connection after 10 seconds, preventing the buildup of incomplete connections at the host.

The configuration that will be delivered to the router to set the TCP synwait time to 10 seconds is as follows:

```
ip tcp synwait-time <10>
```

Set Banner

Security Audit configures a text banner whenever possible. In some jurisdictions, civil and/or criminal prosecution of crackers who break into your systems is made much easier if you provide a banner informing unauthorized users that their use is in fact unauthorized. In other jurisdictions, you may be forbidden to monitor the activities of even unauthorized users unless you have taken steps to notify them of your intent to do so. The text banner is one method of performing this notification.

The configuration that will be delivered to the router to create a text banner is as follows, replacing <*company name*>, <*administrator email address*>, and <*administrator phone number*> with the appropriate values that you enter into Security Audit:

```
banner ~
Authorized access only
This system is the property of <company name> Enterprise.
Disconnect IMMEDIATELY as you are not an authorized user!
Contact <administrator email address> <administrator phone number>.
~
```

Enable Logging

Security Audit will enable logging with time stamps and sequence numbers whenever possible. Because it gives detailed information about network events, logging is critical in recognizing and responding to security events. Time stamps and sequence numbers provide information about the date and time and sequence in which network events occur.

The configuration that will be delivered to the router to enable and configure logging is as follows, replacing <*log buffer size*> and <*logging server ip address*> with the appropriate values that you enter into Security Audit:

```
logging console critical
logging trap debugging
logging buffered <log buffer size>
logging <logging server ip address>
```

Set Enable Secret Password

Security Audit will configure the **enable secret** Cisco IOS command for more secure password protection whenever possible. The **enable secret** command is used to set the password that grants privileged administrative access to the Cisco IOS system. The **enable secret** command uses a much more secure encryption algorithm (MD5) to protect that password than the older **enable password** command. This stronger encryption is an essential means of protecting the router password, and thus network access.

The configuration that will be delivered to the router to configure the command is as follows:

```
enable secret <>
```

Disable SNMP

Security Audit disables the Simple Network Management Protocol (SNMP) whenever possible. SNMP is a network protocol that provides a facility for retrieving and posting data about network performance and processes. It is very widely used for router monitoring, and frequently for router configuration changes as well. Version 1 of the SNMP protocol, however, which is the most commonly used, is often a security risk for the following reasons:

- It uses authentication strings (passwords) called *community strings* which are stored and sent across the network in plain text.
- Most SNMP implementations send those strings repeatedly as part of periodic polling.
- It is an easily spoofable, datagram-based transaction protocol.

Because SNMP can be used to retrieve a copy of the network routing table, as well as other sensitive network information, Cisco recommends disabling SNMP if your network does not require it. Security Audit will initially request to disable SNMP.

The configuration that will be delivered to the router to disable SNMP is as follows:

```
no snmp-server
```

Set Scheduler Interval

Security Audit configures the scheduler interval on the router whenever possible. When a router is fast-switching a large number of packets, it is possible for the router to spend so much time responding to interrupts from the network interfaces that no other work gets done. Some very fast packet floods can cause this condition. It may stop administrative access to the router, which is very dangerous when the device is under attack. Tuning the scheduler interval ensures that management access to the router is always available by causing the router to run system processes after the specified time interval even when CPU usage is at 100%.

The configuration that will be delivered to the router to tune the scheduler interval is as follows:

```
scheduler interval 500
```

Set Scheduler Allocate

On routers that do not support the command **scheduler interval**, Security Audit configures the **scheduler allocate** command whenever possible. When a router is fast-switching a large number of packets, it is possible for the router to spend so much time responding to interrupts from the network interfaces that no other work gets done. Some very fast packet floods can cause this condition. It may stop administrative access to the router, which is very dangerous when the device is under attack. The **scheduler allocate** command guarantees a percentage of the router CPU processes for activities other than network switching, such as management processes.

The configuration that will be delivered to the router to set the scheduler allocate percentage is as follows:

```
scheduler allocate 4000 1000
```

Set Users

Security Audit secures the console, AUX, vty, and tty lines by configuring Telnet user accounts to authenticate access to these lines whenever possible. Security Audit will display a dialog box that lets you define user accounts and passwords for these lines.

Enable Telnet Settings

Security Audit secures the console, AUX, vty, and tty lines by implementing the following configurations whenever possible:

- Configures **transport input** and **transport output** commands to define which protocols can be used to connect to those lines.
- Sets the exec-timeout value to 10 minutes on the console and AUX lines, causing an administrative user to be logged out from these lines after 10 minutes of no activity.

The configuration that will be delivered to the router to secure the console, AUX, vty, and tty lines is as follows:

```
!
line console 0
transport output telnet
exec-timeout 10
login local
!
line AUX 0
transport output telnet
exec-timeout 10
login local
!
line vty ….
transport input telnet
login local
```

Enable NetFlow Switching

Security Audit enables NetFlow switching whenever possible. NetFlow switching is a Cisco IOS feature that enhances routing performance while using Access Control Lists (ACLs) and other features that create and enhance network security.

NetFlow identifies flows of network packets based on the source and destination IP addresses and TCP port numbers. NetFlow then can use just the initial packet of a flow for comparison to ACLs and for other security checks, rather than having to use every packet in the network flow. This enhances performance, allowing you to make use of all of the router security features.

The configuration that will be delivered to the router to enable NetFlow is as follows:

```
ip route-cache flow
```

This fix can be undone. To learn how, click Undoing Security Audit Fixes.

Disable IP Redirects

Security Audit disables Internet Message Control Protocol (ICMP) redirect messages whenever possible. ICMP supports IP traffic by relaying information about paths, routes, and network conditions. ICMP redirect messages instruct an end node to use a specific router as its path to a particular destination. In a properly functioning IP network, a router will send redirects only to hosts on its own local subnets, no end node will ever send a redirect, and no redirect will ever be traversed more than one network hop. However, an attacker may violate these rules; some attacks are based on this. Disabling ICMP redirects will cause no operational impact to the network, and it eliminates this possible method of attack.

The configuration that will be delivered to the router to disable ICMP redirect messages is as follows:

```
no ip redirects
```

Disable IP Proxy ARP

Security Audit disables proxy Address Resolution Protocol (ARP) whenever possible. ARP is used by the network to convert IP addresses into MAC addresses. Normally ARP is confined to a single LAN, but a router can act as a proxy for ARP requests, making ARP queries available across multiple LAN segments. Because it breaks the LAN security barrier, proxy ARP should be used only between two LANs with an equal security level, and only when necessary.

The configuration that will be delivered to the router to disable proxy ARP is as follows:

```
no ip proxy-arp
```

This fix can be undone. To learn how, click Undoing Security Audit Fixes.

Disable IP Directed Broadcast

Security Audit disables IP directed broadcasts whenever possible. An IP directed broadcast is a datagram which is sent to the broadcast address of a subnet to which the sending machine is not directly attached. The directed broadcast is routed through the network as a unicast packet until it arrives at the target subnet, where it is converted into a link-layer broadcast. Because of the nature of the IP addressing architecture, only the last router in the chain, the one that is connected directly to the target subnet, can conclusively identify a directed broadcast. Directed broadcasts are occasionally used for legitimate purposes, but such use is not common outside the financial services industry.

IP directed broadcasts are used in the extremely common and popular “smurf” Denial-of-Service attack, and they can also be used in related attacks. In a “smurf” attack, the attacker sends ICMP echo requests from a falsified source address to a directed broadcast address, causing all the hosts on the target subnet to send replies to the falsified source. By sending a continuous stream of such requests, the attacker can create a much larger stream of replies, which can completely inundate the host whose address is being falsified.

Disabling IP directed broadcasts causes directed broadcasts that would otherwise be “exploded” into link-layer broadcasts at that interface to be dropped instead.

The configuration that will be delivered to the router to disable IP directed broadcasts is as follows:

```
no ip directed-broadcast
```

This fix can be undone. To learn how, click Undoing Security Audit Fixes.

Disable MOP Service

Security Audit will disable the Maintenance Operations Protocol (MOP) on all Ethernet interfaces whenever possible. MOP is used to provide configuration information to the router when communicating with DECNet networks. MOP is vulnerable to various attacks.

The configuration that will be delivered to the router to disable the MOP service on Ethernet interfaces is as follows:

```
no mop enabled
```

This fix can be undone. To learn how, click Undoing Security Audit Fixes.

Disable IP Unreachables

Security Audit disables Internet Message Control Protocol (ICMP) host unreachable messages whenever possible. ICMP supports IP traffic by relaying information about paths, routes, and network conditions. ICMP host unreachable messages are sent out if a router receives a nonbroadcast packet that uses an unknown protocol, or if the router receives a packet that it is unable to deliver to the ultimate destination because it knows of no route to the destination address. These messages can be used by an attacker to gain network mapping information.

The configuration that will be delivered to the router to disable ICMP host unreachable messages is as follows:

```
int <all-interfaces>
no ip unreachables
```

This fix can be undone. To learn how, click Undoing Security Audit Fixes.

Disable IP Mask Reply

Security Audit disables Internet Message Control Protocol (ICMP) mask reply messages whenever possible. ICMP supports IP traffic by relaying information about paths, routes, and network conditions. ICMP mask reply messages are sent when a network devices must know the subnet mask for a particular subnetwork

in the internetwork. ICMP mask reply messages are sent to the device requesting the information by devices that have the requested information. These messages can be used by an attacker to gain network mapping information.

The configuration that will be delivered to the router to disable ICMP mask reply messages is as follows:

```
no ip mask-reply
```

This fix can be undone. To learn how, click Undoing Security Audit Fixes.

Disable IP Unreachables on NULL Interface

Security Audit disables Internet Message Control Protocol (ICMP) host unreachable messages whenever possible. ICMP supports IP traffic by relaying information about paths, routes, and network conditions. ICMP host unreachable messages are sent out if a router receives a nonbroadcast packet that uses an unknown protocol, or if the router receives a packet that it is unable to deliver to the ultimate destination because it knows of no route to the destination address. Because the null interface is a packet sink, packets forwarded there will always be discarded and, unless disabled, will generate host unreachable messages. In that case, if the null interface is being used to block a Denial-of-Service attack, these messages flood the local network with these messages. Disabling these messages prevents this situation. In addition, because all blocked packets are forwarded to the null interface, an attacker receiving host unreachable messages could use those messages to determine Access Control List (ACL) configuration.

If the “null 0” interface is configured on your router, Security Audit will deliver the following configuration to the router to disable ICMP host unreachable messages for discarded packets or packets routed to the null interface is as follows:

```
int null 0
no ip unreachables
```

This fix can be undone. To learn how, click Undoing Security Audit Fixes.

Enable Unicast RPF on Outside Interfaces

Security Audit enables unicast Reverse Path Forwarding (RPF) on all interfaces that connect to the Internet whenever possible. RPF is a feature that causes the router to check the source address of any packet against the interface through which the packet entered the router. If the input interface is not a feasible path to the source address according to the routing table, the packet will be dropped. This source address verification is used to defeat IP spoofing.

This works only when routing is symmetric. If the network is designed in such a way that traffic from host A to host B may normally take a different path than traffic from host B to host A, the check will always fail, and communication between the two hosts will be impossible. This sort of asymmetric routing is common in the Internet core. Ensure that your network does not use asymmetric routing before enabling this feature.

In addition, unicast RPF can be enabled only when IP Cisco Express Forwarding (CEF) is enabled. Security Audit will check the router configuration to see if IP CEF is enabled. If IP CEF is not enabled, Security Audit will recommend that IP CEF be enabled and will enable it if the recommendation is approved. If IP CEF is not enabled, by Security Audit or otherwise, unicast RPF will not be enabled.

To enable unicast RPF, the following configuration will be delivered to the router for each interface that connects outside of the private network, replacing <*outside interface*> with the interface identifier:

```
interface <outside interface>
ip verify unicast reverse-path
```

Enable Firewall on All of the Outside Interfaces

If the Cisco IOS image running on the router includes the Firewall feature set, then Security Audit will enable Context-Based Access Control (CBAC) on the router whenever possible. CBAC, a component of the Cisco IOS Firewall feature set, filters packets based on application-layer information, such as what kinds of commands are being executed within the session. For example, if a command that is not supported is discovered in a session, the packet can be denied access.

CBAC enhances security for TCP and User Datagram Protocol (UDP) applications that use well-known ports, such as port 80 for HTTP or port 443 for Secure Sockets Layer (SSL). It does this by scrutinizing source and destination

addresses. Without CBAC, advanced application traffic is permitted only by writing Access Control Lists (ACLs). This approach leaves firewall doors open, so most administrators tend to deny all such application traffic. With CBAC enabled, however, you can securely permit multimedia and other application traffic by opening the firewall as needed and closing it all other times.

To enable CBAC, Security Audit will use Cisco CP's Create Firewall screens to generate a firewall configuration.

Set Access Class on HTTP Server Service

Security Audit enables the HTTP service on the router with an access class whenever possible. The HTTP service permits remote configuration and monitoring using a web browser, but is limited in its security because it sends a clear-text password over the network during the authentication process. Security Audit therefore limits access to the HTTP service by configuring an access class that permits access only from directly connected network nodes.

The configuration that will be delivered to the router to enable the HTTP service with an access class is as follows:

```
ip http server
ip http access-class <std-acl-num>
!
!HTTP Access-class:Allow initial access to direct connected subnets !
!only
access-list <std-acl-num> permit <inside-network>
access-list <std-acl-num> deny any
```

Set Access Class on VTY Lines

Security Audit configures an access class for vty lines whenever possible. Because vty connections permit remote access to your router, they should be limited only to known network nodes.

The configuration that will be delivered to the router to configure an access class for vty lines is as follows:

```
access-list <std-acl-num> permit <inside-network>
access-list <std-acl-num> deny any
```

In addition, the following configuration will be applied to each vty line:

```
access-class <std-acl-num>
```

Enable SSH for Access to the Router

If the Cisco IOS image running on the router is a crypto image (an image that uses 56-bit Data Encryption Standard (DES) encryption and is subject to export restrictions), then Security Audit will implement the following configurations to secure Telnet access whenever possible:

- Enable Secure Shell (SSH) for Telnet access. SSH makes Telnet access much more secure.
- Set the SSH timeout value to 60 seconds, causing incomplete SSH connections to shut down after 60 seconds.
- Set the maximum number of unsuccessful SSH login attempts to two before locking access to the router.

The configuration that will be delivered to the router to secure access and file transfer functions is as follows:

```
ip ssh time-out 60
ip ssh authentication-retries 2
!
line vty 0 4
transport input ssh
!
```

Note After making the configuration changes above, you must specify the SSH modulus key size and generate a key. Use the SSH page to do so.

Enable AAA

Cisco IOS Authentication, Authorization, and Accounting (AAA) is an architectural framework for configuring a set of three independent security functions in a consistent manner. AAA provides a modular way of performing authentication, authorization, and accounting services.

Cisco CP will perform the following precautionary tasks while enabling AAA to prevent loss of access to the router:

- Configure authentication and authorization for VTY lines

  The local database will be used for both authentication and authorization.
- Configure authentication for a console line

  The local database will be used for authentication.
- Modify HTTP authentication to use the local database

Configuration Summary Screen

This screen displays a list of all the configuration changes that will be delivered to the router configuration, based on the security problems that you selected to fix in the Report Card screen.

Cisco CP and Cisco IOS AutoSecure

AutoSecure is a Cisco IOS feature that, like Cisco CP, lets you more easily configure security features on your router, so that your network is better protected. Cisco CP implements almost all of the configurations that AutoSecure affords.

AutoSecure Features Implemented in Cisco CP

The following AutoSecure features are implemented in this version of Cisco CP. For an explanation of these services and features, click the links below:

- Disable SNMP
- Disable Finger Service
- Disable PAD Service
- Disable TCP Small Servers Service
- Disable IP BOOTP Server Service
- Disable IP Identification Service
- Disable CDP
- Disable IP Source Route

- Disable IP Redirects
- Disable IP Proxy ARP
- Disable IP Directed Broadcast
- Disable MOP Service
- Disable IP Unreachables
- Disable IP Unreachables on NULL Interface
- Disable IP Mask Reply
- Enable Password Encryption Service
- Disable IP Unreachables on NULL Interface
- Set Minimum Password Length to Less Than 6 Characters
- Enable IP CEF
- Enable Firewall on All of the Outside Interfaces
- Set Users
- Enable Logging
- Enable Firewall on All of the Outside Interfaces
- Set Minimum Password Length to Less Than 6 Characters
- Enable Firewall on All of the Outside Interfaces
- Enable Unicast RPF on Outside Interfaces
- Enable Firewall on All of the Outside Interfaces

AutoSecure Features Not Implemented in Cisco CP

The following AutoSecure features are not implemented in this version of Cisco CP:

- Disabling NTP—Based on input, AutoSecure will disable the Network Time Protocol (NTP) if it is not necessary. Otherwise, NTP will be configured with MD5 authentication. Cisco CP does not support disabling NTP.
- Configuring AAA—If the Authentication, Authorization, and Accounting (AAA) service is not configured, AutoSecure configures local AAA and prompts for configuration of a local username and password database on the router. Cisco CP does not support AAA configuration.

- Setting SPD Values—Cisco CP does not set Selective Packet Discard (SPD) values.
- Enabling TCP Intercepts—Cisco CP does not enable TCP intercepts.
- Configuring anti-spoofing ACLs on outside interfaces—AutoSecure creates three named access lists used to prevent anti-spoofing source addresses. Cisco CP does not configure these ACLs.

AutoSecure Features Implemented Differently in Cisco CP

- Disable SNMP—Cisco CP will disable SNMP, but unlike AutoSecure, it does not provide an option for configuring SNMP version 3.
- Enable SSH for Access to the Router—Cisco CP will enable and configure SSH on crypto Cisco IOS images, but unlike AutoSecure, it will not enable Service Control Point (SCP) or disable other access and file transfer services, such as FTP.

Security Configurations Cisco CP Can Undo

This table lists the security configurations that Cisco CP can undo.

Security Configuration	Equivalent CLI
Disable Finger Service	No service finger
Disable PAD Service	No service pad
Disable TCP Small Servers Service	No service tcp-small-servers no service udp-small-servers
Disable IP BOOTP Server Service	No ip bootp server
Disable IP Identification Service	No ip identd
Disable CDP	No cdp run
Disable IP Source Route	No ip source-route
Enable NetFlow Switching	ip route-cache flow
Disable IP Redirects	no ip redirects
Disable IP Proxy ARP	no ip proxy-arp

Security Configuration	Equivalent CLI
Disable IP Directed Broadcast	no ip directed-broadcast
Disable MOP Service	No mop enabled
Disable IP Unreachables	int <all-interfaces> no ip unreachables
Disable IP Mask Reply	no ip mask-reply
Disable IP Unreachables on NULL Interface	int null 0 no ip unreachables
Enable Password Encryption Service	service password-encryption
Enable TCP Keepalives for Inbound Telnet Sessions	service tcp-keepalives-in
Enable TCP Keepalives for Outbound Telnet Sessions	service tcp-keepalives-out
Disable IP Gratuitous ARPs	no ip gratuitous arps

Undoing Security Audit Fixes

Cisco CP can undo this security fix. If you want Cisco CP to remove this security configuration, run the Security Audit wizard. In the Report Card window, select the option **Undo Security Configurations**, place a check mark next to this configuration and other configurations that you want to undo, and click **Next>**.

Add or Edit Telnet/SSH Account Screen

This screen lets you add a new user account or edit an existing user account for Telnet and SSH access to your router.

User Name

Enter the username for the new account in this field.

Password

Enter the password for the new account in this field.

Confirm Password

Reenter the new account password in this field for confirmation. The entry in this field must match the entry in the password field.

Configure User Accounts for Telnet/SSH Page

This screen lets you manage the user accounts that have Telnet or Secure Shell (SSH) access to your router. The table in this screen shows each Telnet user account, listing the account username and displaying asterisks to represent the account password. Note that this screen appears only if you have not already configured any user accounts; therefore, the table on this screen is always empty when it is initially displayed.

Enable Authorization for Telnet Check Box

Check this box to enable Telnet and SSH access to your router. Clear this box to disable Telnet and SSH access to your router.

Add... Button

Click this button to display the Add a User Account screen, letting you add an account by assigning the account a username and password.

Edit... Button

Click a user account in the table to select it, and click this button to display the Edit a User Account screen, letting you edit the username and password of the selected account.

Delete Button

Click a user account in the table to select it, and click this button to delete the selected account.

Enable Secret and Banner Page

This screen lets you enter a new enable secret and a text banner for the router.

The enable secret is an encrypted password that provides administrator-level access to all functions of the router. It is vital that the secret be secure and difficult to crack. Your secret must be a minimum of six characters long, and it is recommended that you include both alphabetic and numeric characters and that you do not use a word that can be found in a dictionary, or that might be personal information about yourself that someone might be able to guess.

The text banner will be displayed whenever anyone connects to your router using Telnet or SSH. The text banner is an important security consideration because it is a method of notifying unauthorized individuals that access to your router is prohibited. in some jurisdictions, this is a requirement for civil and/or criminal prosecution.

New Password

Enter the new enable secret in this field.

Re-enter New Password

Re-enter the new enable secret in this field for verification.

Login Banner

Enter the text banner that you want configured on your router.

Logging Page

This screen lets you configure the router log by creating a list of syslog servers where log messages will be forwarded, and by setting the logging level, which determines the minimum severity a log message must have in order for it to be captured.

IP Address/Hostname Table

This table displays a list of hosts to where the router log messages will be forwarded. These hosts should be syslog servers that can trap and manage the router log messages.

Add... Button

Click this button to display the IP Address/Host Name screen, letting you add a syslog server to the list by entering either its IP address or host name.

Edit... Button

Click a syslog server in the table to select it, and click this button to display the IP Address/Host Name screen, letting you edit the IP address or host name of the selected syslog server.

Delete Button

Click a syslog server in the table to select it, and click this button to delete the selected syslog server from the table.

Set logging level Field

In this field, select the minimum severity level that a router log message must have in order for it to be trapped and forwarded to the syslog server(s) in the table on this screen. A log message severity level is shown as a number from 1 through 7, with lower numbers indicating more severe events. The descriptions of each of the severity levels are as follows:

- 0 - emergencies

  System unusable
- 1- alerts

  Immediate action needed
- 2 - critical

  Critical conditions
- 3 - errors

  Error conditions

- 4 - warnings

  Warning conditions
- 5 - notifications

  Normal but significant condition
- 6 - informational

  Informational messages only
- 7 - debugging

  Debugging messages

PART 5

Configuring Unified Communications Features

This section provides information about how to configure voice features on the router.

CHAPTER 47

Unified Communications

You can configure the device in one of the following modes: Cisco Unified Border Element, Cisco Unified Communications Manager Express, TDM Gateway, Media Resources, and Cisco Unified CME as SRST.

Note For ISR-G2 routers, the Unified Communications folder is available only if the Unified Communications license is installed and enabled on the router.

See the following topics for more information:

- Understanding Unified Communications Features, page 47-2
- Configuring Unified Communication Features, page 47-4
- Features Available in Each Unified Communication Feature, page 47-5
- Unified Communications Features Reference, page 47-7

Understanding Unified Communications Features

If Cisco Configuration Professional (Cisco CP) discovers that no Unified Communication feature is configured on the device, you are prompted to configure the device in one of the modes before you can configure any of the other voice features.

You can configure the device in one of the following modes:

- Cisco Unified Border Element mode—You can configure the device to work as a Cisco Unified Border Element (CUBE). The Cisco Unified Border Element carries end-to-end IP traffic through SIP trunking across different enterprises and service provider networks.
- Cisco Unified Communications Manager Express mode—You can configure the device as a host for Cisco Unified Communications Manager Express (Cisco Unified CME). In this mode, the Integrated Services Router (ISR) acts as a call processing agent, and all the phones are registered with the ISR. You should configure all dial plans on this router to process the call.
- TDM Gateway mode—You can configure the device as a gateway to the router hosting Cisco Unified CME. Call control and media translation are separated into two devices, the voice gateway handles media translation and a call agent handles call control. A call-control device controls and tracks the state of each voice port on the gateway. Typically, public switched telephone network (PSTN) connections, such as FXO, FXS, and PRI lines, terminate in the gateway. The gateway translates calls made between the PSTN and the IP network. The gateway does not make any call routing decisions; it routes calls in response to instructions from the call agent, Cisco Unified Call Manager.

- Cisco Unified SRST mode—You can configure the device to operate in Survivable Remote Site Telephony (SRST) mode when the connection to the Cisco Unified Communications Manager is lost, choose the Cisco Unified SRST radio button. During fallback, the router uses the H.323 default call-routing application when it looses contact with the Cisco Unified Call Manager. When using fallback, you must configure at least one dial peer with a destination pattern that routes outbound calls if Cisco Unified Call Manager is not available. That destination pattern is typically a wild card pattern that matches all outbound call, such as "9T." Typically, calls are forwarded to PSTN using plain old telephone service (POTS) dial-peers. Occasionally the calls are forwarded to a different gateway with VoIP dial-peers. Incoming dial-peers can also be configured to serve incoming calls during fallback. During normal operation of gateway, these dial peers are not used.
- Cisco Unified CME as SRST mode—You can configure the device to provide call-handling support for Cisco Unified IP phones if the phones lose connection to remote primary, secondary, or tertiary Cisco Unified Communications Manager installations, choose the Cisco Unified CME as SRST radio button. When Cisco Unified SRST functionality is provided by Cisco Unified CME, provisioning of phones is automatic. In addition, during periods of fallback, most of the Cisco Unified CME features, such as hunt-groups, call park, and access to the Cisco Unity voice messaging services using SCCP protocol, are available for the phones.
- Media Resources mode—You can configure conferencing and transcoding on the device. Cisco Unified Communications Manager media resource groups and media resource group lists provide a way to manage resources within a cluster. The Media Resources option is available if DSP (Digital Signal Processor) resources (PVDM cards) are installed on the device.

Related Topics

- Configuring Unified Communication Features, page 47-4
- Features Available in Each Unified Communication Feature, page 47-5
- Unified Communications Features Reference, page 47-7

Configuring Unified Communication Features

When you first click the **Unified Communications** folder, Unified Communications Features is the only branch visible. To display the voice features to configure, do the following:

Step 1 Choose the mode in which you want the device to operate. The options are:

- Cisco Unified Border Element—Check the **Cisco Unified Border Element** check box to have the device act as a CUBE. CUBE facilitates connectivity to the IP Trunk provider and other enterprise applications.
- IP Telephony—Configures the device as a call processing agent for IP Phones or in case of connection failure, configures it to provide call processing.

The IP Telephony mode contains three options:

  - Cisco Unified Call Manager Express—Click the **Cisco Unified CME** radio button for the device to operate in CME mode.
  - Cisco Unified SRST—Click the **Cisco Unified SRST** radio button for the device to operate in SRST mode when the connection to Cisco Unified Communications Manager is lost.
  - Cisco Unified CME as SRST—Click the **Cisco Unified CME as SRST** radio button for the device to operate in CME mode providing the SRST functionality when the connection to the Cisco Unified Communications Manager is lost.

- TDM Gateway—Check the **TDM Gateway** check box to configure the device as a MGCP/H.323/SIP gateway.
- Media Resources—Check the **Media Resources** check box to use the device for conferencing and transcoding. This option is seen only if PVDMs are available on the device.

Step 2 Click **OK**.

Step 3 Click **Unified Communications** in the left navigation tree. The configuration options are displayed for the mode that you chose. See Features Available in Each Unified Communication Feature, page 47-5.

Related Topics

- Understanding Unified Communications Features, page 47-2
- Features Available in Each Unified Communication Feature, page 47-5
- Unified Communications Features Reference, page 47-7

Features Available in Each Unified Communication Feature

The voice features you can configure depend on the mode that you choose.

- When you choose the **Cisco Unified Communications Manager Express** mode option, you can configure these features:
  - Telephony Settings
  - Users, Phones, and Extensions
  - PSTN
  - Dial Plans
  - Telephony Features
  - Voice Mail (Voice Mail is available only if CUE module is present)
  - Firmware

- When you choose the TDM **Gateway** mode option, you can configure these features:
  - Telephony Settings
  - Users, Phones, and Extensions
  - PSTN
  - Dial Plans
  - Voice Mail
  - Firmware
- When you choose the **SRST** mode option, you can configure these features:
  - SRST Settings
  - Gateway Settings (if TDM Gateway mode is also selected)
  - VoIP Settings
  - Trunks
  - Dial Plan
  - Media Resources (if DSPs are present on the device)
- When you choose the **Cisco Unified CME as SRST** mode option, you can configure these features:
  - CME as SRST Settings
  - Users, Phones, and Extensions
  - Advanced Telephony features
  - Gateway Settings (if TDM Gateway mode is also selected)
  - Telephony Features
  - Trunks
  - VoIP Settings
  - Dial Plans
  - Media Resources

Note When you choose the **Cisco Unified CME as SRST** option that is provided under the Gateway mode, the left navigation tree displays both the Cisco Unified CME as SRST and the Gateway features.

- When you choose the **Cisco Unified Border Element** mode option, you can configure these features:
  - VoIP Settings
  - Gateway Settings (if TDM Gateway mode is selected)
  - Trunks
  - Dial Plan
  - Media Resources
  - Telepresence

Related Topics

- Understanding Unified Communications Features, page 47-2
- Configuring Unified Communication Features, page 47-4
- Unified Communications Features Reference, page 47-7

Unified Communications Features Reference

The following topic describes the window used to configure Unified Communication Features:

- Unified Communications Features Summary Page, page 47-8
- Edit Unified Communications Features Page, page 47-8

Unified Communications Features Summary Page

Use the Unified Communications Features Summary page to view the configured mode and available hardware on the device.

How to Get to This Page

Choose **Configure > Unified Communications > Unified Communications Features**.

Related Topics

- Edit Unified Communications Features Page, page 47-8

Field Reference

Table 47-1 Unified Communications Features Summary Page

Element	Description
The values displayed depend on the options selected under **Configure > Unified Communications > Unified Communications Features > Edit**.	
Edit Button	Click the Edit button to configure or edit the Unified Communications features.
Reset to Default Button	Click the Reset to Default button to clear voice configuration from the device.

Edit Unified Communications Features Page

Use the Edit Unified Communications Features page to select the mode in which you want the device to operate.

How to Get to This Page

Choose **Configure > Unified Communications > Unified Communications Features > Edit**.

Related Topics

- Unified Communications Features Summary Page, page 47-8
- Understanding Unified Communications Features, page 47-2
- Configuring Unified Communication Features, page 47-4
- Features Available in Each Unified Communication Feature, page 47-5

Field Reference

Table 47-2 Edit Unified Communications Features Page

Element	Description
Cisco Unified Border Element check box	Check this check box to enable connectivity to IP Trunk provider and other enterprise applications.
Check the IP Telephony check box to select one of the options under it. You can configure the device as a call processing agent, or in case of connection failure to the Cisco Unified Communications Manager, configure it to provide connection:	
• CUCME—Cisco Unified Communications Call Manager Express radio button	Click this radio button to use the device as a Cisco Unified Communications Manager Express (Cisco Unified CME) configuration device. This option is selected when telephony-service is configured. When you choose the **Cisco Unified Communications Manager Express** option, and click **OK**, the left navigation tree displays the following: – Telephony Settings – Users, Phones, and Extensions – PSTN – Dial Plans – Telephony Features – Voice Mail – Firmware
• SRST—Cisco Unified Survivable Remote Site Telephony radio button	Click this radio button to have the device operate in Survivable Remote Site Telephony (SRST) mode when connection to the Cisco Unified Communications Manager is lost.

Table 47-2 Edit Unified Communications Features Page (continued)

Element	Description
• Cisco Unified Call Manager Express as Cisco Unified Survivable Remote Site Telephony radio button	Click this radio button for the device to provide CME functionality during fallback when connection to the WAN interface or to the Cisco Unified Communications Manager is lost. When you choose the **Cisco Unified CME as SRST** option and click **OK**, the left navigation tree displays the following: – CME as SRST Settings – Users, Phones, and Extensions – PSTN – Dial Plans – Telephony Features – Voice Mail
TDM Gateway check box	Check this check box to configure the device to connect the private voice network to the external network. The device can be configured as a MGCP/SIP/H.323 gateway. The TDM Gateway option is available if trunks are installed on the device.
Media Resources check box	Check this check box to enable conferencing and transcoding on the device. The Media Resources option is available if DSP (Digital Signal Processor) resources (PVDM cards) are installed on the device.

CHAPTER 48

CME as SRST

For information about how to use Cisco Configuration Professional (Cisco CP) to configure the CME as SRST feature, see the screencast at: http://www.cisco.com/en/US/docs/net_mgmt/cisco_configuration_professional/scrcst/ccpsc.html.

Note You must have internet access to view the screencast.

CHAPTER 49

SRST Settings

Cisco Unified Survivable Remote Site Telephony (SRST) is embedded in the software running on Cisco routers. This chapter describes how to set parameters such as licenses, date format, and time format.

This chapter contains the following sections:

- Configuring SRST Settings
- Configure SRST Settings

Configuring SRST Settings

Configure SRST Settings by selecting the related parameters.

Related Link

- Configure SRST Settings

SRST Settings Reference

The following topic describes the window used to configure voice gateway mode:

- Configuring SRST Settings
- Configure SRST Settings

Configure SRST Settings

Cisco Unified Survivable Remote Site Telephony (SRST) is embedded in the software running on Cisco routers. Use this page to set parameters such as max phones, extensions supported, date format, time format, phone registration source IP address and message on fallback phones.

How to get to this screen

Click **Configure > Unified Communications > SRST Settings**.

Field Reference

Table 49-1 SRST Settings

Element	Description
Maximum number of Phones drop-down list - mandatory	Enter the maximum number of phones the device can support. **Note** This is a mandatory field.
Maximum number of Extensions field - mandatory	Enter the maximum number of extensions the device can support. **Note** This is a mandatory field.
Message on Fallback Phones field	Enter the status message displayed on the phones when they are in fallback mode.
Date Format drop-down list	Choose the format the date displays in on the phones.
Time Format	Click the 12 hour or 24 hour radio button.
Phone Registration Source IP Address drop-down list - mandatory	Choose the SRST router IP address. **Note** This is a mandatory field.

Related Link

- Configuring SRST Settings

CHAPTER 50

SRST Rerouting

Cisco Unified Survivable Remote Site Telephony (SRST) is embedded in the software running on Cisco routers. It takes advantage of a remote office's existing network to provide multi feature call-processing redundancy for centralized Cisco Manager and Cisco Manager Business Edition deployments if the office's WAN connection is lost.

This chapter contains the following sections:

- Configuring SRST Rerouting
- Configure SRST Rerouting

Note SRST Rerouting is available only if the router is in Gateway with SRST mode.

Configuring SRST Rerouting

Cisco Unified SRST is used for the remote office routers that support from 24 to 720 users in a centralized Call Manager processing environment, to back up IP phone calls and provide 911 emergency access by the public switched telephone network (PSTN).

Related Links

- Configure SRST Rerouting
- Edit or Create SRST Rerouting

SRST Rerouting Reference

The following topic describes the window used to configure voice gateway mode:

- Configuring SRST Rerouting
- Configure SRST Rerouting
- Edit or Create SRST Rerouting

Configure SRST Rerouting

In the SRST Rerouting screen, you can select the Cisco Unified Call Manager fallback parameters.

Up to 50 sets of rerouting alias rules can be created for calls to telephone numbers that are unavailable during Cisco Unified Call Manager fallback. An alias is activated when a telephone registers that has a phone number matching a configured alternate-number alias. Under that condition, an incoming call is rerouted to the alternate number. You can reroute multiple different numbers to the same target number.

The configured alternate-number must be a specific E.164 phone number or extension that belongs to an IP phone registered on the Cisco Unified SRST router. When an IP phone registers with a number that matches an alternate-number, an additional POTS dial peer is created. The destination pattern is set to the initial configured number-pattern, and the POTS dial peer voice port is set to match the voice port associated with the alternate-number.

How to get to this screen

Click **Configure > Unified Communications > Dial Plans > SRST Rerouting**.

Field Reference

Table 50-1 Telephony Settings

Element	Description
Numbers to Reroute During SRST Fallback	Source numbers to be rerouted.
Extension to Reroute To	Target number.

Edit or Create SRST Rerouting

You can edit an existing fallback alias or create a new one.

How to get to this screen

- Click **Configure > Unified Communications > Dial Plans > SRST Rerouting > Edit**.
- Click **Configure > Unified Communications > Dial Plans > SRST Rerouting > Create**.

Field Reference

Table 50-2 SRST Rerouting

Element	Description
... Reroute Numbers that are unavailable During SRST Fallback	Numbers to be rerouted can be identified by selection from a pre-population list, entered as a range, or entered as an individual number.
Extension to Reroute To	Target extension number.

Related Links

- Configuring SRST Rerouting
- Configure SRST Rerouting

CHAPTER 51

Gateway Settings

Cisco Configuration Professional supports a gateway mode with Media Gateway Control Protocol (MGCP), Session Initiation Protocol (SIP), or H.323 protocol for communication from the gateway. When you change the mode from Voice Mode to Gateway Mode, all the configuration that was done as part of Voice Mode, that is telephony service and the rest of all voice features, is erased on the device and from the database. The configuration on CUE is also erased. If SRST is configured, that is also erased.

This chapter contains the following sections:

- Configuring Gateway Settings
- Gateway Settings

Configuring Gateway Settings

Configure gateway settings (the gateway to Cisco Communications Manager (CCM)) by selecting the gateway type and setting the related parameters.

Gateway Settings Reference

The following topic describes the window used to configure gateway settings:

- Gateway Settings
- Configuring Gateway Settings

Gateway Settings

In the Gateway Settings screen, you can select the gateway and operating parameters.

Dial Plans configured on PSTN Trunks translate E.164 numbers into extensions. VoIP dial plans forward those calls to a Cisco Call Manager. For redundancy, there can be more than one Cisco Call Manager. If communication with the primary Cisco Call Manager fails, the gateway queries the secondary Cisco Call Manager to process the call, and so forth. In Cisco Configuration Professional, up to three Cisco Call Managers are supported.

How to get to this screen

Click **Configure > Unified Communications > Gateway Settings**.

Related Link

- Configuring Gateway Settings

Field Reference

Table 51-1 Gateway Setting

Element	Description
Gateway Type	Choose one of these protocols: • MGCP • H.323 • SIP
Primary Call Manager IP Address/Host Name	After the last active call ends (when there is no voice call in setup mode on the gateway), control returns to this primary Cisco Call Manager.
Secondary Call Manager IP Address/Host Name	After the last active call ends, control returns to the secondary Cisco Call Manager if the primary Cisco Call Manager is not available.
Tertiary Call Manager IP Address/Host Name	After the last active call ends, control returns to the tertiary Cisco Call Manager if the primary and secondary Cisco Call Manager are not available.
TFTP Server IP Address/Host Name	Location (audio file URL or directory in the TFTP server) where the audio files are stored.

CHAPTER 52

Unified Communication Security Audit

This chapter contains the following:

- Configuring Unified Communication Security Audit, page 52-1
- Configuring CUE: Restriction Table, page 52-2

Configuring Unified Communication Security Audit

For information about how to use Cisco Configuration Professional (Cisco CP) to configure the Unified Communication Security Audit feature, see the screencast at:
http://www.cisco.com/en/US/docs/net_mgmt/cisco_configuration_professional/scrcst/ccpsc.html.

For configuring the CUE restriction table in the Unified Communication Security Audit wizard, see Configuring CUE: Restriction Table, page 52-2.

Note

- The Unified Communication Security Audit feature is introduced in Cisco CP 1.4.
- The CUE restriction table in the Unified Communication Security Audit wizard is introduced in Cisco CP 2.1.
- You must have internet access to view the screencast.

Configuring CUE: Restriction Table

You can configure the CUE restriction table from the Unified Communication Security Audit wizard pages. For information about how to configure the CUE restriction table in the Unified Communication Security Audit wizard, see the screencast at: http://www.cisco.com/en/US/docs/net_mgmt/cisco_configuration_professional/scrcst/ccpsc.html.

Note

- The Unified Communication Security Audit feature is introduced in Cisco CP 1.4.
- The CUE restriction table in the Unified Communication Security Audit wizard is introduced in Cisco CP 2.1.
- You must have internet access to view the screencast.

CHAPTER 53

Telephony Settings

Configure telephony licenses and softkey functions.

This chapter contains the following sections:

- Configuring Telephony Settings, page 53-1
- Telephony Settings page, page 53-2
- Edit Telephony Settings dialog box, page 53-4

Configuring Telephony Settings

Configure telephony by selecting the license type and softkey settings.

Telephony Settings Reference

The following topic describes the windows used to view and configure telephony settings:

- Telephony Settings page, page 53-2
- Edit Telephony Settings dialog box, page 53-4

Telephony Settings page

Use the Telephony Settings page to view the general telephony settings and softkey telephony values.

When you click **Apply**, the appropriate phone reset or restart prompt is displayed, based on what parameters you have edited.

How to get to this page

Click **Configure > Unified Communications > Telephony Settings**.

Related Topics

- Edit Telephony Settings dialog box, page 53-4

Field Reference

Table 53-1 Telephony Settings

Element	Description
General Settings	
Cisco Communications Manager Express version	Displays the version of Cisco Communications Manager Express that the router is running.
Supported Endpoints	Displays the supported endpoint, e.g. SIP or SCCP.
Telephony License Type	Choose the license that specifies the maximum number of users that can be configured on your device or select **Other**. If you selected **Other**, enter the custom maximum number of licenses you support. If you enter a number that matches a system license, that value is displayed after you apply the configuration. If it does not match, the license type remains **Other** and your custom entry is displayed.
Maximum Number of Phones	Displays the maximum number of phones configured on the router. **Note** Depending on the version of Cisco Unified CME that is installed on the router, the range of extension numbers that you can add changes.

Table 53-1 Telephony Settings (continued)

Element	Description
Maximum Number of Extensions	Displays the maximum number of extensions that can be configured on the router. **Note** Depending on the version of Cisco Unified CME that is installed on the router, the range of extension numbers that you can add changes.
IP Address for Phone Registration	Displays the IP address for registering the phone.
Date Format	Displays the telephony date format.
Time Format	Displays the telephony time format.
System Config	
Message Displayed on Phone	Displays the message on the phone.
Timeouts	
Interval Between Subsequent Digits Entered	Displays the time interval between digits entered.
Wait Duration After Busy Tone	Displays the time to wait after busy tone.
Duration of Phone Ring Without Answer	Displays how long the phone will ring when there is no answer.
Enable FXO Hook Flash	Check to enable Flash soft-key display. Certain public switched telephone network (PSTN) services, such as three-way calling and call waiting, require hook flash. A soft key labeled **flash** is available on phones that support a soft-key display and use foreign exchange office (FXO) lines attached to the Cisco Manager Express (Cisco Unified CME) system.
Enable Hunt Group Logout (Hlog)	Check to enable **Hlog** soft-key. This enables separate handling of do-not-disturb (DND). When the Hunt Group Logout (Hlog) soft-key is pressed, the phone changes from the ready to not-ready status or from the not-ready to ready status. When the phone is in the not-ready status, it does not receive calls from the hunt group, but it is still able to receive calls that do not come through the hunt group (calls that are dialed directly to the extension number).

Edit Telephony Settings dialog box

Use this dialog box to edit the configured values for telephony settings.

Note To configure endpoints as SIP or SCCP and SIP, enable SIP to SIP connection and Local SIP Registrar server from VoIP Settings.

How to get to this page

Click **Configure > Unified Communications > Telephony Settings > Edit**.

Related Topics

- Telephony Settings page, page 53-2

Field Reference

Table 53-2 Edit Telephony Settings

Element	Description
General tab	
General Settings pane	
Cisco Communications Manager Express version	*Display only.* Displays the version of Cisco Communications Manager Express that the router is running.
Supported Endpoints drop-down list	Choose SCCP, SIP, or SCCP and SIP from the drop-down list.
Telephony License Type	Choose the license that specifies the maximum number of users that can be configured on your device or select **Other**. If you selected **Other**, enter the custom maximum number of licenses you support. If you enter a number that matches a system license, that value is displayed after you apply the configuration. If it does not match, the license type remains **Other** and your custom entry is displayed.

Table 53-2 Edit Telephony Settings (continued)

Element	Description
Maximum Number of Phones drop-down list	Choose the maximum number of phones that can be configured on the router. If you choose Other, enter the maximum number of phones in the field, within the range specified. **Note** Depending on the version of Cisco Unified CME that is installed on the router, the range of phone numbers that you can add changes. This is a mandatory field.
Maximum Number of Extensions field	Enter the maximum number of extensions that can be configured on the router, within the range specified. **Note** Depending on the version of Cisco Unified CME that is installed on the router, the range of extension numbers that you can add changes. This is a mandatory field.
Date Format drop-down list	Choose the telephony date format.
Time Format radio buttons	Click the telephony time format.
Phone Registration Source IP Address drop-down list	Choose the phone registration source IP address. This is a mandatory field.
Secondary dial-tone digit field	Enter a value for the secondary dial-tone.
SoftKeys Settings pane	
Enable FXO hook flash for softkey templates check box	This check box is displayed if you chose SCCP or SCCP and SIP as the supported endpoints. Check to enable Flash soft-key display. Certain public switched telephone network (PSTN) services, such as three-way calling and call waiting, require hook flash. A soft key labeled **flash** is available on phones that support a soft-key display and use foreign exchange office (FXO) lines attached to the Cisco Unified Communications Manager Express (Cisco Unified CME) system.

Table 53-2 Edit Telephony Settings (continued)

Element	Description
Enable hunt group logout (Hlog) for softkey templates check box	This check box is displayed if you chose SCCP or SCCP and SIP as the supported endpoints. Check to enable **Hlog** soft-key. This enables separate handling of do-not-disturb (DND). When the Hunt Group Logout (Hlog) soft-key is pressed, the phone changes from the ready to not-ready status or from the not-ready to ready status. When the phone is in the not-ready status, it does not receive calls from the hunt group, but it is still able to receive calls that do not come through the hunt group (calls that are dialed directly to the extension number.
System Config tab **Timeouts tab** **DialPlan Pattern tab** **Transfer Pattern tab** **Phone URLs tab**	See the Edit Telephony Settings screencast at: http://www.cisco.com/en/US/docs/net_mgmt/cisco_configuration_professional/scrcst/ccpsc.html

CHAPTER 54

Advanced Telephony

For information about how to use Cisco Configuration Professional (Cisco CP) to configure the Advanced Telephony feature, see the screencast at: http://www.cisco.com/en/US/docs/net_mgmt/cisco_configuration_professional/scrcst/ccpsc.html.

Note You must have internet access to view the screencast.

CHAPTER 55

Importing Bulk Data

It is time consuming to enter data for individual users, extensions, phones, and voice mailboxes. To help you save time, Cisco Configuration Professional (Cisco CP) can import user, phone, extension, and mailbox information captured in a Cisco-compatible comma-separated-value (CSV) file that you create, and add that information to the device configuration. This chapter explains how to do this.

This chapter contains the following sections:

- Understanding the .CSV File, page 55-1
- Downloading the .CSV Template, page 55-6
- Using the Cisco Template to Create the .CSV File, page 55-6
- Using Cisco CP to Import Bulk Data, page 55-8
- Correcting Data Conflicts, page 55-9
- Import Bulk Data Screen Reference, page 55-10

Understanding the .CSV File

In an office phone system, user, phone, and extension information is interrelated. A user is assigned a user ID and a phone, and may be given a mailbox and call forwarding capabilities. That phone has a MAC address, and one or more extensions are assigned to it. You can input all this information in a .CSV file. The template .CSV file is shown in Example 55-1.

Example 55-1 Template Bulk Import Comma-Separated Value File

```
Version,1_1,,,,,,,,,,,,
Columns applicable to SCCP,ALL,,,,,,,,,,,,
Columns applicable to SIP,"UserID, Password, MAC Address, Phone Type, Protocol, Extension
Primary Number, Extension Label, Mailbox, CFB, CFNA, CFNA Timeout",,,,,,,,,,,,
UserID *,Password,First Name,Last Name,MAC Address *,Phone Type ,Protocol,Extension
Primary Number *,Extension Secondary Number,Line Mode,Extension Label,Mailbox
,CFB,CFNA,CFNA Timeout

jjsmith,John,Smith,AAAA.BBBB.CCCC,7940,201,4085551000,single,4085551001,Yes,411,410,15
ppeterson,James,Peterson,BBBB.CCCC.DDDD,7960,202,4085553006,dual,4085551002,No,412,420,16
lljohnson,Lisa,Johnson,CCCC.DDDD.EEEE,7940,203,4085553007,octal,4085551003,No,413,430,17
jjlee,Jane,Lee,DDDD.EEEE.FFFF,7931,204,4085553008,dual,4085551004,Yes,414,440,18
,Bob,Doe,DDDD.ECEE.FFFF,7931,205,4085553009,dual,4085551005,Yes,414,440,18
7931,206,4085553006,dual,4085551006,Yes,414,440,18,,,,
Bones,ny,DDDD.ECEE.FFFF,7931,207,4085553007,dual,4085551007,Yes,414,440,18,
allen,Allen,Long,DDDD.ECEE.FFFF,,,4085553008,dual,4085551008,Yes,414,440,18
```

The rows before the carriage return are used for the version number and the column headings. These must not be modified. The next rows contain sample data. You must replace this text with the data for your site.

Example 55-2 shows rows with real data that use the correct format:

Example 55-2 .CSV Bulk Import File Records

```
Version,1_1,,,,,,,,,,,,
Columns applicable to SCCP,ALL,,,,,,,,,,,,
Columns applicable to SIP,"UserID, Password, MAC Address, Phone Type, Protocol, Extension
Primary Number, Extension Label, Mailbox, CFB, CFNA, CFNA Timeout",,,,,,,,,,,,
UserID *,Password,First Name,Last Name,MAC Address *,Phone Type ,Protocol,Extension
Primary Number *,Extension Secondary Number,Line Mode,Extension Label,Mailbox
,CFB,CFNA,CFNA Timeout

jjones,John,Jones,000C.F142.4CDE,7940,201,4085551000,single,4085551001,Yes,411,410,15
ssmith,Steve,Smith,000C.F142.4CDF,7960,202,4085553006,dual,4085551002,No,400,400,15
ljohnson,Lisa,Johnson,000C.F142.5DDE,7940,203,4085553007,octal,4085551003,No,400,400,15
jlee,Jane,Lee,000C.F142.5EEC,7931,204,4085553008,single,4085551003,No,400,400,15
jlock,john,lock,001A.1234.ABCD,7961/14,206,4085553006,dual,4085551006,Yes,414,440,18
Bones,ny,,DDDD.ECEE.FFFF,7970/14x2,207,4085553007,dual,4085551007,Yes,414,440,18
alng,Al,Long,DDDD.ECEE.FFFF,IP Communicator,208,4085553008,dual,4085551008,Yes,414,440,18
```

Downloading the .CSV Template, page 55-6 explains how to use Cisco CP to download this file to the PC. Table 55-1 describes the data in this file.

Table 55-1 .CSV File Field Values

Field	Purpose, Value Types, and Examples	Default Value
Version	The version number is supplied in the template file and must not be changed. Value Type: Numbers Example: 1_1	The number supplied in the template. The template version 1_0 is supported for SCCP phones, extensions, and users.
User ID (Mandatory)	The user ID of the person who will use this phone. Value Type: Letters and numbers. Examples: jjones jjones2	No default value
First Name	The user's first name. Value Type: Letters Examples: Bill Julianne	No default value
Last Name	The user's last name. Value Type: Letters Examples: Jones Smith	No default value
MAC Address (Mandatory)	The phone's MAC address. Value Type: Hexadecimal numbers in 3 groups of 4, separated by periods. Examples: 000C.F142.4CDE 000C.F142.4CDF	No default value

Table 55-1 .CSV File Field Values (continued)

Field	Purpose, Value Types, and Examples	Default Value
Phone Type (Mandatory)	The phone model number. Value Type: Numbers The phone type is the model number of the phone. Examples: 7940 IP Communicator 7970/14x2 7961/14 Analog **Note** If a particular phone is non-Cisco or not supported on the IOS version, the phone type is displayed as Other.	No default value
Protocol	SIP/SCCP	SCCP.
Extension primary number (Mandatory)	The phone's primary extension number. Value Type: Numbers Examples: 201 202	No default value
Extension secondary number	The phone's secondary extension number. Value Type: Numbers Examples: 4085551000 4085553006 **Note** This field is not supported on SIP protocol.	No default value

Table 55-1 .CSV File Field Values (continued)

Field	Purpose, Value Types, and Examples	Default Value
Line Mode	The number of calls an extension on the phone can support. One of the following values: • single—The line supports a single call. • dual—The line supports two calls. This can be used for call waiting. • octo—The line supports eight calls.	dual
Extension Label	The softkey label for the extension. Value Type: Letters and numbers Examples: 4085551001 Service	None
Mailbox	Whether or not the user has a mailbox. One of the following values: • Yes, Y • No, N	No
Call Forward Busy (CFB)	The number to forward the call to when the number called does not answer. Value Type: Numbers Examples: 410, 411	No default value
Call Forward No Answer (CFNA)	The number to forward the call to when the number called does not answer. Value Type: Numbers Examples: 410, 411	No default value
CFNA Timeout	The number of seconds to wait before the number is forwarded. Value Type: Numbers Example: 20	18

Use the procedure in Downloading the .CSV Template, page 55-6 to download the template.

Downloading the .CSV Template

Cisco CP enables you to download a template that you can use to create the .CSV file. Perform the following steps to download the template:

Step 1 Choose a community, and select the device with Cisco Manager Express (Cisco Unified CME) installed for which you want to import the user, phone, and extension data.

Step 2 Click **Configure > Unified Communications > Unified Communications Features**.

Step 3 Ensure that Use router as Unified CME is chosen. If it is not, choose it.

Step 4 Click **Unified Communications > Users, Phones and Extensions > Extensions** or **Phones and Users**.

Step 5 In the Guided Configuration panel, click **Download** to begin downloading the Bulk Import .CSV template file. See Bulk Import, page 55-10 for more information.

Step 6 Save the file to the PC. Be sure to save it with the .CSV extension.

Using the Cisco Template to Create the .CSV File

You can use the Cisco-supplied template that you downloaded in Downloading the .CSV Template, page 55-6 to guide you in creating the .CSV file.

Complete the following tasks to create the .CSV file:

Step 1 Verify that you have enough telephony licenses to support the number of users that you are importing as well as the number of users already configured. You can verify the number of users already configured by going to **Configure > Unified Communications > Users, Phones and Extensions > Phones and Users** and

counting the users. You can verify the telephony license type that specifies the total number of licenses by going to **Configure > Unified Communications > Telephony Settings** and looking in the **Telephony License Type** field.

Step 2 Open a text editor. You can use a spreadsheet program if you want, but a spreadsheet program is not required to edit this file.

Step 3 In the editor, open the .CSV file that you downloaded in Downloading the .CSV Template, page 55-6. The first two or three rows contain the version number and column headings.

Note Be sure not to change the version number or column headings. Doing so will corrupt the .CSV file.

Step 4 Sample data is provided after the version number and column headings. Review this sample data to see how data must be entered in the file. See Understanding the .CSV File, page 55-1 for information on the type of data that you can enter in each column, and examples.

Step 5 Starting from the left, enter the information described in Understanding the .CSV File, page 55-1 for each row, using the column headings as your guide. It is not necessary to enter a value for every column, but for each row, the following columns must contain values:

- UserID
- MAC Address
- Phone Type
- Extension Primary Number

Step 6 When you have entered the rows that you need, delete the sample data. If you do not, the sample data will be imported along with the data that you have entered.

Step 7 Save the file. Be sure to save it with a .CSV file extension or Cisco CP will not be able to read it.

Step 8 Go to Using Cisco CP to Import Bulk Data, page 55-8 to import this data to the configuration for the device.

Using Cisco CP to Import Bulk Data

Use the following procedure to import user, phone, and extension data contained in a .CSV file into the device configuration.

Step 1 Choose a community, and select the device with Cisco Manager Express (Cisco Unified CME) installed for which you want to import the user, phone, and extension data.

Step 2 Click **Configure > Unified Communications > Unified Communications Features**.

Step 3 Ensure that Use router as Unified CME is chosen. If it is not, choose it.

Step 4 Click **Unified Communications > Users, Phones and Extensions > Extensions** or **Phones and Users**.

Step 5 In the Guided Configuration panel, click **Launch Wizard**. See Bulk Import, page 55-10 for more information.

Step 6 In the Select Bulk File screen, click **Browse** to locate the .CSV file on your PC or on the network. You cannot copy the path and paste it into the field; you must use the Browse button. When you have located the .CSV file, choose it and click **OK** in the dialog. The .CSV filename appears in the Bulk import file field. See Bulk Import Wizard—Select Bulk File, page 55-11 for information about this screen.

Step 7 Click **Next**. The .CSV file is read and basic validation is performed. When the .CSV file is being read in, you cannot click Cancel to stop the operation. The Summary screen is displayed after the .CSV file has been read.

Step 8 In the Summary screen, review the results of the operation. If a row is read in successfully, the screen displays the user ID, primary and secondary extension, and other information, and displays the word Imported in the Status column. If a row could not be read in, a Not Imported button is displayed in the Status column, and clicking this button displays the data that could not be read. Click Not Imported to view details about the record. See Bulk Import Wizard—Summary, page 55-12 for information about this screen.

Step 9 If there are errors that you want to correct click **Back** and follow the procedure in Correcting Data Conflicts, page 55-9 to correct them and have Cisco CP reread the file**.**

Step 10 Click **Next**. The Enable Rollback screen is displayed.

Step 11 To rollback the configuration and restore the router to the previous known stable configuration, check the **Enable Rollback** check box. See Bulk Import Wizard—Enable Rollback, page 55-13 for information about this screen.

Step 12 To start the bulk import process, click **Next**. During the bulk import operation, the Cancel button is disabled. The Apply Data screen is displayed.

Step 13 In the Apply Data screen, view the progress of the bulk import operation. See Bulk Import Wizard—Apply Data, page 55-14 for information about this screen.

Step 14 Click **Next**. The Finish screen is displayed.

Step 15 In the Finish screen, do the following:

- To open a browser window that displays details about the bulk import operation, click the **View Details** button.
- To restore the router to the previous known stable configuration, click the **Rollback** button, and then click **Yes** in the confirmation dialog box.

See Bulk Import Wizard—Finish, page 55-15 for information about this screen.

Step 16 Click **Finish** to close the wizard.

Step 17 Click **Unified Communications > Users**, **Phones**, **and Extensions > Phones and Users** to see the imported data.

Correcting Data Conflicts

If there are errors or conflicting data in the .CSV file, these problems are flagged in the Summary screen so that you can back out of the import operation and correct them before completing the import operation. To correct these data conflicts and other errors, complete these steps:

Step 1 Follow the procedure in Using Cisco CP to Import Bulk Data, page 55-8 to have Cisco CP read the .CSV file.

Step 2 In the Summary screen, note any errors found.

Step 3 Click **Back** to return to the Select .CSV File screen. You can leave the wizard open at this screen.

Step 4 Open the editor you used to create the .CSV file and correct the errors that Cisco CP found. For more information on .CSV file input requirements, review .CSV File Field Values, page 55-3.

Step 5 Save the .CSV file.

Step 6 In the Select .CSV File screen, click **Next**. Cisco CP rereads the file.

Step 7 In the Summary Screen, review the results. The word Imported appears in the Status column for rows that were successfully imported. If a row was successfully read on a previous attempt, or if there was an error, the Not Imported button is displayed for that row.

Step 8 Click **Not Imported** to determine if there is an error, or if the row was already successfully read.

Step 9 To correct additional errors, click **Back** and repeat Step 4 and Step 5.

Step 10 Repeat steps Step 3 through Step 9 to correct all errors found, then resume the procedure in Using Cisco CP to Import Bulk Data, page 55-8.

Import Bulk Data Screen Reference

The following topics describe the screens in the Import Bulk Data wizard:

- Bulk Import, page 55-10
- Bulk Import Wizard—Select Bulk File, page 55-11
- Bulk Import Wizard—Summary, page 55-12
- Bulk Import Wizard—Enable Rollback, page 55-13
- Bulk Import Wizard—Apply Data, page 55-14
- Bulk Import Wizard—Finish, page 55-15

Bulk Import

In this screen, download the .CSV template file and save it to the PC. Then, return to this screen to launch the bulk import wizard that allows you to import user, phone, extension, and mailbox information stored in the .CSV file.

How to get to this screen

Click **Configure > Unified Communications > Users, Phones, and Extensions > Extensions** or **Phones and Users > Launch Wizard**.

Related Links

- Using Cisco CP to Import Bulk Data, page 55-8

Field Reference

Table 55-2 Wizard Start Screen

Element	Description
Text description area	This text describes the capabilities of the bulk import wizard, and provides a short procedure for downloading the CSV template and launching the wizard.
Download link	To obtain a .CSV template file that you can use to enter the user and phone data, click **Download** and save the template file to the PC.
Launch Wizard	To start importing a .CSV file with user, phone, and extension information, click **Launch Wizard**.

Bulk Import Wizard—Select Bulk File

In the Select CSV File screen, browse for the .CSV file. The .CSV file may be stored on the PC or on the network.

How to get to this screen

Click **Configure > Unified Communications > Users, Phones, and Extensions > Extensions** or **Phones and Users > Launch Wizard**. Then click **Next** until you get to this screen.

Related Links

- Using the Cisco Template to Create the .CSV File, page 55-6
- Using Cisco CP to Import Bulk Data, page 55-8
- Correcting Data Conflicts, page 55-9

Field Reference

Table 55-3 Select CSV File

Element	Description
Bulk Import File	In this field, click **Browse** to locate and choose the .CSV file that contains the data that you want to import. Be sure that the .CSV file has the format described in Understanding the .CSV File, page 55-1. **Note** Do not copy the path and paste it into this field. You must use the Browse button. The name of the .CSV file appears in this field after you have located it and clicked **OK** in the browse dialog.

Bulk Import Wizard—Summary

In this screen, review the results of the read operation that Cisco CP performed on the .CSV file. For each record, this screen displays the user ID, primary extension, phone type, MAC address, and whether a mailbox is enabled. The data in this screen has not been imported to the router yet. If errors are reported, you can click **Back**, fix any errors found, and then click next in the previous screen to have Cisco CP reread the file and take you to this screen again.

Note Clicking **Next** starts the import process. Once started, the import process cannot be cancelled.

How to get to this screen

Click **Configure > Unified Communications > Users, Phones, and Extensions > Extensions** or **Phones and Users > Launch Wizard**. Then click **Next** until you get to this screen.

Related Links

- Using Cisco CP to Import Bulk Data, page 55-8
- Understanding the .CSV File, page 55-1
- Correcting Data Conflicts, page 55-9

Field Reference

Table 55-4 Bulk Import Wizard—Summary

Element	Description
Record Count	The number of records in the .CSV file.
Success	The number of user records imported in this attempt.
Failure	The number of records not imported in this attempt.
Not Imported Button	Appears when an error has been detected for the row, or when the row was successfully read on a previous attempt. Click for more information.

Summary Table Example

File Line Number	User ID	Primary Extension	Phone Type	MAC Address	Mailbox	Status
3	jsmith	201	7940	000C.F142.4CDE	Y	Imported
4	tjones		7960	000C.F142.4CDF	N	Not Imported
5	rwhite	204	7940	000C.F142.4CDC	Y	Imported

Bulk Import Wizard—Enable Rollback

In the Enable Rollback screen, check the **Enable Rollback** check box to rollback the entire configuration and restore the router to the previous known stable configuration.

The Rollback feature can be used in two scenarios:

- There are errors in the router configuration and you want to restore the router to the previous known stable configuration.
- There are no errors in the router configuration, but you want to revert back to the previous successful configuration.

How to get to this screen

Click **Configure > Unified Communications > Users, Phones, and Extensions > Extensions** or **Phones and Users > Launch Wizard**. Then click **Next** until you get to this screen.

Related Links

- Using the Cisco Template to Create the .CSV File, page 55-6
- Using Cisco CP to Import Bulk Data, page 55-8

Field Reference

Table 55-5 Bulk Import Wizard—Enable Rollback

Element	Description
Enable Rollback check box	Check this check box to rollback the entire configuration and restore the router to the previous known stable configuration. After you check the **Enable Rollback** check box, the Rollback button in the last wizard step (Finish page) is enabled. **Note** If the device contains module related configuration, then Cisco CP will save the running configuration before it delivers the actual configuration to the router.

Bulk Import Wizard—Apply Data

In this screen, view the progress of the import operation. The numbers shown in this screen change dynamically until all records are read.

How to get to this screen

Click **Configure > Unified Communications > Users, Phones, and Extensions > Extensions** or **Phones and Users > Launch Wizard**. Then click **Next** until you get to this screen.

Related Links

- Using Cisco CP to Import Bulk Data, page 55-8

Field Reference

Table 55-6 Bulk Import Wizard—Apply Data

Element	Description
Applying data to router	This is a progress bar that displays how much of the import process has been completed.

Table 55-6 Bulk Import Wizard—Apply Data (continued)

Element	Description
Current progress	Which record is being processed against the total number of records.
Total records processed	Total number of records processed.
Success	The number of records from the bulk import file successfully configured on the router.
Failure	The number of records from the bulk import file that were not configured on the router.

Bulk Import Wizard—Finish

In this screen, you can review details of the bulk import operation by clicking the **View Details** button, or you can restore the router to the previous known stable configuration by clicking the **Rollback** button.

How to get to this screen

Click **Configure > Unified Communications > Users, Phones, and Extensions > Extensions** or **Phones and Users > Launch Wizard**. Then click **Next** until you get to this screen.

Related Links

- Using Cisco CP to Import Bulk Data, page 55-8
- Understanding the .CSV File, page 55-1

Field Reference

Table 55-7 Bulk Import Wizard—Finish

Element	Description
Total records applied	The number of records imported.
Success	The number of records imported without error.
Failure	The number of records that could not be imported because of errors.
View Details button	Click to open a web page containing the log of the import operation. The log displays all fields in the .CSV file.

Table 55-7 Bulk Import Wizard—Finish (continued)

Element	Description
Rollback button	Click this button to restore the router to the previous known stable configuration, and then click **Yes** in the confirmation dialog box. Cisco CP verifies if there is sufficient memory in Flash to support Rollback. If there is sufficient memory, Cisco CP restores the router to the previous known stable configuration. **Note** The Rollback button is enabled when you check the **Enable Rollback** check box in the Enable Rollback wizard step, otherwise it is disabled.

CHAPTER 56

Users, Phones, and Extensions

This chapter provides information about how to configure extensions and phones, and then define a user and assign a phone, extensions, and mailbox to that user.

See the following sections for more information:

- User, Phones, and Extensions Basic Workflow, page 56-1
- Extensions, page 56-2
- Phones and Users Settings, page 56-21
- Importing Bulk Data, page 55-1

User, Phones, and Extensions Basic Workflow

1. Configure extensions.
2. Configure phones or users.
3. Assign the user with extensions, and optionally a mailbox.

Related Topics

- Extensions, page 56-2
- Phones and Users Settings, page 56-21
- Importing Bulk Data, page 55-1

Extensions

An extension, also known as a directory number or ephone-dn, is the software configuration that represents the line connecting a voice channel to a phone. An extension has one or more telephone numbers associated with it to allow call connections to be made. There are several types of extensions, which have different characteristics; for example, single-line, dual-line, and octo-line extensions. Each extension has a unique sequence number to identify it during configuration. Extensions are assigned to line buttons on phones during configuration.

To configure extensions in Cisco CP, enter the primary number; secondary number; and other parameters such as, call forwarding, extension preference, hunt settings, hold alert, night service bell, permission, watch mode, and single number reach, for each extension:

- Call Forwarding—Incoming calls are diverted to a specified number when the dialed number is busy or is not answered.
- Extension Preference—Order of preference in which the phone line is chosen when multiple lines have the same extension number.
- Hunt Settings—Incoming call is rolled over to another extension when the extension to which the call is sent is busy or is not answered.
- Hold Alert—Audible alert notification that starts when the call is on-hold, and repeats after a specified time interval.
- Night Service Bell—Calls are forwarded from extensions that are unstaffed during night service hours to another designated phone. You can either configure the night service phone to pickup the calls or you can forward the calls to a designated number.
- Permission—Dialing restrictions (permissions) configured on the extension number.

- Watch Mode Settings—Allows a phone user, such as a receptionist, to visually monitor the in-use status of an extension.

Note The Watch Mode Settings feature is supported on routers running Cisco Unified CME 4.1 and later versions.

- Single Number Reach (SNR)—Allows users to answer incoming calls on their desktop IP phone or at a remote destination, such as a mobile phone, and to pick up in-progress calls on the desktop phone or the remote phone without losing the connection. This allows callers to use a single number to reach the phone user. Calls that are not answered can be forwarded to voice mail.

  For incoming calls to the SNR extension, Cisco Unified CME rings the desktop IP phone first. If the IP phone does not answer within the configured amount of time, it rings the configured remote number while continuing to ring the IP phone. Unanswered calls are sent to a configured voice-mail number.

  SNR can be enabled only if Mobility exits in the ephone-dn. The Mobility feature allows you to manage calls using a single number and to transfer calls that are in progress between the desktop phone and the remote destination, for example a mobile phone.

Note The SNR feature is supported on routers running Cisco Unified CME 7.1 and later versions.

To configure extension numbers, choose **Configure > Unified Communications > Users, Phones, and Extensions > Extensions**. The Extensions summary page opens. From the Extensions summary page you can view configured extensions, create new extensions, edit extension information, delete extensions, and clone extensions.

See the following topics for more information:

- Creating, Editing, Deleting, and Cloning Extensions, page 56-4
- Extensions Reference, page 56-7
- Importing Bulk Data, page 55-1

Creating, Editing, Deleting, and Cloning Extensions

Procedure

Use this procedure to create, edit, delete, and clone extensions.

Step 1 Choose **Configure > Unified Communications > Users, Phones, and Extensions > Extensions**. The Extensions summary page opens. See Extensions Summary Page, page 56-7.

Step 2 To create an extension, do the following:

a. Click **Create**.

The Create Extension dialog box opens with the General tab selected by default.

b. In the General area, enter the primary number, secondary number, name to be displayed on phone line, and description. See Create or Edit Extension Dialog Box, page 56-12.

c. Choose the required values from the Line Mode/Simultaneous Number of Active Calls allowed on a Phone Button drop-down list and E.164 registration drop-down list.

d. To block caller ID, check the Block caller ID for calls from this extension check box.

e. In the Call Forwarding area, enter the number to forward all calls to, number to divert calls to when called number is busy, and number to divert unattended calls to. The No Answer Timeout is auto-populated when you fill in the other fields, you can then edit the value if required.

f. Click the **Single Number Reach** tab in the Create Extension dialog box.

The Single Number Reach area is displayed.

g. Check the Enable SNR for this extension check box.

The fields and check boxes on the page become active. The Enable mobility feature for this extension number check box is checked by default, when SNR is enabled.

h. Enter the remote number, seconds after which remote number is to be rung, seconds for time out, and number to forward unanswered calls to.

i. Check the Replace the original calling party number with the SNR extension number in the caller ID display of the remote phone check box to display the SNR number in the destination phone's caller ID.

j. Click the **Call Restrictions** tab in the Create Extension dialog box.

   The Call Restrictions area is displayed.

k. Choose the incoming and outgoing permissions from the drop-down lists.

l. Enter the value for call forward max length.

m. Check the Deny forwarding of calls from an internal extension to outside number to prevent forwarding of unauthorized calls.

n. Click the **Night-service Bell** tab in the Create Extension dialog box.

   The Night-service Bell area is displayed.

o. Check the Enable night-service checkbox.

   The Allow night-service phones to pickup call radio button is selected by default when night service is enabled. Click the Automatically forward calls to designated number radio button to enable it and enter the number calls should be forwarded to.

p. Click the **Hunt Settings** tab in the Create Extension dialog box.

   The Hunt Settings area is displayed.

q. Check the Disallow incoming calls to rollover (hunt) to another extension check box or the Allow incoming calls to hunt to another channel check box.

r. Click the **Hold Alert** tab in the Create Extension dialog box.

   The Hold Alert area is displayed.

s. Choose when to activate alert from the drop-down list.

t. Enter seconds after which alert is to be repeated.

u. Click the **Extension Preference** tab in the Create Extension dialog box.

   The Extension Preference area is displayed.

v. Choose the primary and secondary numbers from the drop-down lists.

w. Click the **Watch Mode Settings** tab in the Create Extension dialog box.

   The Watch Mode Settings area is displayed.

x. Check the Allow the status of this extension to be watched check box to enable monitoring of the phone.

y. Click **OK** to apply your changes or **Cancel** to discard them.

The Deliver Configuration to Device dialog box is displayed.

z. Click **Deliver** or **Cancel**.

Step 3 To edit an extension, do the following:

a. Choose an extension row parameter to modify, and click **Edit**. The Edit Extension dialog box opens.

b. See steps b. to z. under Creating, Editing, Deleting, and Cloning Extensions, page 56-4

Step 4 To delete extensions, do the following:

a. Choose an extension row or multiple rows to delete, and click **Delete**. A confirmation dialog box opens.

b. Click **Yes** in the confirmation dialog box.

Step 5 To edit all extensions:

a. Click **Edit All**. The Edit All Extensions dialog box opens.

b. To modify values, select an extension row and make the required changes in-line for Primary Number, Secondary Number, Label, Call Forward Busy, Call Forward No Answer, Call Forward No Answer Timeout.

c. To add a new extension, click **Add**. Extension Type, Primary Number, and Line Mode are mandatory fields.

d. To delete an extension, select it and click **Delete**.

e. Click **OK**.

Step 6 To duplicate an extension, do the following:

a. Choose an extension row to duplicate, and click **Clone**. The Create Extension dialog box opens, which contains all of the settings of the source extension.

b. Enter the primary number, make changes to the configuration, and click **OK**.

Related Topics

- Extensions, page 56-2
- Extensions Reference, page 56-7
- User, Phones, and Extensions Basic Workflow, page 56-1

- Importing Bulk Data, page 55-1

Extensions Reference

This section describes the pages and dialog boxes you can use when working with extensions and includes the following topics:

- Extensions Summary Page, page 56-7
- Create or Edit Extension Dialog Box, page 56-12

Extensions Summary Page

Use the Extensions summary page to view the extensions that are configured, to create new extensions, modify parameters of a selected extension, delete selected extensions, edit certain parameters of selected extensions quickly, and to clone extensions.

How to Get to This Page

Click **Configure > Unified Communications > Users, Phones, and Extensions > Extensions**.

Related Topics

- Create or Edit Extension Dialog Box, page 56-12
- Creating, Editing, Deleting, and Cloning Extensions, page 56-4
- Extensions, page 56-2
- User, Phones, and Extensions Basic Workflow, page 56-1
- Importing Bulk Data, page 55-1

Field Reference

Table 56-1 Extensions Summary Page

Element	Description
Extension Tag	Number of the extension in the list. Example 1, 2, and so on.
Extension Type	Type of the extension. Example SCCP or SIP.
Primary Number	Primary number of the extension.
Label	Text string that identifies the extension.
User	Name associated with the extension number. **Note** If an extension is associated with more than one user and the line type chosen is Regular, the user name Shared is displayed in this field.
Line Mode	This column can contain the following values: • SINGLE—Single-line mode. A single voice channel per directory number is allowed. • DUAL—Dual-line mode. Two voice channels per directory number are allowed. • OCTO—Octo-line mode. Eight voice channels per directory number are allowed. This option is available when the router uses Cisco Unified CME 4.3 or later.
Call Forward Busy	Call forward number Numbers that can dialed or the voice mail number.
Call Forward No Answer	Call forward number Numbers that can dialed or the voice mail number.
Create button	The Create button opens the Create Extensions dialog box to enter the information required for the extension. See Create or Edit Extension Dialog Box, page 56-12.
Edit button	The Edit button opens the Edit Extensions dialog box to modify the parameters of the selected extension. See Create or Edit Extension Dialog Box, page 56-12.

Table 56-1 Extensions Summary Page (continued)

Element	Description
Delete button	The Delete button removes the selected extension. If the deleted extension is associated with a user, a phone restart confirmation box is displayed. To restart the phone, click **Yes**, otherwise, click **No**.
Edit All button	The Edit All button opens the Edit All Extensions dialog box to quickly modify certain parameters of all extensions, add, and delete extensions. See Edit All Extensions Dialog Box, page 56-9.
Clone button	The Clone button creates a new extension with the settings of an existing extension.
Guided Configuration pane	
Download link	Click the Download link to download and save the Bulk Import CSV template. See "Downloading the .CSV Template" section on page 55-6.
Launch Wizard button	Click the button to open the Bulk Import wizard. See "Import Bulk Data Screen Reference" section on page 55-10.

Edit All Extensions Dialog Box

Use the Edit All Extensions dialog box to quickly modify certain parameters for all extensions, add new extensions fast with only the mandatory parameters configured, and delete extensions.

How to Get to This Dialog Box

- Choose **Configure > Unified Communications > Users, Phones, and Extensions > Extensions > Edit All**.

Related Topics

- Extensions Summary Page, page 56-7
- Creating, Editing, Deleting, and Cloning Extensions, page 56-4
- Extensions, page 56-2

Field Reference

Table 56-2 lists the fields in the Edit All Extensions Dialog Box.

Table 56-2 Edit All Extensions Dialog Box

Element	Description
Extension Type	View the extension types for all the configured extensions. If adding a new extension, choose SCCP or SIP from the drop-down list. **Note** This is a mandatory field if you are adding a new extension.
Primary Number	View the primary numbers for all the configured extensions. To modify the primary number, select an extension and click in the primary number column. If adding a new extension, enter the primary number for the extension. **Note** This is a mandatory field if you are adding a new extension.
Secondary Number	View the secondary numbers for all the configured extensions. To modify the secondary number, select an extension and click in the secondary number column. If adding a new extension, enter the secondary number for the extension.
Label	View the labels for all the configured extensions. To modify the label, select an extension and click in the label column. If adding a new extension, enter the label for the extension.
User	View the users for all the configured extensions.

Table 56-2 Edit All Extensions Dialog Box

Element	Description
Line Mode	View the line modes for all the configured extensions. If adding a new extension, choose the line mode from the drop-down list. **Note** This is a mandatory field if you are adding a new extension.
Call Forward Busy	View the call forward number. To modify the value, select an extension and click in the Call Forward Busy column. If adding a new extension, enter the value for Call Forward Busy.
Call Forward No Answer	View the call forward number. To modify the value, select an extension and click in the Call Forward No Answer column. If adding a new extension, enter the value for Call Forward No Answer.
Call Forward No Answer Timeout	View the timeout value for call forward no answer. To modify the value, select an extension and click in the Call Forward No Answer Timeout column. If adding a new extension, enter the value for Call Forward No Answer Timeout.
Add button	Click to add a new extension. A new row appears at the end of the list. Choose or enter in-line the required formation for each column, except User. **Note** Extension Type, Primary Number, and Line Mode are mandatory fields.
Delete button	Select an extension and click to delete.

Table 56-2 Edit All Extensions Dialog Box

Element	Description
OK button	Click to display the Deliver Configuration to Device dialog box.
Cancel button	Click to discard your changes.

Create or Edit Extension Dialog Box

Use the Create or Edit Extension dialog box to create or edit an extension. This dialog box contains eight tabs: General, Single Number Reach, Call Restrictions, Night-service Bell, Hunt Settings, Hold Alert, Extension Preferences, and Watch Mode Settings. See the following topic:

- Create or Edit Extension Dialog Box, page 56-12

How to Get to This Dialog Box

- Choose **Configure > Unified Communications > Users, Phones, and Extensions > Extensions > Create**.
- Choose **Configure > Unified Communications > Users, Phones, and Extensions > Extensions > Edit**.

Create or Edit Extension Dialog Box

Use the Create Extension or Edit Extension dialog box to enter parameters for the extension.

Note To configure SIP extension, enable local SIP Registrar Server from **Unified Communications > VoIP Settings**.

How to Get to This Dialog Box

- Choose **Configure > Unified Communications > Users, Phones, and Extensions > Extensions > Create > Create Extension**.
- Choose **Configure > Unified Communications > Users, Phones, and Extensions > Extensions > Edit > Edit Extension**.

Related Topics

- Extensions Summary Page, page 56-7
- Creating, Editing, Deleting, and Cloning Extensions, page 56-4
- Extensions, page 56-2

Field Reference

Table 56-3 lists the fields in the Create or Edit Extension Dialog Box.

Table 56-3 Create or Edit Extension Dialog Boxes

Element	Description
General tab	
General pane	
Extension Type	Click the SCCP radio button or the SIP radio button. **Note** This is a mandatory field.
Primary Number field	The primary extension number. The primary extension number creates a number, and by default, assigns the number with dual-line mode. To change the line mode, use the Line Mode field. **Note** This is a mandatory field.
Secondary Number field	The secondary extension number. **Note** This field is not available with the SIP extension type.
Name to Be Displayed on Phone Line field	The name to be displayed on the phone that receives the call.
Description field	The text string that identifies the extension. **Note** This field is not available with the SIP extension type.

Table 56-3 Create or Edit Extension Dialog Boxes

Element	Description
Line Mode/Simultaneous Number of Active Calls allowed on a Phone Button drop-down list	Choose one of the following options from the drop-down list. These options are disabled when you edit an extension. • Dual-line—In dual-line mode, two voice channels are associated with the directory number. A user can make two call connections at the same time by using one phone line button. A dual-line extension is required if the user is using dual-line functions, such as hold, transfer, and conference. A dual-line directory number is shared exclusively among phones. After a call is answered, that phone owns both channels of the dual-line directory number. • Single-line—In single-line mode, a user makes one call connection at a time by using one phone line button. • Octo-line—In octo-line mode, available with Cisco Unified CME 4.3 or later versions, eight voice channels are associated with the directory number. An octo-line directory number can split its channels among other phones that share the directory number. All phones are allowed to initiate or receive calls on the idle channels of the shared octo-line directory number. **Note** If you try to configure octo-line mode for a Cisco Unified IP Phone 7902, 7920, or 7931, or an analog phone connected to a Cisco VG224 or Cisco ATA device, an error message is displayed. **Note** This field is not available with the SIP extension type.
E.164 Registration drop-down list	E.164 is a Telecommunication Standardization Sector (ITU-T) recommendation that defines the international public telecommunication numbering plan used in the PSTN and some other data networks. It also defines the format of telephone numbers. Choose a registration option from the drop-down list. The options are: Register Both Numbers, Do Not Register Any Number, Register Secondary Number, and Register Primary Number. The default option is Register Both Numbers. **Note** This field is not available with the SIP extension type.

Table 56-3 Create or Edit Extension Dialog Boxes

Element	Description
Block Caller ID for Calls from this Extension check box	Check this check box if you do not want the name of the caller to be displayed on calls that are sent from this particular extension. **Note** This field is not available with the SIP extension type.
Call Forwarding pane	The incoming calls are diverted to a specified number when the dialed number is busy or is not answered. • Forward All Calls To field—Enter the number to which all the incoming calls are forwarded. • When Busy, Divert Calls To field—The number to which all the incoming calls are forwarded when the dialed number is busy. • Divert Unattended Calls To—The number to which all the incoming calls are forwarded when the dialed number is not answered. • No Answer Timeout—The number of seconds the call is unanswered before it is forwarded. Range is from 3 to 60,000.
Single Number Reach tab	Click this tab in the Create/Edit Extension dialog box. **Note** This tab is not available with the SIP extension type.

Table 56-3 Create or Edit Extension Dialog Boxes

Element	Description
Single Number Reach tab (continued)	**Note** The SNR feature is supported on routers running Cisco Unified CME 7.1 and later versions. If the Cisco Unified CME version is earlier than 7.1, the SNR feature is not displayed. Users can answer incoming calls on their desktop IP phone or at a remote destination, such as a mobile phone, and can pick up in-progress calls on the desktop phone or the remote phone without losing the connection. This allows callers to use a single number to reach the phone user. Calls that are not answered can be forwarded to voice mail. • Enable SNR for this extension check box—Check this check box to enable SNR. SNR can be enabled only if Mobility exits in the ephone-dn. When you enable or disable SNR, the Mobility check box is automatically enabled or disabled. • Remote Number field—Enter the number of the remote destination device. Range is from 1 to 15 digits. Remote destinations can include the following devices: – Mobile (cellular) phones. – Smart phones. – IP phones that do not belong to the same Cisco Unified CME router as the desktop phone. – Home phone numbers in the PSTN. Supported PSTN interfaces include PRI, BRI, SIP, and FXO. **Note** This field is active when SNR is enabled.
Single Number Reach tab (continued)	• Ring Remote Number After field—Enter the number of seconds that the call rings the IP phone before ringing the remote phone. Range is from 0 to 10. **Note** This field is active when SNR is enabled.

Table 56-3 Create or Edit Extension Dialog Boxes

Element	Description
Single Number Reach tab (continued)	• Time Out field—Enter the number of seconds that the call rings after the configured delay. Call continues to ring for the configured length of time on the IP phone even if the remote phone answers the call. Range is from 5 to 60. **Note** This field is active when SNR is enabled. • Forward Unanswered Calls To field—Enter the number to which the call is forwarded if the user does not answer. The call is forwarded to a voice mail number if the user does not answer. Range is from 1 to 15 digits. **Note** This field is active when SNR is enabled. • Enable mobility feature for this extension number check box—Check this check box to enable the Mobility feature on the directory number. The Mobility feature allows you to manage calls using a single number and to transfer calls that are in progress between the desktop phone and the remote destination, for example a mobile phone. When you enable or disable SNR, the Mobility check box is enabled or disabled accordingly. **Note** You can also use the IP phone soft keys to enable or disable Mobility.
Single Number Reach tab (continued)	• Replace the original calling party number with the SNR extension number in the caller ID display of the remote phone check box—Check this check box to display the SNR number in the destination phone's caller-ID. **Note** This field is active when SNR is enabled.
Call Restrictions tab	Click this tab in the Create/Edit Extension dialog box. **Note** This tab is not available with the SIP extension type.

Table 56-3 Create or Edit Extension Dialog Boxes

Element	Description
Call Restrictions tab (continued)	The call restrictions configured on the extension number. To configure calling restrictions, choose **Configure > Dial Plans > Calling Restrictions**. • Incoming Permissions drop-down list—Choose a calling restriction from the list. • Outgoing Permissions drop-down list—Choose a calling restriction from the list. Valid calling restrictions are: • Internal—Can place outgoing calls by dialing internal and emergency numbers only. Restricted from placing all other calls. • Local—Can place outgoing calls by dialing local, internal, and emergency numbers only. Restricted from placing domestic, long distance, and international calls. • Domestic—Can place outgoing calls by dialing internal, emergency, local, domestic, and long distance numbers only. Restricted from placing international calls. • International—Can place outgoing calls by dialing internal, local, domestic, long distance, and international numbers. • No Restrictions—No access limits. **Note** The Internal, Local, Domestic, and International permission options are available from the drop-down list if you have configured Dialing Restrictions, otherwise, only the No Restrictions option is available. • Call forward max length field—Enter the maximum number of digits that can be entered using the CfwdALL key on an IP phone. • Deny forwarding of calls from an internal extension to outside number check box—Check this check box to prevent forwarding of internal calls to outside numbers.

Table 56-3 Create or Edit Extension Dialog Boxes

Element	Description
Night-service Bell tab	Click this tab in the Create/Edit Extension dialog box. **Note** This tab is not available with the SIP extension type.
Night-service Bell tab (continued)	The calls are forwarded from extensions that are unstaffed during night service hours to another designated phone. You can either configure the night service phone to pick up the calls, or you can forward the calls to a designated number. Before you configure the Night Service Bell feature, you must configure the Night Service schedule. To configure the Night Service schedule, choose **Configure > Unified Communications > Telephony Features > Night Service Bell**. • Enable night-service check box—Check this check box to enable night service. • Allow night-service Phones to Pickup Call radio button—Choose this radio button to have the night service phone pick up the calls. • Automatically Forward Calls To Designated Number radio button—Choose this button to forward the calls to a designated number, and then enter the number in the Forward Call to Number field. • Forward Call to Number—The number to which the night service call is forwarded. For example, you can forward the calls that are sent to the daytime receptionist to an employee who is working the night shift. This field is displayed when you choose the Automatically Forward Calls to Designated radio button.
Hunt Settings tab	Click this tab in the Create/Edit Extension dialog box.

Table 56-3 Create or Edit Extension Dialog Boxes

Element	Description
Hunt Settings tab (continued)	The incoming call is rolled over to another extension when the extension to which the call is sent is busy or is not answered. • Disallow Incoming Call to Rollover (Hunt) to Another Extension check box—Check this check box to disallow the incoming call to rollover to another extension when the extension to which the call is sent is busy or is not answered. • Allow Incoming Call to Rollover (Hunt) to Another Channel check box—Check this check box to allow the incoming call to rollover to another channel when the extension to which the call is sent is busy or is not answered. If you have chosen the line mode as Octo in the General tab, and you have checked the Allow Incoming Call to Rollover (Hunt) to Another Channel check box, you must specify the channel number. Choose a channel number from the drop-down list. Range is from 1 to 8. **Note** This field is not available with the SIP extension type.
Hold Alert tab	Click this tab in the Create/Edit Extension dialog box. An audible alert notification that starts when the call is on-hold, and repeats after a specified time interval. • Activate Alert When drop-down list—The situation when the audible alert notification must start. The options are: idle, shared, shared-idle, and idle or busy. • Repeat Alert After a Gap of field—The number of seconds after which the audible alert sound repeats. Range is from 15 to 300. **Note** This tab is not available with the SIP extension type.

Table 56-3 Create or Edit Extension Dialog Boxes

Element	Description
Extension Preference tab	Click this tab in the Create/Edit Extension dialog box. The order of preference in which the phone line is chosen when multiple lines have the same extension number. • For Primary Number drop-down list—Enter the preference in which the primary number is chosen when multiple lines have the same extension number. Options are from 0 to 9. **Note** This field is applicable for SIP extensions. • For Secondary Number drop-down list—Enter the preference in which the secondary number is chosen when multiple lines have the same extension number. Options are from 1 to 9. **Note** This field is not available with the SIP extension type.
Watch Mode Settings tab	Click this tab in the Create/Edit Extension dialog box. The phone user, such as a receptionist, can visually monitor the in-use status of an individual extension. **Note** The Watch Mode Settings feature is supported on routers running Cisco Unified CME 4.1 and later versions. Allow the Status of this Extension to be Watched check box—Check this check box to allow the phone user to monitor the in-use (idle or busy) status of the extension.
OK button	Click this button to apply the extension configuration to the router.
Cancel button	Click this button to discard the configuration values that you entered.

Phones and Users Settings

A phone or Ethernet phone is the physical instrument with which a user can make and receive calls in a Cisco Unified Call Manager Express (Cisco Unified CME) system. The physical instrument is either a Cisco Unified IP phone or an analog

phone. The maximum number of phones per system is platform, version, and license dependent and is listed in *Cisco Unified CME and Cisco IOS Software Version Compatibility Matrix,* which can be found at Cisco.com.

You can configure user settings by defining a user, and then associating a phone, extensions, and optionally a mailbox to that user. You can also configure speed dial for the selected user phone.

To configure user settings, choose **Configure > Unified Communications > Users, Phones and Extensions > Phones and Users**. The Phones and Users summary page opens. From the Phones and Users summary page, you can view configured user information, create new users, edit user information, delete a user, and reset or restart phones.

See the following topics for more information:

- Phones and Users Settings, page 56-21
- Configuring Line Types, page 56-26
- Phones and Users Reference, page 56-35
- Importing Bulk Data, page 55-1

Creating, Editing, Deleting, Restarting, and Resetting Phones and Users

Procedure

Use this procedure to set up a new phone or user, modify parameters of a selected phone or user, delete a user, and reset or restart selected phones.

Note Before you begin, make sure you have configured extensions. See Create or Edit Extension Dialog Box, page 56-12.

Step 1 Choose **Configure > Unified Communications > Users, Phones, and Extensions > Phones and Users.** The Phones and Users summary page opens. See Phones and Users Settings, page 56-21.

Step 2 To set up a new phone or user:

a. Click **Create**. The Create Phone/User dialog box opens with the **Phone** tab.

b. Choose the phone type and phone model. Enter the MAC address of the phone and choose the router port to which the phone is connected. Choose auto-line selection, associate extensions, choose phone line type, and ring type. See Create or Edit Phone/User—Phone Tab, page 56-42.

Note Router port connection and auto-line selection are not available for SIP phones.

c. Click the **User** tab. Enter the user ID, first name, last name, display name, password, and Personal Identification Number (PIN). See Create or Edit Phone/User—User Tab, page 56-47.

Note PIN is not available for SIP phone type.

d. Click the **Mailbox** tab. Enable dial-by-name, add voice mailbox and enter information for mailbox user credentials and mailbox configuration. Create or Edit Phone/User—Mailbox Tab, page 56-50.

e. Click the **Phone Settings** tab. Enable night-service, remote worker, and configure speed-dial. See Create or Edit Phone/User—Phone Settings Tab, page 56-54

Note Allowing the phone to make blocked calls during after-hours is not available for SIP phone type.

f. Click **OK**.

Step 3 To edit phones or users settings:

a. Choose a user row with information to edit, and click **Edit**. The Edit Phone/User dialog box opens with the **Phone** tab. See Create or Edit Phone/User Dialog Box, page 56-41.

b. Change the required parameters in the **Phone** tab. See Create or Edit Phone/User—Phone Tab, page 56-42

c. Click the **User** tab, and change the required parameters. See Create or Edit Phone/User—User Tab, page 56-47.

d. Click the **Mailbox** tab, and change the required parameters. See Create or Edit Phone/User—Mailbox Tab, page 56-50.

e. Click the **Phone Settings** tab, and change the required parameters. See Create or Edit Phone/User—Phone Settings Tab, page 56-54.

f. Click **OK**.

Step 4 To delete phones or user settings:

a. Choose a row or multiple rows to delete, and click **Delete**. A confirmation dialog box opens.

b. Click **Yes** in the confirmation dialog box to delete the user or users.

Step 5 To edit all phones or user settings:

a. Click **Edit All**. The Edit All Users/Phones dialog box opens.

b. To modify values, select a phone row and make the required changes in-line for Extension on Phone Line #1, user ID, password, first name, and last name.

c. To add a new phone or user, click **Add**. Phone model and MAC address are mandatory fields.

d. To delete a phone or user, select a phone row and click **Delete**.

e. Click **OK**.

Step 6 For the configuration changes to be effective, you must reboot the Cisco Unified IP phones after you have made changes to the configuration. When the phone reboots, the configuration is downloaded on the phone. You can reboot a single phone or you can reboot all the phones in a Cisco Unified CME system by clicking the Restart or Reset button.

- Restart—To quickly reboot the phones, choose the phone row or rows, and click **Restart**. A confirmation dialog box opens. Click **Yes** in the confirmation dialog box.
- Reset—To power off and then power on (reboot) the phones, choose the phone row or rows, and click **Reset**. A confirmation dialog box opens. Click **Yes** in the confirmation dialog box.

Note You can choose either the Restart or the Reset button to reboot phones. If you are rebooting multiple phones, the Restart option is faster than the Reset option.

Related Topics

- Phones and Users Settings, page 56-21

- Phones and Users Reference, page 56-25
- User, Phones, and Extensions Basic Workflow, page 56-1
- Configuring Line Types, page 56-26
- Importing Bulk Data, page 55-1

Phones and Users Reference

This section describes the pages and dialog boxes you can use when working with phones and includes the following topics:

- Phones and Users Settings, page 56-21
- Create or Edit Phone/User Dialog Box, page 56-41

Configuring Line Types

This section contains the following topics:

- Creating a Regular Line, page 56-26
- Creating a Shared Extension, page 56-27
- Creating a Monitor Line, page 56-30
- Creating an Overlay or Call Waiting on Overlay Line, page 56-31
- Changing an Overlay Line to Monitor or Regular Line, page 56-33
- Creating a Watch Line, page 56-34

Creating a Regular Line

A regular line is assigned to one user. When you choose the Regular line type option, you can choose one of the following ring behaviors: normal, feature, beep or silent.

Before You Begin

- Make sure you have configured extensions. See Create or Edit Extension Dialog Box, page 56-12.

Procedure

Use this procedure to create a regular line.

Step 1 Choose **Configure > Unified Communications > Users, Phones, and Extensions > Phones and Users**. The Phones and Users summary page opens. See Phones and Users Summary Page, page 56-36.

Step 2 Click **Create**. The Create Phone/User dialog box opens with the **Phone** tab. See Create or Edit Phone/User Dialog Box, page 56-41.

Step 3 Do the following

a. From the Phone Type field, choose SIP or SCCP.

b. From the Phone Model field, choose the phone to configure.

c. In the MAC address field, enter the MAC address of the phone.

d. From the Extensions pane, assign one of the available extensions to a phone. Do the following:

   Choose an extension from the Available Extensions pane, and click the **>** arrow button or use the drag and drop feature to move it to the Selected Extensions pane. Information about that extension is displayed in the left pane.

e. From the Line Type field, choose the line type as **Regular**.

f. From the Ring Type field, choose the ring type to use.

g. Click **OK**.

   See Create or Edit Phone/User—Phone Tab, page 56-42.

Related Topics

- Creating, Editing, Deleting, Restarting, and Resetting Phones and Users, page 56-22
- Configuring Line Types, page 56-26

Creating a Shared Extension

An extension that is shared by more than one user with the line type as Regular is called a *shared extension*.

A shared extension has the following characteristics:

- Appears on two different phones but uses the same ephone-dn and number.
- Can make one call at a time and that call appears on both phones.
- Should be used when you want the capability to answer or pick up a call at more than one phone.

Because these phones share the same ephone-dn, if the ephone-dn is connected to a call on one phone, that ephone-dn is unavailable for other calls on the second phone. If a call is placed on hold on one phone, it can be retrieved on the second phone. This is like having a single-line phone in your house with multiple extensions. You can answer the call from any phone on which the number appears, and you can pick it up from hold on any phone on which the number appears.

Before You Begin

- Make sure you have configured extensions. See Create or Edit Extension Dialog Box, page 56-12.
- Make sure you have configured phones. See Create or Edit Phone/User Dialog Box, page 56-41.

Procedure

Use this procedure to create a shared line between two users.

Step 1 Choose **Configure > Unified Communications > Users, Phones, and Extensions > Phones and Users**. The Phones and Users summary page opens. See Phones and Users Summary Page, page 56-36.

Step 2 Click **Create**. The Create Phone/User dialog box opens with the **Phone** tab. See Create or Edit Phone/User Dialog Box, page 56-41.

Step 3 Click the **User** tab, and enter a username (for example, user1), password, PIN, and other parameters. See Create or Edit Phone/User—User Tab, page 56-47

Step 4 Click the **Phone** tab. Do the following:

a. From the Phone Type field, choose SIP or SCCP.

b. From the Phone Model field, choose the phone to configure.

c. In the MAC address field, enter the MAC address of the phone.

d. From the Extensions pane, assign one of the available extensions (for example, extension 1000) to a phone button. Do the following:

   In this example, choose extension 1000 from the Available Extensions pane, and then click the **>** arrow button or use the drag and drop feature to move it to the Selected Extensions pane. Information about that extension is displayed in the left pane.

e. From the Line Type field, choose the line type as **Regular**.

f. From the Ring Type field, choose the ring type to use.

g. Click **OK**.

Step 5 Click the **User** tab, and enter another username (for example, user2), password, PIN, and other parameters. See Create or Edit Phone/User—User Tab, page 56-47.

Step 6 Click the **Phone** tab and do the following:

a. From the Phone Type field, choose SIP or SCCP.

b. From the Phone Model field, choose the phone to configure.

c. In the MAC address field, enter the MAC address of the phone.

d. From the Extensions pane, assign the same extension that you assigned to the first user your created (in this example, extension 1000) to a phone button.

e. From the Line Type field, choose the line type as **Regular**.

f. From the Ring Type field, choose the ring type to use.

g. Click **OK**.

   See Create or Edit Phone/User—Phone Tab, page 56-42.

Both users (user1 and user2) now share the same extension (1000). Note that in the Available Extensions and Selected Extensions pane this extension displays Shared in parenthesis; for example, 1000 (Shared). Also, in the Extensions summary page, the username Shared is displayed for the shared extension (1000).

Related Topics

- Creating, Editing, Deleting, Restarting, and Resetting Phones and Users, page 56-22
- Configuring Line Types, page 56-26
- Importing Bulk Data, page 55-1

Creating a Monitor Line

A monitor line is a line that is shared by two people. Only one person can make and receive calls on the shared line at a time, while the other person, whose line is in monitor mode, is able to see that the line is in use.

Before You Begin

- Make sure you have configured extensions. See Create or Edit Extension Dialog Box, page 56-12.
- Make sure you have configured phones. See Create or Edit Phone/User Dialog Box, page 56-41.

Procedure

Use this procedure to create a monitor line.

Step 1 Choose **Configure > Unified Communications > Users, Phones, and Extensions > Phones and Users**. The Phones and Users summary page opens. See Phones and Users Summary Page, page 56-36.

Step 2 Click **Create**. The Create Phone/User dialog box opens with the **Phone** tab. See Create or Edit Phone/User Dialog Box, page 56-41.

Step 3 Click the **User** tab, and enter the username, password, PIN, and other parameters. See Create or Edit Phone/User—User Tab, page 56-47.

Step 4 Click the **Phones** tab and do the following:

a. From the Phone Type field, choose SIP or SCCP.

b. From the Phone Model field, choose the phone to configure.

c. In the MAC address field, enter the MAC address of the phone.

d. From the Extensions pane, assign one of the available extensions to the phone. Do the following:

   Choose an extension from the Available Extensions pane, and click the **>** arrow button or use the drag and drop feature to move it to the Selected Extensions pane. Information about that extension is displayed in the left pane.

e. From the Line Type field, choose **Monitor**.

f. Click **OK**.

   See Create or Edit Phone/User—Phone Tab, page 56-42.

Related Topics

- Creating, Editing, Deleting, Restarting, and Resetting Phones and Users, page 56-22
- Configuring Line Types, page 56-26
- Importing Bulk Data, page 55-1

Creating an Overlay or Call Waiting on Overlay Line

Overlaid ephone-dns are directory numbers that share the same button on a phone. Overlaid ephone-dns can be used to receive incoming calls and place outgoing calls. Up to 25 ephone-dns can be assigned to a single phone button. They can have the same extension number or different numbers. The same ephone-dns can appear on more than one phone, and more than one phone can have the same set of overlaid ephone-dns.

Call waiting on an overlay line allows phone users to know that another person is calling them while they are talking on the phone. Phone users hear a call-waiting tone indicating that another party is trying to reach them. When phone users

answer a call-waiting call, their original call is automatically put on hold. If phone users ignore a call-waiting call, the caller is forwarded if call-forward no-answer has been configured.

Before You Begin

- Make sure you have configured extensions. See Create or Edit Extension Dialog Box, page 56-12.
- Make sure you have configured phones. See Create or Edit Phone/User Dialog Box, page 56-41.

Procedure

Use this procedure to create an overlay or a call waiting on overlay line.

Step 1 Choose **Configure > Unified Communications > Users, Phones, and Extensions > Phones and Users**. The Phones and Users summary page opens. See Phones and Users Summary Page, page 56-36.

Step 2 Click **Create**. The Create Phone/User dialog box opens with the **Phone** tab. See Create or Edit Phone/User Dialog Box, page 56-41.

Step 3 Click the **User** tab, and enter the username, password, PIN, and other parameters. See , page 56-48.

Step 4 Click the **Phones/Extensions** tab, and then do the following:

a. From the Phone Type field, choose SIP or SCCP.

b. From the Phone Model field, choose the phone to configure.

c. In the MAC address field, enter the MAC address of the phone.

d. From the Extensions pane, assign two or more available extensions to any of the phone buttons. Do the following:

   Choose the extensions from the Available Extensions pane, and click the **>>** arrow button or use the drag and drop feature to move them to the Selected Extensions pane. Information about the chosen extensions is displayed in the left pane.

e. From the Line Type field, choose **Overlay** or **Call Waiting on Overlay**.

f. Click **OK**.

See Create or Edit Phone/User—Phone Tab, page 56-42.

Related Topics

- Creating, Editing, Deleting, Restarting, and Resetting Phones and Users, page 56-22
- Configuring Line Types, page 56-26
- Importing Bulk Data, page 55-1

Changing an Overlay Line to Monitor or Regular Line

Before You Begin

- Make sure you have created the overlay line. See Creating an Overlay or Call Waiting on Overlay Line, page 56-31.

Procedure

Use this procedure to change the overlay line to a monitor or regular line.

Step 1 Choose **Configure > Unified Communications > Users, Phones, and Extensions > Phones and Users**. The Phones and Users summary page opens. See Phones and Users Summary Page, page 56-36.

Step 2 Click **Edit**. The Edit Phone/User dialog box opens with the **Phone** tab. See Create or Edit Phone/User Dialog Box, page 56-41.

Step 3 Do the following:

a. From the Phone Model field, choose the phone with information to modify.

b. From the Line field, choose the phone line that was assigned as Overlay or Call Waiting on Overlay.

c. From the Line Type field, choose the line type as **Regular or Monitor** from the drop-down list. All of the extensions that were in the Selected Extensions pane (which you had originally selected for overlay), move to the Available Extensions pane.

d. From the Extensions pane, assign one of the available extensions to the phone. Do the following:

Choose an extension from the Available Extensions pane, and click the > arrow button or use the drag and drop feature to move it to the Selected Extensions pane. Information about that extension is displayed in the left pane.

e. Click **OK**.

See Create or Edit Phone/User—Phone Tab, page 56-42.

Related Topics

- Creating, Editing, Deleting, and Cloning Extensions, page 56-4
- Configuring Line Types, page 56-26
- Importing Bulk Data, page 55-1

Creating a Watch Line

When you configure a watch line, you allow the phone user, such as a receptionist, to visually monitor the in-use status of an individual extension.

Note The Watch Mode Settings feature is supported on routers running Cisco Unified CME 4.1 and later versions.

Before You Begin

- Make sure you have configured extensions and have enabled watch mode for that extension. See Create or Edit Extension Dialog Box, page 56-12.
- Make sure you have configured phones. See Create or Edit Phone/User Dialog Box, page 56-41.

Procedure

Use this procedure to create watch line.

Step 1 Choose **Configure > Unified Communications > Users, Phones, and Extensions > Phones and Users**. The Phones and Users summary page opens. See Phones and Users Summary Page, page 56-36.

Step 2 Click **Create**. The Create Phone/User dialog box opens with the **Phone** tab. See Create or Edit Phone/User Dialog Box, page 56-41.

Step 3 Click the **User** tab, and enter the username, password, PIN, and other parameters. See Create or Edit Phone/User—User Tab, page 56-47.

Step 4 Click the **Phones** tab and do the following:

a. From the Phone Type field, choose SIP or SCCP.

b. From the Phone Model field, choose the phone to configure.

c. In the MAC address field, enter the MAC address of the phone.

d. From the Line field, choose the phone line to use. You can also choose a phone line by clicking on a line in the table below.

e. From the Line Type field, choose **Watch**.

f. From the Extensions pane, assign one of the available extensions to the phone. Do the following:

   Choose an extension from the Available Extensions pane, and click the **>** arrow button or use the drag and drop feature to move it to the Selected Extensions pane. Information about that extension is displayed in the left pane.

g. Click **OK**.

   See Create or Edit Phone/User—Phone Tab, page 56-42.

Related Topics

- Creating, Editing, Deleting, Restarting, and Resetting Phones and Users, page 56-22
- Configuring Line Types, page 56-26

Phones and Users Reference

This section describes the pages and dialog boxes you can use when working with Phones and Users and includes the following topics:

- Phones and Users Summary Page, page 56-36
- Create or Edit Phone/User Dialog Box, page 56-41

Phones and Users Summary Page

Use the Phones and Users summary page to view phones or users that are configured, setup a new phone or user, modify parameters of a selected phone or user, modify certain parameters of all phones or users through the Edit All button, delete phones or users and to reset or restart selected phones.

How to get to this page

Choose **Configure > Unified Communications > Users, Phones, and Extensions > Phones and Users**.

Related Links

- Create or Edit Phone/User Dialog Box, page 56-41
- Creating, Editing, Deleting, Restarting, and Resetting Phones and Users, page 56-22
- Configuring Line Types, page 56-26
- User, Phones, and Extensions Basic Workflow, page 56-1
- Importing Bulk Data, page 55-1

Field Reference

Table 56-4 Phones and Users

Element	Description
Phone Tag	*Display only.* Number of the phone in the list. Example 1, 2, and so on.
Phone Type	*Display only.* Type of the phone. Example SCCP or SIP.
Phone Model	*Display only.* Model of the phone assigned to the user. Example 6901.
MAC Address	*Display only.* MAC address (hardware address) of the phone assigned to the user.
Extensions	*Display only.* Extensions configured for a user.
User ID	*Display only.* ID of the user.

Table 56-4 Phones and Users

Element	Description
First Name	*Display only.* First name of the user.
Last Name	*Display only.* Last name of the user.
Mailbox	*Display only.* Displays **Yes** if there is a mailbox associated with the user, otherwise, displays **No**.
Create button	Button to open the Create Phone/User dialog box where you can create new phones or users. See Create or Edit Phone/User Dialog Box, page 56-41.
Edit button	Button to open the Edit Phone/User dialog box where you can modify the parameters that are configured for a selected phone or user. See Create or Edit Phone/User Dialog Box, page 56-41.
Delete button	Button to delete a selected phone or user configuration. A confirmation dialog box opens. Click **Yes** in the confirmation dialog box to delete the selected user or users.
Edit All button	Button to open the Edit All Users/Phones dialog box where you can quickly modify certain parameters for all users or phones, add new users or phones fast with only the mandatory parameters configured, and delete phones or users. See Edit All Users/Phones Dialog Box, page 56-38.
Restart button	Button to quickly reboot the selected phone or phones. A confirmation dialog box opens. Click **Yes** in the confirmation dialog box to restart the selected phone. For the configuration changes to be effective, you must reboot the Cisco Unified IP phones after you have made changes to the configuration. When the phone reboots, the configuration is downloaded on the phone. You can reboot a single phone or you can reboot all the phones in a Cisco Unified CME system. **Note** You can choose either the Restart or the Reset button to reboot phones. If you are rebooting multiple phones, the Restart option is faster than the Reset option.

Table 56-4 Phones and Users

Element	Description
Reset button	Button to power off or power on (reboot) the selected phone or phones. A confirmation dialog box opens. Click **Yes** in the confirmation dialog box to reset the selected phone. For the configuration changes to be effective, you must reboot the Cisco Unified IP phones after you have made changes to the configuration. When the phone reboots, the configuration is downloaded on the phone. You can reboot a single phone or you can reboot all the phones in a Cisco Unified CME system. **Note** You can choose either the Restart or the Reset button to reboot phones. If you are rebooting multiple phones, the Reset option takes longer to process than the Restart option.
Guided Configuration pane	
Download link	Click the Download link to download and save the Bulk Import CSV template. See "Downloading the .CSV Template" section on page 55-6.
Launch Wizard button	Click the button to open the Bulk Import wizard. See "Import Bulk Data Screen Reference" section on page 55-10.

Edit All Users/Phones Dialog Box

Use the Edit All Users/Phones dialog box to quickly modify certain parameters for all users or phones, add new users or phones fast with only the mandatory parameters configured, and delete phones or users.

How to get to this page

Choose **Configure > Unified Communications > Users, Phones, and Extensions > Phones and Users > Edit All**.

Related Links

- Phones and Users Summary Page, page 56-36
- Create or Edit Phone/User Dialog Box, page 56-41

Field Reference

Table 56-5 Edit All Users/Phones Dialog Box

Element	Description
Phone Type	View the phone types of all the configured phones or users. If adding a new phone or user, choose SCCP or SIP from the drop-down list.
Phone Model	View the phone models for all the configured phones or users. If adding a new phone or user, choose the phone model from the drop-down list. This is a mandatory field.
MAC Address	View the MAC address of the phone. If adding a new phone or user, enter MAC address of the phone. This is a mandatory field.
Extension On Phone Line # 1	View extensions for all phones and users. To modify parameters, select the required phone or user, click in the Extension column and choose from the drop-down list. If adding a new phone or user, choose the required extension from the drop-down list.
User ID	View user IDs of all configured phones or users. To modify the user ID, select the required phone or user, click in the User ID column and make the changes in-line. If adding a new phone or user, enter user ID of the new user.
Password	To modify the password, select the required phone or user, click in the password column and make the changes in-line. If adding a new phone or user, enter password of the user.

Table 56-5 Edit All Users/Phones Dialog Box

Element	Description
First Name	View the first names of all configured users or phones. To modify the first name, select the required phone or user, click in the First Name column and make the required change in-line. If adding a new phone or user, enter first name of the user.
Last Name	View the last names of all configured users or phones. To modify the last name, select the required phone or user, click in the Last Name column and make the required change in-line. If adding a new phone or user, enter last name of the user.
Mailbox	*Display only.* Displays **Yes** if there is a mailbox associated with the user, otherwise, displays **No**. To add a mailbox, select the user and click the Edit button from the Phones and Users page.
Add button	Click to add a new user. A new row appears at the end of the list. Choose or enter in-line the required formation for each column, except Mailbox. **Note** Phone Model and MAC Address are mandatory fields.
Delete button	Select a user or phone and click to delete.
OK button	Click to display the Deliver Configuration to Device dialog box.
Cancel button	Click to discard your changes.

Create or Edit Phone/User Dialog Box

Use the Create or Edit Phone/User dialog box to set up new phone or user or to modify the parameters of a selected phone or user.

The Create or Edit Phone/User dialog box contains four tabs: Phone, User, Mailbox, and Phone Settings.

See the following topics as appropriate:

- Create or Edit Phone/User—Phone Tab, page 56-42
- Create or Edit Phone/User—User Tab, page 56-47
- Create or Edit Phone/User—Mailbox Tab, page 56-50
- Create or Edit Phone/User—Phone Settings Tab, page 56-54
- User, Phones, and Extensions Basic Workflow, page 56-1

How to Get to This Page

- To create a phone or user, choose **Configure > Unified Communications > Users, Phones, and Extensions > Phones and Users > Create**.
- To edit phone or user information, choose **Configure > Unified Communications > Users, Phones, and Extensions > Phones and Users > Edit**.

Note To configure SIP phones, enable SIP to SIP connection from **Unified Communications > VoIP settings**.

Create or Edit Phone/User—Phone Tab

Use the Phone tab to assign users with phones and extensions.

Specify the phone type, phone model, MAC address, router port phone connection, auto-line selection, and extensions.

A user can have multiple extensions. The number of extensions assigned to each user must not exceed the number of phone lines available for the phone.

How to Get to This Page

- To assign users with phone and extensions, choose **Configure > Unified Communications > Users, Phones, and Extensions > Phones and Users > Create > Phone** tab.
- To edit user information, choose **Configure > Unified Communications > Users, Phones, and Extensions > Phones and Users > Edit > Phone** tab.

Related Links

- Creating, Editing, Deleting, Restarting, and Resetting Phones and Users, page 56-22
- Configuring Line Types, page 56-26
- User, Phones, and Extensions Basic Workflow, page 56-1

Field Reference

Table 56-6 Phone Tab

Element	Description
Phone Type	Click the SCCP radio button or SIP radio button. **Note** This is a mandatory field.
Phone Model drop-down list	Choose the model of phone to configure from the drop-down list. The list might include the model numbers of the phones, IP communicator, ATA, and Analog. **Note** This is a mandatory field. **Note** If you are editing a configuration, this field is read only.

Table 56-6 Phone Tab (continued)

Element	Description
MAC address field	Enter the MAC address of the phone. The MAC address must include one of the following formats: • xxxx.xxxx.xxxx. For example, 000C.F142.4CDE. • xx-xx-xx-xx-xx-xx. For example, 00-0C-F1-42-4C-DE. • xx:xx:xx:xx:xx:xx. For example, 00:0C:F1:42:4C:DE. • xxxxxxxxxxxx. For example, 000CF1424CDE **Note** This is a mandatory field. **Note** The MAC Address field is disabled if you choose Analog as the phone type. After you choose a port from the Router's Port Phone is Connected To field, the value in this field is populated automatically. Router's Port Phone is Connected To field is not available with SIP phone type. **Note** If you are editing a configuration, this field is read only.
Router's port phone is connected to drop-down list	Choose the router port to which the analog phone is connected, from the drop-down list. The available ports that are not configured as a trunk are listed. **Note** Applicable for Analog phones only. **Note** You cannot modify the FXS Port or the type of analog phone. To move an analog phone to another port, you must create a new analog phone using the new FXS port. **Note** This field is not available with SIP phone type.

Table 56-6 Phone Tab (continued)

Element	Description
Auto-line selection drop-down list	Choose the auto-line from the drop-down list. The options are: • Enable—The Enable option is selected by default. On multiline IP phones, when you lift the handset, it automatically selects the first ringing line on the phone. If no line is ringing, it selects the first available idle line for the outgoing call. • Disable—When you press the Answer soft key, the first ringing line is answered. When you press a line button, the line for an outgoing call is selected. When you lift up the handset, the call is not answered and there is no dial tone. • Incoming—When you lift the handset, it automatically selects the first ringing line on the phone. If no line is ringing, it does not select the first available idle line for the outgoing call. You must press a line button to select a line for the outgoing call. **Note** This field is not available with SIP phone type.
Extensions Pane	
Available Extensions pane	Lists the available extension numbers that you configured. See Create or Edit Extension Dialog Box, page 56-12.
Extensions—Right Pane (Displays summary information about the selected phone.)	
Line	The phone line number.

Table 56-6 Phone Tab (continued)

Element	Description
Associated Extension	Lists the extension numbers that you added from the Available Extensions pane into the Associated Extension table. You can add or remove extensions from the Associated Extension table by using the arrow buttons or by using the drag and drop feature. **Note** If you selected the line type as Overlay or Call Waiting on Overlay, you can select more than one extension. A minimum of two extensions are required for Overlay and Call Waiting on Overlay line types. For all other line types, you can select one extension only. To add the extension, do one of the following: • Use the arrow buttons—Select an extension from the Available Extensions list, and then click the **>** button. The extension number is added to the Associated Extension list. To add all the extension numbers, click the **>>** button. • Use the drag and drop feature—Select the extension or extensions from the Available Extensions list, and then drag and drop it into the Associated Extension list. To remove the extension, do one of the following: • Use the arrow buttons—Select the extension from the Associated Extension list, and then click the **<** button. The extension number is removed from the Associated Extension list. To remove all the numbers from the Associated Extension list, click the **<<** button. • Use the drag and drop feature—Select the extension or extensions from the Associated Extension list, and then drag and drop it into the Available Extensions list pane.

Table 56-6 Phone Tab (continued)

Element	Description
Line Type drop-down list	Choose one of the following options: • Regular—In a regular line, one directory number is assigned to one phone; whereas in a shared line, multiple phones share a common directory number. See Creating a Regular Line, page 56-26 and Creating a Shared Extension, page 56-27. When you choose this option, the Ring Behavior field is enabled. **Note** A mail box can be associated with a regular line only. If a mail box is associated with a regular line, and later, that line is shared with another user, the mail box is deleted. • Overlay—Overlaid ephone-dns are directory numbers that share the same button on a phone. Overlaid ephone-dns can be used to receive incoming calls and place outgoing calls. See Creating an Overlay or Call Waiting on Overlay Line, page 56-31. • Monitor—A monitor line is a line that is shared by two people. Only one person can make and receive calls on the shared line at a time, while the other person, whose line is in monitor mode, is able to see that the line is in use. See Creating a Monitor Line, page 56-30. • Call Waiting on Overlay—Call waiting allows phone users to know that another person is calling them while they are talking on the phone. See Creating an Overlay or Call Waiting on Overlay Line, page 56-31. • Watch—The watch line allows the phone user, such as a receptionist, to visually monitor the in-use status of an individual extension. See Creating a Watch Line, page 56-34. **Note** The Watch Mode Settings feature is supported on router's running Cisco Unified CME 4.1 and later versions.

Table 56-6 Phone Tab (continued)

Element	Description
Ring Type drop-down list	This field is enabled only if you choose the Line Type as Regular. For all other line types, this field is disabled. To specify the ring behavior, choose one of the following options: • Normal—The phone produces an audible ringing, a flashing ((< icon in the phone display, and a flashing red light on the handset for incoming calls. A flashing yellow light also accompanies incoming calls on the Cisco Unified IP Phone Expansion Module 7914. • Feature—A triple-pulse cadence that differentiates incoming calls on one line from incoming calls on other lines on the phone. • Beep (no ring)—Suppresses an audible ring for incoming calls, and allows call-waiting beeps. Visible cues are the same as described for normal ring. • Silent—You cannot hear a call-waiting beep or call-waiting ring regardless of whether the number associated with the button is configured to generate a call-waiting beep or call-waiting ring.
Buttons	
OK button	Click this button to send the configured phone and extension information to the router.
Cancel button	Click this button to discard the configuration values that you entered.

Create or Edit Phone/User—User Tab

Use the User tab to specify the user ID, display name, password, PIN, and other parameters.

How to Get to This Page

- To create a user, choose **Configure > Unified Communications > Users, Phones, and Extensions > Phones and Users > Create > User** tab.
- To edit user information, choose **Configure > Unified Communications > Users, Phones, and Extensions > Phones and Users > Edit > User** tab.

Related Links

- Creating, Editing, Deleting, Restarting, and Resetting Phones and Users, page 56-22
- Configuring Line Types, page 56-26
- User, Phones, and Extensions Basic Workflow, page 56-1

Field Reference

Table 56-7 User Tab

Element	Description
User ID field	ID of the user. The user ID is a combination of letters and numbers. A user ID must start with a letter (a—z or A—Z) and end with a letter (a—z or A—Z) or a number (0—9). Allowed special characters: • . (dot) • - (hypen) • _ (underscore)
First Name field	First name of the user.
Last Name field	Last name of the user.
Display Name field	First name and last name of the user that you entered. This name appears in phone and voice monitoring displays. This field is read-only.
Password Generation drop-down list	Choose one of the following: • Use Blank Password—This option is selected by default. • Use Custom Password Below—To use a custom password, choose this option, and then enter the password in the New Password and Confirm Password fields.

Table 56-7 User Tab (continued)

Element	Description
New Password field	If you chose Use Custom Password Below in the Password Generation field, enter the password in this field. A password can consist of letters and numbers. It must contain at least one character, and no more than 120 characters.
Confirm Password field	Reenter the password. Cisco Configuration Professional compares the text you enter in this field with the text in the New Password field and displays a message if they are not the same.
PIN Generation drop-down list	Personal Identification Number (PIN). Choose one of the following: • Use Blank PIN—This option is selected by default. • Use Custom PIN Below—To use a custom PIN, choose this option, and then enter the PIN in the New PIN and Confirm PIN fields. **Note** This field is not available for SIP phone type.
New PIN field	If you chose Use Custom PIN Below in the PIN Generation field, enter the PIN in this field. Enter only digits. Enter at least four digits, but no more than eight digits. **Note** This field is not available for SIP phone type.
Confirm PIN field	Re-enter the PIN. Cisco Configuration Professional compares the text you enter in this field with the text in the New PIN field and displays a message if they are not the same. **Note** This field is not available for SIP phone type.
OK button	The OK button cannot be used from the Create User dialog box. After you enter the user information in the User tab, you must assign the user with phones and extensions in the Phone/Extensions tab, otherwise, you will get an error message when you click OK. The OK button can be used from the Edit User dialog box. After you make changes in the Password Generation and Pin Generation fields (the only fields that are editable), and then you click **OK**, the updated information is sent to the router.
Cancel button	Click this button to discard the configuration values that you entered.

Create or Edit Phone/User—Mailbox Tab

In the Mailbox tab, configure the user mailbox.

If mailbox size settings are not made in this screen, the default size setting for all phones is used.

At least one regular unshared extension is required for a mailbox.

Note The Mailbox tab is disabled if Cisco Unified CME is not available on the router.

The Mailbox tab has two tabs, Mailbox User Credentials and Mailbox Configuration. See Mailbox User Credentials Tab, page 56-51 and Mailbox Configuration Tab, page 56-53.

How to Get to This Page

- To assign a user with a mailbox, choose **Configure > Unified Communications > Users, Phones, and Extensions > Phones and Users > Create > Mailbox** tab.
- To assign a user with a mailbox, choose **Configure > Unified Communications > Users, Phones, and Extensions > Phones and Users > Edit > Mailbox** tab.

Related Links

- Creating, Editing, Deleting, Restarting, and Resetting Phones and Users, page 56-22
- Configuring Line Types, page 56-26
- User, Phones, and Extensions Basic Workflow, page 56-1

Field Reference

Table 56-8 Mailbox tab

Element	Description
Dial by Name Configurations pane	
Enable Dial-by-name check box	Check to enable dial-by-name.
Associated Extension drop-down list	Choose the associated extension. This is a mandatory field.
Add Voice Mailbox check box	Check to enable a mailbox for a user.
Mailbox User Credentials tab	See Mailbox User Credentials Tab, page 56-51.
Mailbox Configuration tab	See Mailbox Configuration Tab, page 56-53.

Mailbox User Credentials Tab

Configure the user credentials for the user mailbox in this tab.

Field Reference

Table 56-9 Mailbox User Credentials Tab

Element	Description
Password Generation drop-down list	Choose one of the following: • Use Custom Password Below—To use a custom password that you enter, choose this option and enter the password in the New Password and Confirm Password fields. • Use Blank Password—To use a blank password (no password set), choose this option. The New Password and Confirm Password fields are disabled.

Table 56-9 Mailbox User Credentials Tab (continued)

Element	Description
New Password field	If you chose Use Custom Password Below in the Password Generation field, enter the password in this field. A password can consist of letters and numbers. It can be from 3 to 32 characters long.
Confirm Password field	Reenter the password. Cisco Configuration Professional compares the text you enter in this field with the text in the New Password field and displays a message if they are not the same.
PIN Generation drop-down list	To configure a user PIN, choose one of the following: • Use Custom PIN below—To use a custom PIN that you enter, choose this option and enter the PIN in the New PIN and Confirm PIN fields. •Use Blank PIN—To use a blank PIN, choose this option. The New PIN and Confirm PIN fields are disabled. **Note** This field is not available for SIP phone type.
New PIN field	If you chose Use Custom PIN Below in the PIN Generation field, enter the PIN in this field. Enter only digits. Enter at least three digits, but no more than 16 digits. **Note** This field is not available for SIP phone type.
Confirm PIN field	Reenter the PIN. Cisco Configuration Professional compares the text you enter in this field with the text in the New PIN field and displays a message if they are not the same. **Note** This field is not available for SIP phone type.

Mailbox Configuration Tab

Configure the user configuration parameters for the user mailbox in this tab.

Field Reference

Table 56-10 Mailbox Configuration Tab

Element	Description
Mailbox Description	Enter a description of the mailbox. If a user has multiple extensions and multiple mailboxes, entering a different description for each can be helpful.
Associated Extension	Enter the user extension to associate with this mailbox. Only one extension can be associated with a mailbox.
Voice Mailbox Size	Enter the maximum number of seconds of stored messages allowed for the voice mailbox.
Maximum Caller Message Size	Enter the maximum size, in seconds, of a message that can be left by a caller in the voice-mail system.
Voice Mail Message Expiration	Enter the number of days to store messages. After a message has been stored for the specified number of days, the user can resave the message or delete it.
Zero Out Number	Enter the number to which callers are to be transferred when they press 0 at a voice-mail greeting. If callers are to reach the operator when they press 0, enter the operator extension in this field.
Play Voice Mail Tutorial	Choose one of the following: • Yes—Play the system voicemail tutorial the first time that the user logs in to the mailbox. The tutorial provides instructions on setting up a greeting and creating a password. • No—Do not play the system voicemail tutorial.
Voice Mailbox Enabled	Choose one of the following: • Yes—Enable this mailbox immediately. • No—Disable this mailbox.

Table 56-10 Mailbox Configuration Tab (continued)

Element	Description
Greeting Type	Choose one of the following: • Standard—Play the standard system greeting when callers reach the voice mailbox. • Alternate—Play the user's alternate greeting when callers reach the voice mailbox.

Create or Edit Phone/User—Phone Settings Tab

Use the Phone Settings tab to configure night service, remote worker, and speed dial.

How to Get to This Page

- To assign users with phone and extensions, choose **Configure > Unified Communications > Users, Phones, and Extensions > Phones and Users > Create > Phone Settings** tab.
- To edit user information, choose **Configure > Unified Communications > Users, Phones, and Extensions > Phones and Users > Edit > Phone Settings** tab.

Related Links

- Creating, Editing, Deleting, Restarting, and Resetting Phones and Users, page 56-22
- Phones and Users Summary Page, page 56-36
- User, Phones, and Extensions Basic Workflow, page 56-1

Field Reference

Table 56-11 Phone Settings tab

Element	Description
Night Service pane	
Enable this phone to receive calls to unstaffed extensions check box	Check this check box to enable the night-service feature on the phone. The night-service feature allow the phone to receive calls made to unstaffed extensions during hours that you designate as night-service hours. **Note** This field is not available with SIP phone type.
Allow this phone to make blocked calls during after hours check box	Check this check box to allow the phone to make blocked calls during night service hours.
Enable Remote Worker check box	Check this check box to enable options for a remote worker. Remote phones connect to the office network over a WAN. **Note** This field is disabled if you choose an analog phone.
Select codec type drop-down list	Choose the codec type for the remote phone to connect. Based on the Cisco Unified CME version installed on the phone, the codecs that are available from the drop-down list might change.
Speed Dial pane	
Speed dial code field	Click the Add button and select the row to enter speed dial code for the selected phone. This is a mandatory field. To edit an existing configuration, select the row and make the changes in-line. **Note** The maximum number of speed dials that can be configured for a user in Offline Mode is 33, irrespective of the Cisco Unified CME version of the device.

Table 56-11 Phone Settings tab (continued)

Element	Description
Phone number field	Click in the field and enter the phone number. This is a mandatory field. To edit an existing configuration, select the row and make the changes in-line.
Label field	Click in the field and enter the label. To edit an existing configuration, select the row and make the changes in-line.
Add button	Click the Add button to add a new speed dial definition. A new line appears at the end of the list. You can enter the speed dial code, phone number, and label inline. Speed dial code and phone number are mandatory entries.
Delete icon	Select speed dial definitions and click the delete icon to delete that setting.
OK button	Click this button to apply the phone configuration to the router.
Cancel button	Click this button to discard the configuration values that you entered.

CHAPTER 57

Dial Plans

The dial plan instructs a call processing agent, such as Cisco Unified Communication Manager Express (Cisco Unified CME), on how to route calls. Dial plan rules govern how a user reaches any destination. These rules include:

- Extension dialing — how many digits must be dialed to reach an extension on the system
- Extension addressing — how many digits are used to identify extensions
- Dialing privileges — allowing or not allowing certain types of calls
- Path selection — for example, using the IP network for on-net calls, or using one carrier for local PSTN calls and another for international calls
- Automated selection of alternate paths in case of network congestion — for example, using the local carrier for international calls if the preferred international carrier cannot handle the call
- Blocking calling privileges — Devices can be grouped and assigned to different classes of service, granting or denying access to certain destinations. For example, lobby phones might be allowed to reach only internal and local PSTN destinations, while executive phones could have unrestricted PSTN access.

- Transformation of the called number — for example, retaining only the last five digits of a call dialed as a ten-digit number. In some cases, it is necessary to manipulate the dialed string before routing the call. For example, rerouting a call over the PSTN, when the call was originally dialed using the on-net access code.
- Call coverage — Special groups of devices can be created to handle incoming calls for a specific service according to different rules (top-down, circular hunt, longest idle, or broadcast).

A dial plan suitable for an IP telephony system is not fundamentally different from a dial plan designed for a traditional TDM telephony system; however, an IP-based system presents the dial plan architect with some new possibilities. For example, because of the flexibility of IP-based technology, telephony users in separate sites who used to be served by different, independent TDM systems can now be included in one, unified IP-based system.

This chapter describes:

- Configuring Incoming Dial Plan
- Configuring Outgoing Calls
- Configuring International Dial Plan
- Configuring Dial Peer
- Configuring VoIP Dial Peer
- Configuring Translation Rules and Profiles
- Configuring Calling Restrictions
- Configuring Codec Profiles

Configuring Incoming Dial Plan

The incoming calling (dial) plan analyzes, screens, and routes calls originated outside the network based on dialed digits. It defines valid dialing patterns and determines call routing. All records that share a common dial-plan-profile ID are considered a dial plan.

Incoming Dial Plan Reference

The following topic describes the window used to configure an incoming dial or calling plan:

- Configure Incoming Dial Plan

Configure Incoming Dial Plan

For information about how to use Cisco Configuration Professional (Cisco CP) to configure the incoming dial plan feature, see the screencast at:

http://www.cisco.com/en/US/docs/net_mgmt/cisco_configuration_professional/scrcst/ccpsc.html.

Configuring Outgoing Calls

An outgoing dial or calling plan analyzes, screens, and routes calls based on dialed digits.

All dialing destinations added to a device internal call routing table as patterns. These destinations include IP phone lines, voicemail ports, route patterns, translation patterns, and CTI route points.

When a number is dialed, the application uses closest-match logic to select which pattern to match from among all the patterns in its call routing table.

If multiple dial-plan patterns are defined, the system matches extension numbers against the patterns in sequential order, starting with the lowest numbered dial-plan pattern tag first. Once a pattern matches an extension number, the pattern is used to generate an expanded number. If additional patterns subsequently match the extension number, they are not used.

Outgoing Call Reference

An outgoing dial or calling plan analyzes, screens, and routes calls based on dialed digits. It allows you to prioritize the trunks when certain outgoing numbers are dialed. You can also deny or block certain call attempts based on the incoming and outgoing Class of Restrictions (COR) provisioned on the dial-peers.

This section contains the following part:

- Configuring Outgoing Dial Plan

Configuring Outgoing Dial Plan

For information about how to use Cisco Configuration Professional (Cisco CP) to configure this feature, see the screencast at:

http://www.cisco.com/en/US/docs/net_mgmt/cisco_configuration_professional/scrcst/ccpsc.html

Configure Incoming Dial Plan, Outgoing Dial Plan, Import Outgoing Dial Plan Template, and Create/Edit Dial Peer

For information about how to use Cisco Configuration Professional (Cisco CP) to configure the Incoming Dial Plan feature, the Outgoing Dial Plan feature, the Import Outgoing Dial Plan Template, and the Create/Edit Dial Peer feature, see the screencasts at:

http://www.cisco.com/en/US/docs/net_mgmt/cisco_configuration_professional/scrcst/ccpsc.html.

Configuring International Dial Plan

For information about how to use Cisco Configuration Professional (Cisco CP) to configure the International Dial Plan feature, see the Outgoing Dial Plan screencast at:
http://www.cisco.com/en/US/docs/net_mgmt/cisco_configuration_professional/scrcst/ccpsc.html.

Note You must have internet access to view the screencast.

Configuring Dial Peer

Cisco CP enables you to configure dial peer. See Dial Peer Reference for more information.

Dial Peer Reference

The following topic describes the window used to configure dial peer:

- Create or Edit Dial Peer

Create or Edit Dial Peer

For information about how to use Cisco Configuration Professional (Cisco CP) to configure this feature, see the screencast at:

http://www.cisco.com/en/US/docs/net_mgmt/cisco_configuration_professional/scrcst/ccpsc.html.

Configuring VoIP Dial Peer

Cisco CP enables you to configure VoIP dial peer. See VoIP Dial Peer Reference for more information.

VoIP Dial Peer Reference

The following topic describes the window used to configure VoIP dial peer:

- VoIP Dial Peer, page 57-6

VoIP Dial Peer

For information about how to use Cisco Configuration Professional (Cisco CP) to configure this feature, see the screencast at:

http://www.cisco.com/en/US/docs/net_mgmt/cisco_configuration_professional/scrcst/ccpsc.html.

Configuring Translation Rules and Profiles

Cisco CP enables you to configure translation rules and profiles. See Translation Rules and Profiles Reference for more information.

Translation Rules and Profiles Reference

The following topic describes the window used to configure translation rules and profiles:

Create or Edit Translation Rules and Profiles

Create or Edit Translation Rules and Profiles

For information about how to use Cisco Configuration Professional (Cisco CP) to configure this feature, see the screencast at:

http://www.cisco.com/en/US/docs/net_mgmt/cisco_configuration_professional/scrcst/ccpsc.html.

Configuring Calling Restrictions

Cisco CP enables you to restrict the types of calls users can make. See Calling Restrictions Reference for more information.

Calling Restrictions Reference

The following topics describe the window used to configure an incoming dial or calling plan:

- Outgoing Call Types and Permissions
- Create or Edit Outgoing Call Type
- Create or Edit Permission

Outgoing Call Types and Permissions

For information about how to use Cisco Configuration Professional (Cisco CP) to configure the Calling Restrictions feature, see the screencast at:

http://www.cisco.com/en/US/docs/net_mgmt/cisco_configuration_professional/scrcst/ccpsc.html.

Create or Edit Outgoing Call Type

For information about how to use Cisco Configuration Professional (Cisco CP) to configure the Calling Restrictions feature, see the screencast at:

http://www.cisco.com/en/US/docs/net_mgmt/cisco_configuration_professional/scrcst/ccpsc.html.

Create or Edit Permission

For information about how to use Cisco Configuration Professional (Cisco CP) to configure the Calling Restrictions feature, see the screencast at:

http://www.cisco.com/en/US/docs/net_mgmt/cisco_configuration_professional/scrcst/ccpsc.html.

Configuring Codec Profiles

The Voice Class Codec feature enables a Cisco device to connect to other VoIP devices without having prior knowledge about the codec that is used in a call-setup. Use the Voice Class Codec feature to group codecs to use for voice calls. After you configure the voice class codecs, the device chooses the appropriate codec—based on its priority level—to process VoIP calls.

Basic Workflow

1. Group codecs—Create a voice class codec, and then associate available codecs to it. See Create or Edit Voice Class Codec Dialog Box, page 57-11.
2. Assign the voice class codec to Intersite VoIPs and Gateway VoIPs as needed. See VoIP Dial Peer, page 57-6.

   Based on the priority level of the codec in the group, the device chooses the appropriate codec to process VoIP calls.

Related Topics

- Creating, Editing, and Deleting Codec Profiles, page 57-8
- Codec Profiles Reference, page 57-9

Creating, Editing, and Deleting Codec Profiles

Procedure

Use this procedure to create, edit, or delete voice class codecs.

Step 1 Choose **Configure > Unified Communications > Dial Plans > Codec Profiles**. The Codec Profiles summary page opens. See Codec Profiles Summary Page, page 57-10.

Step 2 To create a voice class codec, do the following:

a. Click **Create**. The Create Voice Class Codec dialog box opens. See Create or Edit Voice Class Codec Dialog Box, page 57-11.

b. In the Voice Class Codec Number field, enter a unique identification number to associate with the voice class codec entry. The range is between 1 and 10000.

c. From the Available Codecs pane, select the codec to associate with the Voice Class Codec Number, and then click the **>** button. The codec is added to the Associated Codecs pane. To add all the codecs, click the **>>** button. Use the drag and drop feature to add or remove codecs from the Associated Codecs pane.

Note The associated codecs are listed from highest to lowest priority.

d. To change the priority of a particular codec, use the up or down arrow buttons, or use the drag and drop feature to move the codec up or down the priority list.

e. Click **OK** to send the configuration to the device.

Step 3 To edit a voice class codec, do the following:

a. Choose an entry whose parameters to modify, and click **Edit**. The Edit Voice Class Codec dialog box opens. See Create or Edit Voice Class Codec Dialog Box, page 57-11.

b. Change the parameters by using the arrow buttons, and click **OK**.

Step 4 To delete a voice class codec, do the following:

a. Choose an entry row or multiple entry rows to delete, and click **Delete**. A confirmation dialog box opens.

b. Click **Yes** in the confirmation dialog box.

Related Topics

- Configuring Codec Profiles, page 57-8
- Codec Profiles Reference, page 57-9

Codec Profiles Reference

The following topics describe the Codec Profiles pages and dialog boxes used to configure voice class codecs:

- Codec Profiles Summary Page, page 57-10
- Create or Edit Voice Class Codec Dialog Box, page 57-11

Codec Profiles Summary Page

Use the Codec Profiles summary page to view the codecs that are configured, to create new codecs, to modify parameters of a selected codec, and to delete codecs.

How to Get to This Page

Choose **Configure > Unified Communications > Dial Plans > Codec Profiles**.

Related Topics

- Configuring Codec Profiles, page 57-8
- Creating, Editing, and Deleting Codec Profiles, page 57-8
- Create or Edit Voice Class Codec Dialog Box, page 57-11

Field Reference

Table 57-1 Codec Profiles Summary Page

Element	Description
Filter	Allows you to filter the display according to what you want to view.
Voice Class Codec Number	Identification number that is associated with the voice class codec entry.
Member Codecs	Associated codecs from highest to lowest priority order.
Create button	Click this button to open the Create Voice Class Codec dialog box to select the codecs to group. See Creating, Editing, and Deleting Codec Profiles, page 57-8.
Edit button	Click this button to open the Edit Voice Class Codec dialog box to modify the codecs that are associated. See Creating, Editing, and Deleting Codec Profiles, page 57-8.
Delete button	Click this button to delete a selected voice class codec row or multiple rows. See Creating, Editing, and Deleting Codec Profiles, page 57-8.

Create or Edit Voice Class Codec Dialog Box

Use the Create or Edit Voice Class Codec dialog box to create new voice class codec entries or to modify the parameters of a selected entry.

How to Get to This Dialog Box

- Choose **Configure > Unified Communications > Dial Plans > Codec Profiles > Create**
- Choose **Configure > Unified Communications > Dial Plans > Codec Profiles > Edit**

Related Topics

- Configuring Codec Profiles, page 57-8
- Creating, Editing, and Deleting Codec Profiles, page 57-8
- Codec Profiles Summary Page, page 57-10

Field Reference

Table 57-2 Create or Edit Voice Class Codec Dialog Box

Element	Description
Voice Class Codec Number	Identification number that is associated with the voice class codec entry. The range is between 1 and 10000.
Codecs	
Available Codecs (left pane)	Lists the available codecs that are supported on the device.
> or >> arrow buttons < or << arrow buttons	Use these buttons to add or remove codecs from the Associated Codecs pane. To add a codec, select a codec from the Available Codecs list, and click the > button. The codec is added to the Associated Codecs pane. To add all the codecs, click the >> button. To remove the codec, select the codec from the Associated Codecs pane, and click the < button. The codec is removed from the Associated Codecs pane. To remove all the codecs from the Associated Codecs pane, click the << button. **Note** You can also use the drag and drop feature to add or remove codecs from the Associated Codecs pane.

Table 57-2 Create or Edit Voice Class Codec Dialog Box (continued)

Element	Description
Associated Codecs (right pane)	Contains the codecs that you added from the Available Codecs pane into the Associated Codecs pane. The associated codecs are listed from highest to lowest priority. You can change the codec priority by using the up and down arrows. The codecs that you add to the Associated Codecs pane are grouped under the voice class codec number that you enter in the Voice Class Codec Number field. After you group the codecs, you can assign that voice class codec number to Intersite VoIPs and Gateway VoIPs. See VoIP Dial Peer, page 57-6. Based on the priority level of the codec in the group, the device chooses the appropriate codec to process VoIP calls.
Up and Down arrow buttons	Use these buttons to move the codec up or down in the priority list. **Note** You can also use the drag and drop feature to move the codec up or down in the priority list.
OK button	Click this button to send the configuration to the device.
Cancel button	Click this button to cancel the changes that you made to this page and return to the original values.

CHAPTER 58

VoIP Settings

Use the VoIP Settings feature in Cisco Configuration Professional (Cisco CP) to enable or disable VoIP settings.

The following topics provide more information:

- VoIP Settings, page 58-1
- VoIP Settings Feature Behavior, page 58-11

VoIP Settings

The VoIP Settings feature in Cisco CP allows you to enable or disable connections between specific types of end points. See VoIP Settings Page, page 58-3.

The VoIP Settings feature also allows you to enable or disable supplementary services using SIP or H.323. Supplementary services are used for call transferring, call forwarding, and message waiting indication (MWI) capabilities across a VoIP network. To enable supplementary services, check the appropriate check boxes under the SIP Settings tab or the H.323 Settings tab in the VoIP Settings page. See VoIP Settings Page, page 58-3.

Related Topics

- VoIP Settings Page, page 58-3
- Enabling or Disabling VoIP Settings, page 58-2
- VoIP Settings Feature Behavior, page 58-11

Enabling or Disabling VoIP Settings

Procedure

Use this procedure to enable or disable connections between specific types of end points and to enable or disable supplementary services.

Step 1 Click **Configure > Unified Communications > VoIP Settings**.

The VoIP Settings page opens displaying the configured VoIP parameters and their values.

Step 2 Click **Edit**.

The Edit VoIP Settings page opens with the General VoIP Settings tab, the SIP Settings tab, and the H.323 Settings tab.

The H.323 Settings tab is displayed if the router operating mode is Cisco Manager Express or Cisco Manager Express as SRST. See VoIP Settings Page, page 58-3.

Click the **Reset to default** button to remove the voice service VoIP parameters. A confirmation message is displayed asking your confirmation to proceed with removing the VoIP parameters.

Step 3 To enable a VoIP parameter under the General VoIP Settings tab, check the appropriate check box.

To disable a VoIP parameter under the General VoIP Settings tab, uncheck the appropriate check box.

Step 4 Check the Enable address hiding check box to hide the IP address.

Uncheck the Enable address hiding check box to disable hiding the IP address. This checkbox is available if the router operating mode is Gateway and SRST.

Step 5 Click **Apply** to send the information about all of the VoIP parameters that you enabled or disabled to the device.

Step 6 Click the **SIP Settings** tab, if you have selected a connection with SIP as the end protocol. The available connections are SIP-SIP, H.323-SIP, and SIP-H.323.

Step 7 Choose **UDP** or **TCP** from the Transport protocol for SIP signaling drop-down list. This parameter is available only in the Gateway modes.

Step 8 Choose the interface to use as the source for Control packets from the drop-down list. This parameter is available in the Gateway and Cisco Unified CME modes.

Step 9 Choose the interface to use as the source for Media packets from the drop-down list. This parameter is available in the Gateway and Cisco Unified CME modes.

Step 10 To enable a SIP parameter, check the appropriate check box.

To disable a SIP parameter, uncheck the appropriate check box.

Step 11 Click **OK** to send the information about the SIP parameters that you enabled or disabled to the device.

Click **Cancel** to undo the changes you made.

Step 12 Click the **H.323 Settings** tab.

Step 13 To enable a H.323 parameter, check the appropriate check box.

To disable a H.323 parameter, uncheck the appropriate check box.

Step 14 Click **OK** to send the information about the H.323 parameters that you enabled or disabled to the device.

Click **Cancel** to undo the changes you made.

Related Topics

- VoIP Settings, page 58-1
- VoIP Settings Page, page 58-3
- VoIP Settings Feature Behavior, page 58-11

VoIP Settings Page

Use the VoIP Settings page to display the configured VoIP parameters and their values.

The options displayed on this page depend on the router operating mode you choose under **Configure > Unified Communications > Features** and the Cisco IOS image running on the router.

How to Get to This Page

Choose **Configure > Unified Communications > VoIP Settings**.

Related Topics

- VoIP Settings, page 58-1
- Edit VoIP Settings Page, page 58-4
- Enabling or Disabling VoIP Settings, page 58-2

Field Reference

Table 58-1 VoIP Settings Page

Element	Description
VoIP Parameter list	Use to view the list of parameters configured under the General VoIP Settings tab, SIP Settings tab, and H.323 Settings tab.
Configured Value list	Use to view whether a parameter is enabled or disabled.
Edit button	Click the **Edit** button to display the Edit VoIP Settings page.
Reset to default button	Click the **Reset to default** button to remove the voice service VoIP parameters. Clicking the button issues the CLI **no voice service voip**.

Edit VoIP Settings Page

Use the Edit VoIP Settings page to enable or disable connections between specific types of end points and to enable or disable supplementary services using SIP or H.323.

How to Get to This Page

Choose **Configure > Unified Communications > VoIP Settings > Edit**.

Related Topics

- VoIP Settings Page, page 58-3
- Enabling or Disabling VoIP Settings, page 58-2

Field Reference

Table 58-2 Edit VoIP Settings Page

Element	Description
General VoIP Settings tab	Use to enable or disable connections between specific types of endpoints.
SIP Settings tab	Use to set supplementary services using SIP.
H.323 Settings tab	Use to set supplementary services using H.323. This tab is available when the router operating mode is Cisco Manager Express or Cisco Manager Express as SRST.

Table 58-3 General VoIP Settings Tab

Element	Description
Allow connection between two SIP endpoints checkbox	Check this check box to enable connections between two SIP endpoints.
Allow connection from SIP to H.323 endpoints checkbox	Check this check box to enable connections between SIP (originating) and H.323 (terminating) endpoints.
Allow connection from H.323 to SIP endpoints checkbox	Check this check box to enable connections between H.323 (originating) and SIP (terminating) endpoints.
Allow connection between two H.323 endpoints checkbox	Check this check box to enable connections between two H.323 endpoints.
Enable address hiding checkbox	Check this checkbox to enable hiding of signaling and media peer addresses from endpoints. Uncheck this checkbox to disable address hiding. This checkbox is available if the router operating mode is Gateway and SRST.
OK button	Click the **OK** button to send the information about all of the VoIP parameters that you enabled or disabled to the device.
Cancel button	Click the **Cancel** button to undo the changes you made.

Table 58-4 SIP Settings Tab

Element	Description
Router operating mode—Cisco Manager Express or Cisco Manager Express as SRST	
Allow the device to send a SIP Redirect response to the destination for call forwarding checkbox	Check this checkbox to enable SIP Redirect messages for forwarding of calls.
Allow the device to forward a SIP Refer message to the destination for call transfer checkbox	Check this checkbox to enable SIP Refer messages for transfer of calls.
Enable local SIP registrar check box	Check this checkbox to enable SIP Register messages from local SIP phones.
Router operating mode—Gateway or Gateway and SRST or Gateway and CME as SRST or CUBE	
Note The SIP Settings tab is dimmed if a connection with SIP endpoint is not selected under the General VoIP Settings tab.	

Table 58-4 SIP Settings Tab (continued)

Element	Description
Transport protocol for SIP signaling drop-down list	Choose **UDP** or **TCP** from the Transport protocol for SIP signaling drop-down list.
Interface to be used as source in Control (SIP) packets drop-down list	Choose the interface to use as the source for Control packets from the drop-down list.
Interface to be used as source in Media (SRTP) packets drop-down list	Choose the interface to use as the source for Media packets from the drop-down list.
Enable local SIP registrar check box	Check this checkbox to enable SIP Register messages from local SIP phones. Uncheck this checkbox to disable this feature. The Enable local SIP registrar parameter is not available in Gateway - None router operating mode.
Enable SIP Delayed Offer to SIP Early Offer interworking check box	In a SIP call, the calling endpoint can specify its capabilities in the initial call request (early offer) and let the called endpoint choose its preference. Otherwise, the calling endpoint can wait for the called endpoint to send its capabilities first (delayed offer) and choose the preference from what is sent. Check this check box to enable SIP delayed offer to SIP early offer interworking. Uncheck this check box to disable this feature.
Enable midcall signaling event pass-through check box	SIP-to-SIP video and SIP-to-SIP reinvite-based supplementary services require SIP messages to be passed from one IP leg to the other IP leg. This feature is only applicable for SIP-to-SIP call processing. Check this check box to enable SIP messages to be passed from one IP leg to the other. Uncheck this check box to disable this feature.

Table 58-4 SIP Settings Tab (continued)

Element	Description
Allow media packets to be passed directly between end points checkbox.	Check this checkbox to enable media packets to be passed directly between endpoints, without the intervention of the device. Uncheck this checkbox to disable this feature.
Force the device to send SIP Invite with Early Offer on the out-leg of the call checkbox	In an Early Offer, the session initiator or calling device sends its capabilities (for example, codecs supported) in the initial invite. This allows the called device to choose its preferred codec for the session. Check this checkbox to enable the Early Offer feature. Uncheck this checkbox to disable the Early Offer feature.
Allow SIP messages to pass through from one IP leg to another IP log (enables the support for SIP supplementary services for SIP-to-SIP calls) checkbox	Most SIP-to-SIP video and SIP-to-SIP reinvite-based supplementary services require SIP messages to be passed from one IP leg to the other IP leg. This is applicable only for SIP-to-SIP call processing. Check this checkbox to enable SIP supplementary services support for SIP-to-SIP calls. Uncheck this checkbox to disable SIP supplementary services support.
Allow SIP error messages to pass through without modifications checkbox	The SIP error messages pass through feature allows a received error response from one SIP leg to pass transparently over to another SIP leg. This functionality passes SIP error responses that are not yet supported by the device or preserves the ISDN error codes (Q.850 cause codes) across two SIP call-legs. Check this checkbox to enable SIP error messages to pass through transparently. Uncheck this checkbox to disable SIP error messages passing through transparently.

Table 58-4 SIP Settings Tab (continued)

Element	Description
Allow privacy policies to pass through checkbox	If a received SIP message contains privacy values, the privacy policy pass through feature allows the privacy values to pass from one call leg to the next. Check this checkbox to enable privacy policies to pass. Uncheck this checkbox to disable privacy policies from passing.
Enable the device to insert identity headers checkbox	The PAI[1] or the PPI[2] header field can be used to convey the proven identity of the originator of a SIP request within a trusted network. Check this checkbox to enable the device to insert one of these identity headers in the SIP requests and responses. Uncheck this checkbox to disable identity headers. The Use P-Asserted-Identity and Use P-Preferred-Identity radio buttons are activated when this checkbox is checked. Click the appropriate radio button to choose the type of identity header.
Allow the device to negotiate all favors of G.729 codecs checkbox	There are different variations of G.729 coder-decoder (codec) for audio streams. This feature enables the device to allow connections of calls with two incompatible G.729 codecs through negotiation of G.729 codecs. Check this checkbox to enable the device to negotiate all favors of G.729 codecs. Uncheck this checkbox to disable the device from negotiating G.279 codecs.
OK button	Click the **OK** button to send the information about the SIP parameters that you enabled or disabled to the device.
Cancel button	Click the **Cancel** button to undo the changes you made.

1. PAI = P-Asserted-Identity.

2. PPI = P-Preferred-Identity.

Table 58-5 H.323 Settings Tab

Element	Description
Note The H.323 Settings tab is displayed if the router operating mode is Cisco Manager Express or Cisco Manager Express as SRST.	
Use H.450.2 protocol for call transfers checkbox	Check this check box to enable call transferring across a VoIP network.
Use H.450.3 protocol for call forwarding checkbox	Check this check box to enable call forwarding across a VoIP network.
Use H450.12 protocol for advertising and discovering call transfer and call forward capabilities checkbox	Check this check box to advertise and discover H.450.2 call transfer and H.450.3 call forwarding capabilities in voice gateway endpoints on a call-by-call basis. When H.450.12 is enabled, the H.450.2 and H.450.3 standards for call transfers and call forwards are disabled, unless a positive H.450.12 indication is received from all of the other VoIP endpoints involved in the call. If a positive H.450.12 indication is received, the device uses the H.450.2 standard for call transfers and the H.450.3 standard for call forwarding.
Use H.450.7 protocol for exchange of message waiting indication (WMI) checkbox	Check this check box to enable message waiting indication (MWI) across a VoIP network.
OK button	Click the **OK** button to send the information about the H.323 parameters that you enabled or disabled to the device.
Cancel button	Click the **Cancel** button to undo the changes you made.

VoIP Settings Feature Behavior

Cisco CP supports the following CLIs for the VoIP Settings feature:

- **voice service voip**
  - **allow-connections sip to sip**
  - **allow-connections sip to h323**
  - **allow-connections h323 to sip**
  - **allow-connections h323 to h323**
  - **supplementary-service sip moved-temporarily**
  - **supplementary-service sip refer**
  - **supplementary-service h450.2**
  - **supplementary-service h450.3**
  - **supplementary-service h450.7**
  - **supplementary-service h450.12**
  - **address-hiding**
  - **media flow-around**
  - **sip**

    The following are SIP sub-commands:
  - **registrar server**
  - **session transport** <*tcp*|*udp*|*tcp tls*>
  - **bind control source-interface** <*interface*>
  - **bind media source-interface** <*interface*>
  - **early-offer forced**
  - **midcall-signaling passthru**
  - **header-passing error-passthru**
  - **privacy-policy passthru**
  - **asserted-id** <*pai*|*ppi*>
  - **g729 annexb-all**

However, the VoIP Settings feature displays parameters based on what Unified Communication features are configured on the device. For example, some of the VoIP settings are applicable to CME only, while others are applicable to Cisco Unified Border Element (CUBE) or Gateway scenario.

The options available for VoIP Settings varies based on the following guidelines:

- If an individual Unified Communication (UC) mode is selected (i.e. only CME is selected or only CUBE is selected), the parameters available for each individual mode are as follows:

Table 58-6 Options supported on individual modes

Cisco CP Supported VoIP Settings Options	Cisco Unified CME	Cisco Unified CME as SRSt	SRST	TDM Gateway	CUBE
allow-connections sip to sip	supported	supported	supported	supported	supported
allow-connections sip to h323	supported	supported	supported	supported	supported
allow-connections h323 to sip	supported	supported	supported	supported	supported
allow-connections h323 to h323	supported	supported	✓	supported	supported
supplementary-service sip moved-temporarily	supported	supported			
supplementary-service sip refer	supported	supported			
supplementary-service h450.2	supported	supported			
supplementary-service h450.3	supported	supported			
supplementary-service h450.7	supported	supported			
supplementary-service h450.12	supported	supported			
address-hiding				supported	supported
media flow-around				supported	supported
sip sub-command options					
registrar server	supported	supported	supported		
session transport <*tcp*|*udp*|*tcp tls*>				supported	supported

Table 58-6 Options supported on individual modes (continued)

Cisco CP Supported VoIP Settings Options	Cisco Unified CME	Cisco Unified CME as SRSt	SRST	TDM Gateway	CUBE
bind control source-interface *<interface>*				supported	supported
bind media source-interface *<interface>*				supported	supported
early-offer forced				supported	supported
midcall-signaling passthru				supported	supported
header-passing error-passthru				supported	supported
privacy-policy passthru				supported	supported
asserted-id *<pai|ppi>*				supported	supported
g729 annexb-all				supported	supported

- For combinations of modes (except when Cisco Unified CME only mode is part of the combination), parameters applicable for all selected modes are shown. For example, if CUBE and Cisco Unified CME as SRST are selected, parameters applicable for both modes from the table above are displayed on the screen.
- For combinations of modes when Cisco Unified CME is also part of the combination, only Cisco Unified CME related parameters are displayed regardless of what other modes are present.
- Only parameters supported on the device are displayed on the screen. For example, depending on the CUBE release, certain parameters from the list above may not be supported. Those parameters are not displayed on the screen.

CHAPTER 59

Telephony Features

This chapter explains how to configure telephony features. It contains the following sections:

- After-Hours Tollbar, page 59-2
- Auto Attendant, page 59-7
- Call Conferencing, page 59-8
- Call Park, page 59-8
- Call Pickup Groups, page 59-13
- Directory Services, page 59-16
- Hunt Groups, page 59-18
- Intercom, page 59-31
- Night Service Bell, page 59-44
- Paging Numbers, page 59-49
- Paging Groups, page 59-56
- Phone Templates, page 59-62
- Extension Templates, page 59-72

After-Hours Tollbar

The After-Hours Tollbar prevents the unauthorized use of phones by matching dialed numbers against a pattern of specified digits and matching the time against the time of day and the day of the week or the date that has been specified for call blocking. Up to 32 patterns of digits can be specified. Call blocking is supported on IP phones only and not on analog foreign exchange station (FXS) phones.

When a user attempts to place a call to digits that match a pattern that has been specified for call blocking during a time period that has been defined for call blocking, a fast busy signal is played for approximately 10 seconds. The call is then terminated and the line is placed back in on-hook status.

If a user tries to dial a number that matches a pattern that is specified for call blocking after office hours, the call is terminated and the phone status returns to on-hook.

Individual phone users can override the call blocking that has been defined for designated time periods. The system administrator must first assign a personal identification number (PIN) to any phone that will be allowed to override call blocking.

Logging in to a phone with a PIN only allows the user to override call blocking that is associated with particular time periods. Blocking patterns that are in effect 7 days a week, 24 hours a day cannot be overridden by using a PIN.

When PINs are configured for call-blocking override, they are cleared at a specific time of day or after phones have been idle for a specific amount of time. The time of day and amount of time can be set by the system administrator, or the defaults can be accepted.

Note A phone can be exempted from the Tollbar by using the **Configure > Unified Communications > Users, Phones and Extensions > Phones** window.

Note After-Hours Tollbar is supported with SIP endpoints.

After-Hour Tollbar Reference

The following topics describe the window used to configure the After-Hour Tollbar:

- Configuring Outgoing Call Restrictions, page 59-3
- Configuring a Weekly Schedule, page 59-4
- Configuring a Holiday Schedule, page 59-5
- Configuring an Override (Softkey Login), page 59-6

Configure After-Hour Tollbar

Configure the After-Hour Tollbar as described in these sections:

- Configuring Outgoing Call Restrictions, page 59-3
- Configuring a Weekly Schedule, page 59-4
- Configuring a Holiday Schedule, page 59-5
- Configuring an Override (Softkey Login), page 59-6

Configuring Outgoing Call Restrictions

You can display, add, or modify phone number prefix patterns to be blocked. In gateway mode, call blocking of outgoing calls made by individual users is not supported.

After-Hours Tollbar call blocking restrictions:

- Up to 32 patterns of digits can be specified.
- Supported on IP phones only; not supported on analog (FXS) phones.
- Call blocking applies to all IP phones in the community by default.
- Individual IP phones can be exempted from all call blocking.

Note Duplicate patterns are not allowed.

To always block a particular pattern or prefix, check the Always block this prefix (7-24) check box. In the Blocked Prefixes list, the prefixes with this check box checked, has Always Blocked in brackets next to the prefix. If a user tries to dial a number that matches a pattern that is specified for call blocking, the call is terminated and the phone status returns to on-hook.

How to get to this screen

Click **Configure > Unified Communications > Telephony Features > After-Hour Tollbar > Outgoing Call Restrictions**.

To add the list of blocked prefixes, complete the following tasks:

Step 1 In the Configure tree, choose **Unified Communications > Telephony Features > After-Hour Tollbar > Outgoing Call Restrictions**. Cisco Configuration Professional displays the Outgoing Call Restrictions screen.

Step 2 In the Prefix to block field, enter the number pattern.

Step 3 Check the Always block this prefix (7-24) checkbox, to block that pattern at all times.

Step 4 Click **Add**.

Configuring a Weekly Schedule

The weekly schedule defines a recurring period based on the day of the week during which outgoing calls that match defined block prefix patterns are blocked on IP phones.

How to get to this screen

Click **Configure > Unified Communications > Telephony Features > After-Hour Tollbar > Weekly Schedule**.

Creating a Weekly Schedule

To create or modify a weekly schedule, perform these steps:

Step 1 In the Configure tree, click **Unified Communications > Telephony Features > After-Hour Tollbar > Weekly Schedule**. Cisco Configuration Professional displays the Weekly Schedule screen.

Step 2 Set the times. The Tollbar is applied *before* the time specified and *after* the time specified (the rest of that day is unblocked):

- Select the hour or the minute under the desired day of the week and use the arrows to change the time.
- To toggle between morning and afternoon times, select the **am** or **pm** field and use the arrows to change the setting.

Step 3 Check **All Day** to indicate the settings apply to the entire day.

Copying a Weekly Schedule

To copy a weekly schedule, perform these steps:

Step 1 In the Configure tree, click **Unified Communications > Telephony Features > After-Hour Tollbar > Weekly Schedule**. Cisco Configuration Professional displays the Weekly Schedule screen.

Step 2 Choose a day from the Copy schedule **from** list.

Step 3 Choose a day from the Copy schedule **to** list.

Step 4 Click **Copy**.

Configuring a Holiday Schedule

When a holiday setting is in effect, the system observes off hours blocking rules.

How to get to this screen

Click **Configure > Unified Communications > Telephony Features > After-Hour Tollbar > Holiday Schedule**.

Adding a Holiday

To add a holiday, perform these steps:

Step 1 In the Configure tree, click **Unified Communications > Telephony Features > After-Hour Tollbar > Holiday Schedule**. Cisco Configuration Professional displays the Holiday Schedule screen.

Step 2 Choose a date from the calendar, and click **Add**. Cisco Configuration Professional displays the date in the Select date field.

Step 3 To specify the start and stop times, uncheck **All Day** and use the arrow keys to set the hour and the minute. To toggle between ante meridiem and post meridiem, select **am** or **pm** and use the arrows to change the setting.

Step 4 To put the date in the **Call Restrictions** list, click **Add**.

Configuring an Override (Softkey Login)

Individual phone users can be allowed to override call blocking associated with designated time periods by entering personal identification numbers (PINs) that have been assigned to their phones. To override call blocking, the phone user presses the Login softkey on the phone and enters the PIN that is associated with the phone.

The override is cleared at a specific time of day or after phones have been idle for a specific amount of time.

How to get to this screen

Click **Configure > Unified Communications > Telephony Features > After-Hour Tollbar > Override (Softkey Login)**.

To enable a user to override the after-hours tollbar, perform these steps:

Step 1 In the Configure tree, click **Unified Communications > Telephony Features > After-Hour Tollbar > Override (Softkey Login)**. Cisco Configuration Professional displays the Override (Softkey Login) screen.

Step 2 To allow callers to make calls in spite of the after-hours configuration, click **Enable**.

Step 3 To set the idle time to clear the override, select the **Clear override after** field and use the arrows to change the number of minutes.

Step 4 To clear the override at a specific time, select the hour or the minute in the **Clear override at** field and use the arrows to change the time. To toggle between morning and afternoon times, select **am** or **pm**, and use the arrows to change the setting.

The **Reset to System Defaults** applies the default values of **Clear override after 60 minutes** and **Clear override at 12 am** (midnight).

Auto Attendant

The Auto Attendant feature has the following sections:

- Cisco Unified CME Basic Automatic Call Distribution, page 59-7
- Cisco Unified CME Prompts and Scripts, page 59-7

Cisco Unified CME Basic Automatic Call Distribution

For information on how to use Cisco Configuration Professional (Cisco CP) to configure the Cisco Unified CME Basic Automatic Call Distribution (B-ACD) feature, see the screencast at:
http://www.cisco.com/en/US/docs/net_mgmt/cisco_configuration_professional/scrcst/ccpsc.html

Note You must have Internet access to view the screencast.

Cisco Unified CME Prompts and Scripts

For information about how to use Cisco Configuration Professional (Cisco CP) to configure the Prompts and Scripts feature, see the screencast at:
http://www.cisco.com/en/US/docs/net_mgmt/cisco_configuration_professional/scrcst/ccpsc.html

Note You must have internet access to view the screencast.

Call Conferencing

For information about how to use Cisco Configuration Professional (Cisco CP) to configure the Call Conferencing feature, see the screencast at: http://www.cisco.com/en/US/docs/net_mgmt/cisco_configuration_professional/scrcst/ccpsc.html

Note You must have Internet access to view the screencast.

Note Call conferencing is supported with SIP endpoints.

Call Park

Call park allows a phone user to place a call on hold at a special number that is used as a temporary parking spot from which the call can be retrieved by anyone on the system. In contrast, a call that is placed on hold by using the Hold button or Hold soft key can be retrieved only from the extension that placed the call on hold.

The special number at which a call is parked is known as a call-park slot. A call-park slot is a floating extension, or number that is not bound to a physical phone, to which calls are sent to be held.

After at least one call-park slot has been defined and the Cisco Manager Express (Cisco Unified CME) phones have been restarted, phone users are able to park calls using the Park soft key.

Note Call park is supported with SCCP endpoint and SCCP and SIP endpoint. SIP extensions are not listed.

Call Park Reference

The following topics describe the window used to configure call park:

- Configure Call Park page, page 59-9
- Create or Edit Call-Park Parameters—General Tab, page 59-11
- Create or Edit Call-Park Parameters—Advanced Tab, page 59-12

Configure Call Park page

Display, create, edit, and delete call park parameters. The General tab configures basic call-park parameters, such as the name and number of slots. The Advanced tab configures advanced parameters, such as reminders and termination actions.

How to get to this screen

Click **Configure > Unified Communications > Telephony Features > Call Park**.

Related Links

- Configure Call Park page, page 59-9
- Create or Edit Call-Park Parameters—General Tab, page 59-11
- Create or Edit Call-Park Parameters—Advanced Tab, page 59-12

Field Reference

Table 59-1 Configure Call Park

Element	Description
Call Park type	Choose **General Purpose** or **Directed**. General purpose call park allows the user to place a call on hold so that it can be retrieved from another phone in the system (for example, a phone in another office or in a conference room). If the user is on an active call at that phone, the call can be parked to a call park extension by pressing the Park softkey or the Call Park button. Someone on another phone in the system can then dial the call park extension to retrieve the call. Directed call park allows a user to route a call to another extension or to a voice-messaging mailbox. For example, user A calls user B, and user B parks the call. User B retrieves the call and then decides to send the call to a voice-messaging mailbox. User A receives the voice-messaging mailbox greeting of user B. The user can park only one call at each directed call park number.
Name	Name displayed on a recall or transfer rather than an extension number.
Slots Start From	Starting call-park slot number.
Number of Slots	Number of call-park slots.
Timeout	Interval length during which the call-park reminder ring is timed out or inactive. If the timeout is zero, no reminder ring is sent to the extension that parked the call.
Recall	Interval length which the parked call is returned to the extension that parked the call.

Create or Edit Call-Park Parameters

See the following topics as appropriate:

- Create or Edit Call-Park Parameters—General Tab, page 59-11
- Create or Edit Call-Park Parameters—Advanced Tab, page 59-12

Create or Edit Call-Park Parameters—General Tab

In the General tab, enter the basic call-park parameters, such as the name and number of slots.

How to get to this screen

- Click **Configure > Unified Communications > Telephony Features > Call Park > Create > General** tab.
- Click **Configure > Unified Communications > Telephony Features > Call Park > Edit > General** tab.

Related Links

- Configure Call Park page, page 59-9
- Create or Edit Call-Park Parameters—Advanced Tab, page 59-12

Field Reference

Table 59-2 General Tab

Element	Description
Name	Enter the name to be displayed on a recall or transfer call rather than an extension number.
Number of slots	Enter the number of call-park slots.
Starting number of slots	Enter the starting call-park slot number.
Timeout	Enter the time interval length the call-park reminder ring is timed out or inactive. At the end of the time-out interval, the first reminder ring is sent to the extension that parked the call. If the time-out is zero, no reminder ring is sent.

Create or Edit Call-Park Parameters—Advanced Tab

In the Advanced tab, enter the call-park advanced parameters, such as reminders and termination actions.

How to get to this screen

- Click **Configure > Unified Communications > Telephony Features > Call Park > Create > Advanced** tab.
- Click **Configure > Unified Communications > Telephony Features > Call Park > Edit > Advanced** tab.

Related Links

- Configure Call Park page, page 59-9
- Create or Edit Call-Park Parameters—General Tab, page 59-11

Field Reference

Table 59-3 Advanced Tab

Element	Description
Set reminder to extension	Select an extension from the list, other than the extension from where the call was parked, that will receive a reminder that the call has been parked.
Send reminder to originating phone	To send a reminder to the originating phone extension, click **Yes**. To silence the reminder, click **No**.
Remind user every	Enter the interval length, in seconds, between reminder rings.
Number of reminders to send	Enter the maximum number of reminder ring retries.
Total time in reminder phase	Enter the maximum time that a call will stay parked.

Table 59-4 Advanced Tab Termination Phase

Element	Description
Select Target Phone	Choose to send the call back to the originating extension or to send the call to another extension after the reminder phase has expired. To send the call to another extension, from the Select Number list, select the number to send the call back to after the reminder phase has expired.
Select Action on Target Phone	To send the call back to the target phone immediately after reminder phase: Choose **If target phone is busy...** to set the interval length between retries, and complete the following steps to do so: 1. Enter the number of seconds between retries in the **retry every** field. 2. Enter the number of retries in the **repeating** field. Choose **If target phone busy after retry...** to send a parked call to a different extension when the target phone busy interval expires and complete the following steps to do so: 1. Click **Send call to extension**. 2. Select the target extension from the Select Number list or click **Disconnect**.

Call Pickup Groups

Call pickup groups enable phone users to answer a call that is ringing on a directory number other than their own. The user can answer a ringing phone in any pickup group if the user knows the group number of the ringing phone. If there is only one pickup group defined, the phone user can pick up the call by pressing a soft key. The phone user does not need to belong to the pickup group.

Phone users can pick up the called number on another phone by pressing a soft key plus an asterisk (*) their own phone if both phones are in the same pickup group.

There is no limit to the number of numbers that can be assigned to a pickup group, and there is no limit to the number of pickup groups that can be defined in a system.

Pickup group numbers may be of varying length, but must have unique leading digits. For example, you cannot define pickup group 17 and pickup group 177 for the same system because a pickup in group 17 will always be triggered before the user can enter the final 7 for 177.

Note SIP extensions are not listed for call pickup groups.

Call Pickup Group Reference

The following topics describe the window used to configure call pickup groups:

- Configure Pickup Group, page 59-14
- Create or Edit a Pickup Group, page 59-15

Configure Pickup Group

Display, create, edit, and delete pickup group parameters.

How to get to this screen

Click **Configure > Unified Communications > Telephony Features > Pickup Groups**.

Related Link

- Create or Edit a Pickup Group, page 59-15

Field Reference

Table 59-5 Pickup Group Summary

Element	Description
Pickup Group Number	Number assigned to the pickup group.
Extensions	Extension numbers assigned to the pickup group.

Create or Edit a Pickup Group

Enter or modify the settings for a pickup group.

How to get to this screen

- Click **Configure > Unified Communications > Telephony Features > Pickup Groups > Create**.
- Click **Configure > Unified Communications > Telephony Features > Pickup Groups > Edit**.

Related Links

- Configure Pickup Group, page 59-14

Field Reference

Table 59-6 Create or Edit Pickup Group

Element	Description
Pickup Group Number	Assign a number to the pickup group in the field. Once assigned, the number cannot be edited.
Available Extensions	Extensions eligible to be added to the pickup group. You can choose extensions from this list, and drag them to the Pickup Group Extensions column to add them.
Pickup Group Extensions	Select pickup group extensions: • To add an extension to the list, select an extension in the Available Extensions list and drag it to the Pickup Group Extensions list. Click the right arrow to move it to the Pickup Group Extensions list. • To delete an extension from the list, select an extension in the Pickup Group Extensions list and drag it to the Available Extensions list. Click the left arrow to remove it. • To add all the extensions to the Selected Extensions list, click the right double-arrow. • To delete all the extensions from the Selected Extensions list, click the left double-arrow.

Directory Services

Cisco Configuration Professional automatically creates a local phone directory containing the telephone numbers that are assigned in the directory entry number configuration of the phone.

You can make additional entries to the local directory in telephony services configuration mode. Additional entries can be nonlocal numbers such as telephone numbers on other Cisco systems used by your company.

Note Directory Services is supported with SIP endpoints.

Directory Services Reference

The following topics describe the window used to configure Directory Services:

- Configure Directory Services, page 59-16
- Create or Edit a Directory Entry, page 59-17

Configure Directory Services

You can make additional entries to the local directory. Additional entries can be nonlocal numbers such as telephone numbers on other Cisco systems used by your company.

How to get to this screen

Click **Configure > Unified Communications > Telephony Features > Directory Services**.

Related Link

- Create or Edit a Directory Entry, page 59-17

Field Reference

Table 59-7 Configure Directory Services

Element	Description
Directory Entry Position	A unique system-level directory entry number that supports a maximum of 100 entries. The range is from 1 to 100.
Name	The name associated with the directory number.
Phone Number	The extension associated with the dial position and name.

Create or Edit a Directory Entry

Enter or modify the settings for directory services.

How to get to this screen

- Click **Configure > Unified Communications > Telephony Features > Directory Services > Create**.
- Click **Configure > Unified Communications > Telephony Features > Directory Services > Edit**.

Related Link

- Configure Directory Services, page 59-16

Field Reference

Table 59-8 Create or Edit Directory Services

Element	Description
Directory Entry Position	A unique system-level directory entry number that supports a maximum of 100 entries. The range is from 1 to 100.
Name	The name associated with the directory entry number.
Phone Number	The extension associated with the directory entry position and name.

Hunt Groups

Hunt groups allow the incoming calls on a specific number (pilot number) to be directed to a defined group (list) of numbers.

The first number that receives the incoming call is determined by the type of hunt group you selected and the order in which the numbers in the hunt group are listed. If the first number is busy or does not answer, the call is redirected to the next number in the list. The call continues to be redirected, until it is answered, or until the call reaches the number that is defined as the final number.

There are four types of hunt groups - Parallel, Peer, Longest Idle, and Sequential.

- Parallel (Call Blast)—Call rings all numbers in the hunt group simultaneously.

  Note The Parallel hunt group type is available on Cisco Unified CME 4.3 or higher versions.

- Peer— first number to ring is the number to the right of the directory number that was the last to ring when the pilot number was last called. Ringing proceeds in a circular manner, left to right, for the number of hops specified in the hunt group configuration.
- Longest Idle—Call first goes to the number that has been idle the longest, for the number of hops specified in the hunt group configuration. The longest idle time is determined from the last time that a phone registered, reregistered, or went on-hook.
- Sequential—Numbers always ring in the left-to-right order in which they are listed in the hunt group configuration. The first number in the list is always the first number to be tried when the pilot number is called.

Note Maximum number of hops applies to Peer and Longest Idle hunt group types only.

Note SIP extensions are listed only for parallel hunt groups.

To configure hunt groups, choose **Configure > Unified Communications > Telephony Features > Hunt Groups**.

Related Topics

- Working with Hunt Groups, page 59-19
- Hunt Groups Reference, page 59-22

Working with Hunt Groups

This section contains the following topics:

- Creating Hunt Groups, page 59-19
- Editing Hunt Groups, page 59-20
- Deleting Hunt Groups, page 59-20

Creating Hunt Groups

Before You Begin

Make sure you have configured extension numbers. See Extensions, page 56-2.

Procedure

Use this procedure to create hunt groups.

Step 1 Choose **Configure > Unified Communications > Telephony Features > Hunt Groups** to open the Hunt Groups summary page. See Hunt Groups Summary Page, page 59-22.

Step 2 Click **Create** to open the Create Hunt Groups page.

Step 3 Click the General tab, and then enter the information in the fields provided. See Create or Edit a Hunt Group—General Tab, page 59-24.

Step 4 Click the Advanced tab, and then enter the information in the fields provided. See Create or Edit a Hunt Group—Advanced Tab, page 59-29.

Step 5 Click **OK**.

Related Topics

- Hunt Groups, page 59-18

- Editing Hunt Groups, page 59-20
- Deleting Hunt Groups, page 59-20

Editing Hunt Groups

Before You Begin

Make sure you have created hunt groups. See Creating Hunt Groups, page 59-19.

Procedure

Use this procedure to modify the parameters that are configured on a selected hunt group.

Step 1 Choose **Configure > Unified Communications > Telephony Features > Hunt Groups** to open the Hunt Groups summary page. See Hunt Groups Summary Page, page 59-22.

Step 2 Choose a row and click **Edit** to open the Edit Hunt Groups page.

Step 3 Click the General tab and change the parameters to modify. See Create or Edit a Hunt Group—General Tab, page 59-24.

Step 4 Click the Advanced tab and change the parameters to modify. See Create or Edit a Hunt Group—Advanced Tab, page 59-29.

Step 5 Click **OK**.

Related Topics

- Hunt Groups, page 59-18
- Creating Hunt Groups, page 59-19
- Deleting Hunt Groups, page 59-20

Deleting Hunt Groups

Before You Begin

Make sure you have created hunt groups. See Creating Hunt Groups, page 59-19.

Procedure

Use this procedure to delete hunt groups.

Step 1 Choose **Configure > Unified Communications > Telephony Features > Hunt Groups** to open the Hunt Groups summary page. See Hunt Groups Summary Page, page 59-22.

Step 2 Select a single row or multiple rows, and then click **Delete** to open a confirmation dialog box.

Step 3 Click **Yes** in the confirmation dialog box.

Related Topics

- Hunt Groups, page 59-18
- Creating Hunt Groups, page 59-19
- Editing Hunt Groups, page 59-20

Hunt Groups Reference

The following topics describe the Hunt Group pages and dialog boxes used to configure hunt groups:

- Hunt Groups Summary Page
- Create or Edit a Hunt Group—General Tab
- Set Extension Timeout Dialog Box
- Create or Edit a Hunt Group—Advanced Tab

Hunt Groups Summary Page

Use the Hunt Groups summary page to view the hunt groups that are configured, to create new hunt groups, to modify parameters on a selected hunt group, and to delete hunt groups.

How to Get to this Page

Click **Configure > Unified Communications > Telephony Features > Hunt Groups**.

Related Topics

- Hunt Groups, page 59-18
- Creating Hunt Groups, page 59-19
- Editing Hunt Groups, page 59-20
- Deleting Hunt Groups, page 59-20
- Create or Edit a Hunt Group—General Tab, page 59-24
- Set Extension Timeout Dialog Box, page 59-28
- Create or Edit a Hunt Group—Advanced Tab, page 59-29

Field Reference

Table 59-9 Hunt Groups Summary Page

Element	Description
Pilot Number	Number the callers dial to reach the hunt group.
Type	The type of hunt group. The hunt group types displayed could be any or all of the following: • Parallel (Call Blast)—Call rings all numbers in the hunt group simultaneously. **Note** The Parallel hunt group type is available on Cisco Unified CME 4.3 or higher versions. • Peer—First number to ring is the number to the right of the directory number that was the last to ring when the pilot number was last called. Ringing proceeds in a circular manner, left to right, for the number of hops specified in the hunt group configuration. • Longest Idle—Call first goes to the number that has been idle the longest, for the number of hops specified in the hunt group configuration. The longest idle time is determined from the last time that a phone registered, reregistered, or went on-hook. • Sequential—Numbers always ring in the left-to-right order in which they are listed in the hunt group configuration. The first number in the list is always the first number to be tried when the pilot number is called. **Note** Maximum number of hops applies to Peer and Longest Idle hunt group types only.
Description	Description of the hunt group that appears on the called extension.
List Members	The list size (member count) of the configured hunt group members.
Create button	Click this button to open the Create Hunt Groups page. From this page you can create a new hunt group. See Create or Edit a Hunt Group—General Tab, page 59-24 and Create or Edit a Hunt Group—Advanced Tab, page 59-29.

Table 59-9 Hunt Groups Summary Page (continued)

Element	Description
Edit button	Click this button to modify the parameters that are configured on a selected hunt group. When you click this button, the Edit Hunt Group page appears, in which you can edit the parameters that are configured on the selected hunt group. See Create or Edit a Hunt Group—General Tab, page 59-24 and Create or Edit a Hunt Group—Advanced Tab, page 59-29.
Delete button	Click this button to delete selected hunt groups.

Create or Edit a Hunt Group Dialog Box

See the following topics as appropriate:

- Create or Edit a Hunt Group—General Tab, page 59-24
- Create or Edit a Hunt Group—Advanced Tab, page 59-29

Create or Edit a Hunt Group—General Tab

In the General tab, enter the basic hunt group parameters.

How to Get to this Page

- Click **Configure > Unified Communications > Telephony Features > Hunt Groups > Create > General** tab.
- Click **Configure > Unified Communications > Telephony Features > Hunt Groups > Edit > General** tab.

Related Topics

- Hunt Groups, page 59-18
- Creating Hunt Groups, page 59-19
- Editing Hunt Groups, page 59-20
- Deleting Hunt Groups, page 59-20

- Hunt Groups Summary Page, page 59-22
- Set Extension Timeout Dialog Box, page 59-28
- Create or Edit a Hunt Group—Advanced Tab, page 59-29

Field Reference

Table 59-10 General Tab

Element	Description
Pilot number	Enter a unique pilot number that callers dial to reach the hunt group. This number must be unique throughout the system. You can enter from 1 to 24 alphanumeric characters.
Description	Enter a description for the hunt group. The text appears in the configuration output and on IP phones that are members of a hunt group when they receive hunt-group calls. You can enter a maximum of 29 characters.
Forward call to	Select the disposition of the call at the end of the call forwarding process as follows: • Originating Number forwards the call to the directory number of the phone that transferred the call into the hunt group. • Final Number forwards the call to the final number in the hunt group.
Final number	Enter the final directory number in the hunt group or an extension number. It must be either the voice mail number or the number of some other application, such as Cisco IP Auto Attendant, that can accept multiple inbound calls simultaneously. You can enter from 1 to 30 alphanumeric characters.

Table 59-10 General Tab (continued)

Element	Description
Type	Type of hunt group. Click the drop-down list to choose a hunt group type. The options are: • Parallel (Call Blast)—Call rings all numbers in the hunt group simultaneously. **Note** The Parallel hunt group type is available on Cisco Unified CME 4.3 or higher versions. • Peer—The first number to ring is the number to the right of the directory number that was the last to ring when the pilot number was last called. Ringing proceeds in a circular manner, left to right, for the number of hops specified in the hunt group configuration. • Longest Idle—Call first goes to the number that has been idle the longest, for the number of hops specified in the hunt group configuration. The longest idle time is determined from the last time that a phone registered, reregistered, or went on-hook. • Sequential—Numbers always ring in the left-to-right order in which they are listed in the hunt group configuration. The first number in the list is always the first number to be tried when the pilot number is called. **Note** Maximum number of hops applies to Peer and Longest Idle hunt group types only.

Table 59-10 General Tab (continued)

Element	Description
List Members area	Contains two panes: Available Numbers pane and Selected Numbers pane. • Available Numbers (left pane)—Lists the available extension numbers. • Selected Numbers (right pane)—Lists the extension and non-extension numbers that you added from the Available Numbers pane and the Other Number field into the Selected Numbers pane. **Note** You can add a maximum of 32 numbers for Parallel hunt group type. You can add a maximum of 20 numbers for Peer, Longest Idle, and Sequential hunt group types. You can add or remove numbers from the Selected Numbers pane by using the arrow buttons or by using the drag and drop feature. • To add the number, do one of the following: – Use the arrow buttons—Select a number from the Available Numbers list, and then click the > button. The extension number is added to the Selected Numbers list. To add all the extension numbers, click the >> button. – Use the drag and drop feature—Select the number or numbers from the Available Numbers list, and then drag and drop it into the Selected Numbers list pane. • To remove the number, do one of the following: – Use the arrow buttons—Select the number from the Selected Numbers list, and then click the < button. The extension number is removed from the Selected Numbers list. To remove all the numbers from the Selected Extensions list, click the << button. – Use the drag and drop feature—Select the number or numbers from the Selected Numbers list, and then drag and drop it into the Available Numbers list pane.

Table 59-10 General Tab (continued)

Element	Description
Other number	A non-extension number. You can enter a non-extension number to the hunt group list. This field appears when you choose the **Parallel** hunt group type in the Type field. You can enter a maximum of 32-digits. The non-extension numbers can be for any of the following phone types: SIP phone, FXS analog phone, DS0-group, PRI-group, or SIP trunk. You can also choose to add a cell phone number as a member of the hunt group. To do so, connect the incoming calls to the cell number through an FXO port in which the destination matches the.T wild card pattern.
Add to Selected Numbers button	Click this button to move the non-extension number from the Other Number field into the Selected Numbers pane. The Add to Selected Numbers button is displayed when you choose the Parallel hunt group type in the Type field. This button is enabled when you enter a non-extension number in the Other Number field.
Set Extension Timeout button	Click this button to open the Set Extension Timeout dialog box where you can configure the number of seconds the call must wait on a selected extension number before it moves to the next extension number. See Set Extension Timeout Dialog Box, page 59-28. The Set Extension Timeout button is displayed when you choose the Peer, Longest Idle, or Sequential hunt group type in the Type field. This button is enabled when you add extension numbers to the Selected Numbers area.

Set Extension Timeout Dialog Box

Display, enter, or modify the time outs for selected extensions.

How to Get to this Dialog Box

- Click **Configure > Unified Communications > Telephony Features > Hunt Groups > Edit > General** tab > **Set Extension Timeout**.
- Click **Configure > Unified Communications > Telephony Features > Hunt Groups > Create > General** tab > **Set Extension Timeout**.

Related Topics

- Hunt Groups Summary Page, page 59-22
- Create or Edit a Hunt Group—General Tab, page 59-24
- Create or Edit a Hunt Group—Advanced Tab, page 59-29

Field Reference

Table 59-11 Set Extension Timeout

Element	Description
Extension	Select the extension number for which you want to set the timeout value from the drop-down list.
Timeout	Enter the number of seconds. If the selected extension number has a timeout value configured, that value displays in the Timeout field. The range is 3 to 60000 seconds. Default timeout value is 180 seconds.

Create or Edit a Hunt Group—Advanced Tab

In the Advanced tab, enter the advanced hunt group parameters, such as the primary and secondary pilot number preference, maximum timeout value, number of hops, and so on.

How to Get to this Page

- Click **Configure > Unified Communications > Telephony Features > Hunt Groups > Create > Advanced** tab.
- Click **Configure > Telephony Features > Hunt Groups > Edit > Advanced** tab.

Related Topics

- Hunt Groups, page 59-18
- Creating Hunt Groups, page 59-19
- Editing Hunt Groups, page 59-20
- Deleting Hunt Groups, page 59-20

- Hunt Groups Summary Page, page 59-22
- Create or Edit a Hunt Group—General Tab, page 59-24
- Set Extension Timeout Dialog Box, page 59-28

Field Reference

Table 59-12 Advanced Tab

Element	Description
Primary pilot number preference	Select the preference order for the pilot number.
Secondary pilot number	Enter the backup number that callers dial to enter the hunt group. You can enter a maximum of 24 alphanumeric characters.
Secondary pilot number preference	Select the preference order for the backup number that callers dial to enter the hunt group.
Maximum timeout	Enter the maximum total timeout for all the no-answer periods for all numbers in the hunt group. The call proceeds to the final destination when this timeout period expires, regardless of whether or not it has completed the hunt cycle. The value can be from 3 to 60000 seconds.
Maximum hops	Enter the number of hops before the call proceeds to the final number. The value must be less than or equal to the number of numbers that are specified in the list. If the number is not set, the system defaults to the number of hunt group members. You can enter a maximum of 20 hops. **Note** Maximum number of hops applies to Peer and Longest Idle hunt group types only. This field is disabled for Sequential and Parallel hunt group types.
Unanswered call message	Enter the message to be displayed on the unanswered phones when a phone goes unanswered. You can enter a maximum of 29 characters. **Note** This field is disabled for Parallel hunt group type.

Table 59-12 Advanced Tab (continued)

Element	Description
Present call to	Choose to present hunt group calls only to member phones that are idle or onhook. Idle Phone—The hunt group call is directed to this phone only if all lines on the phone are idle. Onhook Phone—The hunt group call is directed to a phone only if the phone is in on-hook state. **Note** This field is disabled for Parallel hunt group type.
Update on-hook timestamps when	Choose to update the on-hook time stamp when a call is answered or a call is answered and an extension rings. **Note** Applies to the Longest Idle hunt group type only. This field is disabled for all other group types.

Intercom

You can configure two types of intercom lines: Regular Intercom and Whisper Intercom.

Regular Intercom

A regular intercom line is a dedicated two-way audio path between two phones. When an intercom speed-dial button is pressed, the call is speed-dialed to the other half of the dedicated pair. The called phone automatically answers the call in speakerphone mode with mute activated, which provides a one-way voice path from the initiator to the recipient. A beep is heard when the call is auto-answered to alert the recipient of the incoming call.

Intercom lines cannot be used in shared-line configurations. If a directory number is configured for intercom, it must be associated with one IP phone only. The intercom feature causes an IP phone line to operate as an autodial line for outbound calls and as an autoanswer-with-mute line for inbound calls.

To prevent an unauthorized phone from dialing an intercom line (and creating a situation in which a phone automatically answers a call other than an intercom call), you can assign the intercom extension number that includes an alphabetic character, for example, A5001. An alphabetic character cannot be dialed from a typical phone, but the phone at the other end of the intercom can be configured to dial the number that contains the alphabetic character through the Cisco Unified CME router.

Whisper Intercom

When a phone user dials a whisper intercom line, the called phone automatically answers using speakerphone mode, providing a one-way voice path from the caller to the called party, regardless of whether the called party is busy or idle.

Unlike the regular intercom feature, this feature allows an intercom call to a busy extension. The calling party can only be heard by the recipient. The original caller on the receiving phone does not hear the whisper page. The phone receiving the whisper page displays the extension and name of the party initiating the whisper page, and Cisco Unified CME plays a zip zip tone before the called party hears the caller's voice. If the called party wants to speak to the caller, the called party selects the intercom line button on their phone. The lamp for intercom buttons is colored amber to indicate one-way audio for whisper intercom and green to indicate two-way audio for standard intercom.

You must configure a whisper intercom directory number for each phone that requires the Whisper Intercom feature. A whisper intercom directory number can place calls only to another whisper intercom directory number. Calls between a whisper intercom directory number and a standard directory number or intercom directory number are rejected with a busy tone.

Note

- The Whisper Intercom feature is supported in Cisco Unified CME 7.1 and later versions.
- The Whisper Intercom feature is supported on IP phones that have SCCP 12.0 or later versions.
- The Whisper Intercom feature is not supported on phone models that use single-line mode, for example, Cisco Unified IP phone models 7906 and 7911.

Note SIP extensions and phones are not listed for intercoms.

To configure regular or whisper intercom lines, choose **Configure > Unified Communications > Telephony Features > Intercom**.

Related Topics

- Creating, Editing, and Deleting a Regular Intercom Line, page 59-33
- Creating, Editing, and Deleting a Whisper Intercom Line, page 59-35
- Intercom Reference, page 59-37

Creating, Editing, and Deleting a Regular Intercom Line

Before You Begin

Make sure you have defined a user, and have associated that user with a phone and extensions. See Creating, Editing, Deleting, Restarting, and Resetting Phones and Users, page 56-22.

Procedure

Use this procedure to create, edit, or delete a regular intercom line.

Step 1 Choose **Configure > Unified Communications > Telephony Features > Intercom** to open the Intercom summary page. See Intercom Summary Page, page 59-37.

Step 2 To create a regular intercom line, click **Create**. The Setup New Intercom Line dialog box opens. See Setup New Intercom Line or Edit Intercom Dialog Box, page 59-38.

a. From the First Phone area (left pane), enter the parameters for the first phone. Do the following:

- Choose the phone user and the speed dial button, and then enter the able to display on the phone line button.
- The **Automatically Answer Call in Speaker Phone Mode** and **Mute Phone When Auto Answering** check boxes are checked by default.

Note If you uncheck the **Automatically Answer Call in Speaker Phone Mode** check box, the Mute Phone When Auto Answering check box and the Put Existing Call on Hold When this Intercom Call Comes In check box are not displayed.

- To put the existing call on hold when the intercom call is received, check the **Put Existing Call on Hold When this Intercom Call Comes In** check box.

b. From the Second Phone area (right pane), enter the parameters for the second phone. Do the following:

- Choose the phone user and the speed dial button, and then enter the label to display on the phone line button.
- The **Automatically Answer Call in Speaker Phone Mode** and **Mute Phone When Auto Answering** check boxes are checked by default.

Note If you uncheck the **Automatically Answer Call in Speaker Phone Mode** check box, the Mute Phone When Auto Answering check box and the Put Existing Call on Hold When this Intercom Call Comes In check box are not displayed.

- To put the existing call on hold when the intercom call is received, check the **Put Existing Call on Hold When this Intercom Call Comes In** check box.

c. Click **OK**.

See Setup New Intercom Line or Edit Intercom Dialog Box, page 59-38.

Step 3 To edit an intercom line, choose the intercom row for which you want to modify the parameters, and then click **Edit**. The Edit Intercom dialog box opens. Change the parameters that you want to modify, and then click **OK**. See Setup New Intercom Line or Edit Intercom Dialog Box, page 59-38.

Step 4 To delete an intercom line, choose the intercom row or rows that you want to delete, and then click **Delete**. A confirmation dialog box opens. Click **Yes** in the confirmation dialog box.

Related Topics

- Intercom, page 59-31
- Creating, Editing, and Deleting a Whisper Intercom Line, page 59-35
- Intercom Reference, page 59-37

Creating, Editing, and Deleting a Whisper Intercom Line

You can create the following whisper intercom lines: whisper intercom with speed dial, whisper intercom with partial speed dial, and open-ended whisper intercom.

Before You Begin

Make sure you have defined a user, and have associated that user with a phone and extensions. See Creating, Editing, Deleting, Restarting, and Resetting Phones and Users, page 56-22.

Procedure

Use this procedure to create, edit, or delete a whisper intercom line.

Step 1 Choose **Configure > Unified Communications > Telephony Features > Intercom** to open the Intercom summary page. See Intercom Summary Page, page 59-37.

Step 2 To create a whisper intercom with speed dial, do the following:

a. Click **Create**. The Setup New Intercom Line dialog box opens. See Setup New Intercom Line or Edit Intercom Dialog Box, page 59-38.

b. Check the **Enable Whisper Mode** check box.

c. From the First Phone area (left pane), choose the phone user and the speed dial button; and then enter the label to display on the phone line button and the intercom number. Check the **Enable Speed Dial Configuration From this Phone to Second Phone** check box. This check box is checked by default.

d. From the Second Phone area (left pane), choose the phone user and the speed dial button; and then enter the label to display on the phone line button and the intercom number. Check the **Enable Speed Dial Configuration From this Phone to First Phone** check box. This check box is checked by default.

e. Click **OK**.

Step 3 To create a whisper intercom line with partial speed dial, do the following:

a. Click **Create**. The Setup New Intercom Line dialog box opens. See Setup New Intercom Line or Edit Intercom Dialog Box, page 59-38.

b. Check the **Enable Whisper Mode** check box.

c. From the First Phone area (left pane), choose the phone user and the speed dial button; and then enter the name to display on the phone line button and the intercom number. Check the **Enable Speed Dial Configuration From this Phone to Second Phone** check box.

d. From the Second Phone area (left pane), choose the phone user and the speed dial button; and then enter the name to display on the phone line button and the intercom number. Uncheck the **Enable Speed Dial Configuration From this Phone to First Phone** check box.

e. Click **OK**.

Step 4 To create an open-ended whisper intercom line, do the following:

a. Click **Create**. The Setup New Intercom Line dialog box opens. See Setup New Intercom Line or Edit Intercom Dialog Box, page 59-38.

b. Check the **Enable Whisper Mode** check box.

c. From the First Phone area (left pane), choose the phone user and the speed dial button; and then enter the name to display on the phone line button and the intercom number. Uncheck the **Enable Speed Dial Configuration From this Phone to Second Phone** check box.

Note When you uncheck the **Enable Speed Dial Configuration From this Phone to Second Phone** check box, all the fields in the Second Phone area are greyed out.

d. Click **OK**.

Step 5 To edit a whisper intercom line, choose the intercom row for which you want to modify the parameters, and then click **Edit**. The Edit Intercom dialog box opens. Change the parameters that you want to modify, and then click **OK**. See Setup New Intercom Line or Edit Intercom Dialog Box, page 59-38.

Step 6 To delete a whisper intercom line, choose an intercom row or rows that you want to delete, and then click **Delete**. A confirmation dialog box opens. Click **Yes** in the confirmation dialog box.

Related Topics

- Intercom, page 59-31
- Creating, Editing, and Deleting a Regular Intercom Line, page 59-33
- Intercom Reference, page 59-37

Intercom Reference

The following topics describe the Intercom pages and dialog boxes used to configure intercoms:

- Intercom Summary Page, page 59-37
- Setup New Intercom Line or Edit Intercom Dialog Box, page 59-38

Intercom Summary Page

Use the Intercom summary page to view the intercoms that are configured, to setup a new intercom line, to modify the parameters of a selected intercom line, and to delete intercoms.

How to Get to This Page

Click **Configure > Unified Communications >Telephony Features > Intercom**.

Related Link

- Setup New Intercom Line or Edit Intercom Dialog Box, page 59-38
- Creating, Editing, and Deleting a Regular Intercom Line, page 59-33
- Creating, Editing, and Deleting a Whisper Intercom Line, page 59-35
- Intercom, page 59-31

Field Reference

Table 59-13 Intercom Summary Page

Element	Description
Intercom Type	Displays the type of Intercom configured for the user: Regular Intercom or Whisper Intercom.
First Phone	Phone user who is associated with the first number of the intercom connection.
User 1 Phone Button	Button number assigned to the intercom number.
Second Phone	Phone user associated with the second number of the intercom connection.
User 2 Phone Button	Button number assigned to the intercom number.
Create button	Click this button to open the Setup an Intercom Line dialog box, in which you can set up a new intercom line. See Setup New Intercom Line or Edit Intercom Dialog Box, page 59-38.
Edit button	Click this button to open the Edit Intercom dialog box, in which you can edit the parameters that are configured for a selected intercom line. See Setup New Intercom Line or Edit Intercom Dialog Box, page 59-38.
Delete button	Click this button to delete selected intercom lines.

Setup New Intercom Line or Edit Intercom Dialog Box

Use the Setup New Intercom Line or Edit Intercom dialog box to set up a new intercom line or to modify the parameters of a selected intercom line.

How to Get to This Page

- Click **Configure > Unified Communications > Telephony Features > Intercom > Create**.
- Click **Configure > Unified Communications >Telephony Features > Intercom > Edit**.

Related Link

- Intercom Summary Page, page 59-37
- Creating, Editing, and Deleting a Regular Intercom Line, page 59-33
- Creating, Editing, and Deleting a Whisper Intercom Line, page 59-35
- Intercom, page 59-31

Field Reference

Table 59-14 Setup New Intercom Line or Edit Intercom Dialog Box

Element	Description
Enable Whisper Mode check box	Check this check box to enable the Whisper Intercom feature. See Whisper Intercom, page 59-32. **Note** The Whisper Intercom feature is supported in Cisco Unified CME 7.1 and later versions. If the router you are configuring has previous versions of Cisco Unified CME installed on it, this check box is greyed out. When this check box is checked, the fields and check boxes that apply to the Whisper Intercom feature are displayed in the First Phone and the Second Phone areas.
First Phone—Left Pane	
Phone User	Phone user associated with the first number of the intercom connection. Choose the user ID from the drop-down list. When you check the **Enable Whisper Mode** check box, the list of users that have phones that support the Whisper Intercom feature are displayed in the drop-down list. **Note** The Whisper Intercom feature is supported on IP phones that have SCCP 12.0 or later versions.
Speed Dial Button for this Call	Button number assigned to the intercom number. Choose the number from the drop-down list.
Label Display on Phone Line Button	Name that appears in the caller-ID display and in the local directory that is associated with the intercom extension number.

Table 59-14 Setup New Intercom Line or Edit Intercom Dialog Box (continued)

Element	Description
Automatically Answer Call in Speaker Phone Mode check box	**Note** This field is displayed when you are configuring a regular intercom. Check this check box to enable the phone that receives the call to automatically answer the call in speakerphone mode with mute activated. This feature provides a one-way voice path from the initiator to the recipient.
Mute Phone When Auto Answering check box	**Note** This field is displayed when you are configuring a regular intercom. Check this check box to answer the call in speakerphone mode with mute activated. If you uncheck the Automatically Answer Call in Speaker Phone Mode check box, this check box is not displayed.
Put Existing Call on Hold When this Intercom Call Comes In check box	**Note** This field is displayed when you are configuring a regular intercom. Check this check box to put the existing call on hold when the intercom call is received. If you uncheck the Automatically Answer Call in Speaker Phone Mode check box, this check box is not displayed.
Intercom Number	**Note** This field is displayed when you are configuring a whisper intercom. The intercom number assigned to the whisper intercom. Range is 1 to 15 digits. Only numbers are allowed.

Table 59-14 Setup New Intercom Line or Edit Intercom Dialog Box (continued)

Element	Description
Enable Speed Dial Configuration From this Phone to Second Phone check box	**Note** This field is displayed when you are configuring a whisper intercom. • To configure a whisper intercom with speed dial: – From the First Phone area, check the **Enable Speed Dial Configuration From this Phone to Second Phone** check box. – From the Second Phone area, check the **Enable Speed Dial Configuration From this Phone to First Phone** check box. • To configure a whisper intercom with partial speed dial: – From the First Phone area, check the **Enable Speed Dial Configuration From this Phone to Second Phone** check box. – From the Second Phone area, uncheck the **Enable Speed Dial Configuration From this Phone to First Phone** check box. • To configure an open-ended whisper intercom: – From the First Phone area, uncheck the **Enable Speed Dial Configuration From this Phone to Second Phone** check box. When you uncheck this check box from the First Phone area, the fields in the Second Phone area are greyed out.
Second Phone—Right Pane	
Phone User	The phone user associated with the second number of the intercom connection. Choose the user ID from the drop-down list. When you check the Enable Whisper Mode check box, the list of users that have phones that support the Whisper Intercom feature are displayed in the drop-down list. **Note** The Whisper Intercom feature is supported on IP phones that have SCCP 12.0 or later versions.
Speed Dial Button for this Call	The button number assigned to the intercom number. Choose the number from the drop-down list.
Label Display on Phone Line Button	The name that appears in the caller-ID display and in the local directory that is associated with the intercom extension number.

Table 59-14 Setup New Intercom Line or Edit Intercom Dialog Box (continued)

Element	Description
Automatically Answer Call in Speaker Phone Mode check box	**Note** This field is displayed when you are configuring a regular intercom. Check this check box to enable the phone that receives the call to automatically answer the call in speakerphone mode with mute activated. This provides a one-way voice path from the initiator to the recipient.
Mute Phone When Auto Answering check box	**Note** This field is displayed when you are configuring a regular intercom. Check this check box to answer the call in speakerphone mode with mute activated. If you uncheck the Automatically Answer Call in Speaker Phone Mode check box, this check box is not displayed.
Put Existing Call on Hold When this Intercom Call Comes In check box	**Note** This field is displayed when you are configuring a regular intercom. Check this check box to put the existing call on hold when the intercom call is received. If you uncheck the Automatically Answer Call in Speaker Phone Mode check box, this check box is not displayed.
Intercom Number	**Note** This field is displayed when you are configuring a whisper intercom. The intercom number assigned to the whisper intercom. Range is 1 to 15 digits. No characters are allowed.

Table 59-14 Setup New Intercom Line or Edit Intercom Dialog Box (continued)

Element	Description
Enable Speed Dial Configuration From this Phone to First Phone check box	This field is displayed when you are configuring whisper intercom. • To configure whisper intercom with speed dial, do the following: – From the First Phone area, check the **Enable Speed Dial Configuration From this Phone to Second Phone** check box. – From the Second Phone area, check the **Enable Speed Dial Configuration From this Phone to First Phone** check box. • To configure whisper intercom with partial speed dial, do the following: – From the First Phone area, check the **Enable Speed Dial Configuration From this Phone to Second Phone** check box. – From the Second Phone area, uncheck the **Enable Speed Dial Configuration From this Phone to First Phone** check box. • To configure open-ended whisper intercom, do the following: – From the First Phone area, uncheck the **Enable Speed Dial Configuration From this Phone to Second Phone** check box. When you uncheck this check box from the First Phone area, the fields in the Second Phone area are greyed out.
OK button	Click this button to apply the intercom configuration to the router.
Cancel button	Click this button to discard the configuration values that you entered.

Night Service Bell

Silent ringing is overridden when **night service** is active. It allows you to provide coverage for unstaffed extensions during hours that you designate as "night-service" hours. During the night-service hours, calls to the designated extensions (known as night-service directory numbers or night-service lines) send a special "burst" ring to phones that have been specified to receive this special ring (the phones are known as night-service phones). Phone users at the night-service phones can then use the call-pickup feature to answer the incoming calls from the night-service directory numbers

You can configure silent ring on any type of phone. However, you typically set silent ring only on buttons of a phone with multiple lines, such as a Cisco Unified IP Phone 7940, Cisco Unified IP Phones 7960 and 7960G, or a Cisco Unified IP Phone 7914 Expansion Module. The only visible cue is a flashing ((< icon in the phone display.

If you configure a button to have a silent ring, you will not hear a call-waiting beep or call-waiting ring regardless of whether the number associated with the button is configured to generate a call-waiting beep or call-waiting ring.

In Cisco IOS Release 12.4(4)XC and later releases, the silent ringing behavior is overridden during active night-service periods.

Note Night service bell is supported with SIP endpoints.

Night Service Bell Reference

The following topics describe the window used to manage silent ringing when night service is active:

- Configuring Night Service Weekly Schedule, page 59-45
- Configuring Night Service Annual Schedule, page 59-46
- Configuring Night Service Daily Schedule, page 59-47
- Configuring Night Service Code, page 59-48

Configure Night Service Bell

To manage silent ringing when night service is active, follow the instructions in these sections:

- Configuring Night Service Weekly Schedule, page 59-45
- Configuring Night Service Annual Schedule, page 59-46
- Configuring Night Service Daily Schedule, page 59-47
- Configuring Night Service Code, page 59-48

Configuring Night Service Weekly Schedule

A weekly schedule cycles every week.

How to get to this screen

Click **Configure > Unified Communications > Telephony Features > Night Service Bell > Weekly Schedule**.

Configure a Weekly Schedule

To configure a weekly schedule, perform these steps:

Step 1 Click **Configure > Unified Communications > Telephony Features > Night Service Bell > Weekly Schedule**. Cisco Configuration Professional displays the Configure Night Service Weekly Schedule screen.

Step 2 To set the start and stop times:

- Select the hour or the minute under the desired day of the week and use the arrows to change the time.
- To toggle between ante meridiem and post meridiem, select **am** or **pm** and use the arrows to change the setting.

To set the start and stop time for length of the entire day, check **All Day**.

Copying a Weekly Schedule

To copy a weekly schedule, perform these steps:

Step 1 Click **Configure > Unified Communications > Telephony Features > Night Service Bell > Weekly Schedule**. Cisco Configuration Professional displays the Configure Night Service Weekly Schedule screen.

Step 2 Choose a day from the Copy schedule **from** list.

Step 3 Choose a day from the Copy schedule **to** list.

Step 4 Click **Copy**.

Related Links

- Configuring Night Service Annual Schedule, page 59-46
- Configuring Night Service Daily Schedule, page 59-47
- Configuring Night Service Code, page 59-48

Configuring Night Service Annual Schedule

An annual schedule specifies the days to which the parameters are applied.

How to get to this screen

Click **Configure > Unified Communications > Telephony Features > Night Service Bell > Annual Schedule**.

How to use this screen

To add a day for Night Service Bell to the annual schedule, perform these steps:

Step 1 In the Configure tree, click **Configure > Unified Communications > Telephony Features > Night Service Bell > Annual Schedule**. Cisco Configuration Professional displays the Configure Night Service Annual Schedule screen.

Step 2 To choose the desired month, click the arrow keys on the calendar.

Step 3 To choose the desired day of the month, click the day of the month on the calendar.

Step 4 To set the start and stop times:

- Select the hour or the minute under the desired day of the week and use the arrows to change the time.
- To toggle between ante meridiem and post meridiem, select **am** or **pm** and use the arrows to change the setting.

Step 5 Click **Add**.

To set the start and stop time for length of the entire day, check **All Day**.

Related Links

- Configuring Night Service Weekly Schedule, page 59-45
- Configuring Night Service Daily Schedule, page 59-47
- Configuring Night Service Code, page 59-48

Configuring Night Service Daily Schedule

A night service bell can be scheduled for every day of the week.

How to get to this screen

Click **Configure > Unified Communications > Telephony Features > Night Service Bell > Daily Schedule**.

How to use this screen

To configure a daily schedule, perform these steps:

Step 1 Click **Configure > Unified Communications > Telephony Features > Night Service Bell > Daily Schedule**. Cisco Configuration Professional displays the Configure Night Service Daily Schedule screen.

Step 2 Check Enable daily schedule override. To disable this night service, uncheck the check box.

Step 3 To set the start and stop times:

- Select the hour or the minute under the desired day of the week and use the arrows to change the time.

- To toggle between ante meridiem and post meridiem, select **am** or **pm** and use the arrows to change the setting.

Related Links

- Configuring Night Service Weekly Schedule, page 59-45
- Configuring Night Service Annual Schedule, page 59-46
- Configuring Night Service Code, page 59-48

Configuring Night Service Code

The night service code is used to temporarily enable or disable night service. There is one code for all the phones. Dialing the same code toggles the service on or off.

How to get to this screen

Click **Configure > Unified Communications > Telephony Features > Night Service Bell > Code**.

How to use this screen

To configure a night service code, perform these steps:

Step 1 In the Configure tree, click **Configure > Unified Communications > Telephony Features > Night Service Bell > Code**. Cisco Configuration Professional displays the Night Service: Code screen.

Step 2 Check Enable Night Service Code. To disable the night service code, uncheck the check box.

Step 3 Enter the night service code. The first character must be an asterisk (*), followed by a maximum of 16 digits. For example, the default is *1234.

Related Links

- Configuring Night Service Weekly Schedule, page 59-45
- Configuring Night Service Annual Schedule, page 59-46
- Configuring Night Service Daily Schedule, page 59-47

Paging Numbers

When a paging number is called, it relays an audio page to a group of designated phones. When a caller dials the paging number, each idle IP phone that has been configured with the paging number automatically answers using its speakerphone mode. Displays on the phones that answer the page show the caller ID that has been set under the paging number. When the caller finishes speaking the message and hangs up, the phones return to their idle states.

Audio paging provides a one-way voice path to the phones that have been designated to receive paging. It does not have a press-to-answer option like the intercom feature. The paging number can be dialed from anywhere, including on-net.

Note Paging numbers is supported with SCCP and SCCP and SIP endpoints but SIP phones are not listed.

Related Topics

- Creating, Editing, and Deleting a Paging Number, page 59-49
- Paging Numbers Reference, page 59-51

Creating, Editing, and Deleting a Paging Number

Before You Begin

Make sure you have configured a phone. See Create or Edit Phone/User Dialog Box, page 56-41.

Procedure

Use this procedure to create, edit, or delete a paging number.

Step 1 Choose **Configure > Unified Communications > Telephony Features > Paging Numbers** to open the Paging Numbers summary page. See Paging Numbers Summary Page, page 59-51.

Step 2 To create a paging number, click **Create**. The Create Paging Number dialog box opens. Enter the information such as the name corresponding to the paging number, the number that can be called to initiate a page, description, the multicast IP address, and the UDP port number. Associate the phones to the paging number, and then click **OK**. See Create or Edit Paging Number Dialog Box, page 59-53.

Step 3 To modify the paging number parameters, choose the paging number row for which you want to modify the parameters, and then click **Edit**. The Edit Paging Number dialog box opens. Change the parameters, and then click **OK**. See Create or Edit Paging Number Dialog Box, page 59-53.

Step 4 To delete paging numbers, choose a paging number row or rows that you want to delete, and then click **Delete**. A confirmation dialog box opens. Click **Yes** in the confirmation dialog box.

Note You cannot delete a paging number that is part of a paging group.

Step 5 To set the paging type preference for a selected phone, choose the paging number row, and then click **Set Phones Paging Type Preference**. The Set Phones Paging Type Preference dialog box opens. Choose the phone from the drop-down list, then choose the Unicast or the Multicast option, and then click **OK**. See Set Phones Paging Type Preference Dialog Box, page 59-55.

Related Topics

- Paging Numbers, page 59-49
- Paging Numbers Reference, page 59-51

Paging Numbers Reference

The following topics describe the pages and dialog boxes used to configure paging numbers:

- Paging Numbers Summary Page, page 59-51
- Create or Edit Paging Number Dialog Box, page 59-53
- Set Phones Paging Type Preference Dialog Box, page 59-55

Paging Numbers Summary Page

Use the Paging Numbers summary page to view the paging numbers that are configured, to create new paging numbers, to modify the parameters of a selected paging number, to delete paging numbers, and to set the paging type preference for a selected phone.

How to Get to This Page

Click **Configure > Unified Communications > Telephony Features > Paging Numbers**.

Related Topics

- Paging Numbers, page 59-49
- Creating, Editing, and Deleting a Paging Number, page 59-49
- Create or Edit Paging Number Dialog Box, page 59-53
- Set Phones Paging Type Preference Dialog Box, page 59-55

Field Reference

Table 59-15 Paging Numbers Summary Page

Element	Description
Paging Name	The name corresponding to the paging number that appears in caller-ID displays and directories during the page.
Paging Number	The number that can be called to initiate a page.

Table 59-15 Paging Numbers Summary Page

Element	Description
Multicast IP Address	The unique multicast IP address that the paging number uses to broadcast audio paging messages to the idle IP phones that are associated with the paging number.
UDP Port Number	The UDP port used to broadcast audio paging messages to the idle IP phones that are associated with the paging number.
Member Phones	The number of members (phones) associated to the paging number.
Create button	Click this button to open the Create Paging Number dialog box in which you can create a new paging number. See Create or Edit Paging Number Dialog Box, page 59-53.
Edit button	Click this button to open the Edit Paging Number dialog box in which you can modify the parameters that are configured on a selected paging number. See Create or Edit Paging Number Dialog Box, page 59-53.
Delete button	Click this button to delete selected paging numbers. A confirmation dialog box opens. Click **Yes** in the confirmation dialog box to delete the selected paging number. **Note** You cannot delete a paging number that is part of a paging group.
Set Phones Paging Type Preference button	Click this button to open the Set Phones Paging Type Preference dialog box in which you can set the paging type for a selected phone. The options are Unicast or Multicast. See Set Phones Paging Type Preference Dialog Box, page 59-55.

Create or Edit Paging Number Dialog Box

Use the Create or Edit Paging Number dialog box to create a new paging number or to modify the parameters of a selected paging number.

How to Get to This Dialog Box

- Click **Configure > Unified Communications > Telephony Features > Paging Numbers > Create**.
- Click **Configure > Unified Communications > Telephony Features > Paging Numbers > Edit**.

Related Link

- Paging Numbers, page 59-49
- Paging Numbers Summary Page, page 59-51
- Creating, Editing, and Deleting a Paging Number, page 59-49

Field Reference

Table 59-16 Create or Edit Paging Number

Element	Description
Name	The name corresponding to the paging number that appears in caller-ID displays and directories. Once the paging name is configured, it cannot be changed. **Note** This field is mandatory.
Number	The number that can be called to initiate a page. Once the paging number is configured, it cannot be changed.
Description	The text string that describes the paging number.
Multicast IP address	The unique multicast IP address that the paging number uses to broadcast audio paging messages to the idle IP phones that are associated with the paging number. When multiple paging numbers are configured, each paging number must use a unique multicast IP address. **Note** IP phones do not support multicast at 224.x.x.x addresses.

Table 59-16 Create or Edit Paging Number (continued)

Element	Description
UDP port number	The UDP port number that is used to broadcast paging messages to the idle IP phones. The default port number is 2000. **Note** The UDP port number field is enabled after you specify the multicast IP address.
Associate Phones	Contains two panes: • Available Phones (left pane)—Lists the available phones that are not part of the current paging number in the following format: MAC address (username if configured), for example, 1111.1111.1111 (smith). • Selected Phones (right pane)—Lists the phones that you added from the Available Phones pane into the Selected Phones pane. The phones listed in the Selected Phones pane receive an audio page when the number is called. The phones respond to the audio page when they are idle. You can add or remove the phones from the Selected Phones pane by using the arrow buttons or by using the drag and drop feature. • To add the phone, do one of the following: – Use the arrow buttons—Select the phones from the Available Phones list, and then click the > button. The phone is added to the Selected Numbers list. To add all the phones, click the >> button. – Use the drag and drop feature—Select the phones from the Available Phones list, and then drag and drop them into the Selected Phones area. • To remove the phone, do one of the following: – Use the arrow buttons—Select the phones from the Selected Phones list, and then click the < button. To remove all the phones from the Selected Extensions list, click the << button. – Use the drag and drop feature—Select the phones from the Selected Phones list, and then drag and drop them into the Available Phones area.
OK button	Click this button to apply the paging number configuration to the router.
Cancel button	Click this button to discard the configuration values that you entered.

Set Phones Paging Type Preference Dialog Box

Use the Set Phones Paging Type Preference dialog box to set the paging preference for a selected phone. The paging mechanism supports audio distribution using IP multicast, replicated unicast, and a mixture of both (so that multicast is used where possible, and unicast is used for specific phones that cannot be reached using multicast).

How to Get to This Dialog Box

Click **Configure > Unified Communications > Telephony Features > Paging Numbers**. Choose a paging number, and click **Set Phones Paging Type Preference**.

Related Link

- Paging Numbers Summary Page, page 59-51
- Creating, Editing, and Deleting a Paging Number, page 59-49

Field Reference

Table 59-17 Set Phones Paging Type Preference Dialog Box

Element	Description
Phones **Note** This field is mandatory.	The list of phones that are associated with the current paging number. Choose the phone for which you want to set the paging type from the drop-down list. If a paging type is already configured on the selected phone, that paging type radio button is selected. You can change the paging type.
Paging Type radio buttons	The paging mechanism supports audio distribution using IP multicast, unicast, and a mixture of both (so that multicast is used where possible, and unicast is used for specific phones that cannot be reached using multicast). Choose one of the options: • Unicast—Choose this option for phones that cannot be reached through multicast. A maximum of 10 phones are supported. • Multicast—Choose this option to deliver the page to a group of phones simultaneously. This is the default option.

Table 59-17 Set Phones Paging Type Preference Dialog Box (continued)

Element	Description
OK button	Click this button to apply the phone's paging type preference to the router.
Cancel button	Click this button to discard the configuration values that you entered.

Paging Groups

A paging group is a group of paging numbers. After you create two or more paging numbers, you can add them into a paging group. By creating a paging group, you have the flexibility to page a combined set of paging numbers. For example, you can page a group that consists of both the jewelry department and the accessories department.

Note Paging groups is supported with SCCP and SCCP and SIP endpoints but SIP phones are not listed.

Related Topics

- Creating, Editing, and Deleting Paging Groups, page 59-56
- Paging Groups Reference, page 59-57

Creating, Editing, and Deleting Paging Groups

Before You Begin

Make sure that you have configured paging numbers. See Creating, Editing, and Deleting a Paging Number, page 59-49.

Procedure

Use this procedure to create, edit, or delete a paging group.

Step 1 Choose **Configure > Unified Communications > Telephony Features > Paging Groups** to open the Paging Groups summary page. See Paging Groups Summary Page, page 59-58.

Step 2 To create a paging group, click **Create**. Enter the information, such as the group name corresponding to the paging group number, the number that can be called to initiate a page, the multicast IP address, and the UDP port number. Associate the paging numbers to the paging group, and then click OK. See Create or Edit a Paging Group Dialog Box, page 59-59.

Step 3 To modify the paging group parameters, choose a paging group row for which you want to modify the parameters, and then click **Edit**. The Edit Paging Group page opens. Change the parameters, and then click **OK**. See Create or Edit a Paging Group Dialog Box, page 59-59.

Step 4 To delete paging groups, choose the paging group row or rows that you want to delete, and then click **Delete**. A confirmation dialog box opens. Click **Yes** in the confirmation dialog box.

Related Topics

- Paging Groups, page 59-56
- Paging Groups Reference, page 59-57

Paging Groups Reference

The following topics describe the pages and dialog boxes used to configure paging groups:

- Paging Groups Summary Page, page 59-58
- Create or Edit a Paging Group Dialog Box, page 59-59

Paging Groups Summary Page

Use the Paging Groups summary page to view the paging groups that are configured, to create new paging groups, to modify the parameters of a selected paging group, and to delete paging groups.

How to Get to This Page

Click **Configure > Unified Communications > Telephony Features > Paging Groups**.

Related Link

- Paging Groups, page 59-56
- Create or Edit a Paging Group Dialog Box, page 59-59

Field Reference

Table 59-18 Paging Groups Summary Page

Element	Description
Paging Group Name	The paging group name that appears in caller-ID displays and directories during the page.
Paging Group Number	The number associated with the paging group. This is the number that can be called to initiate a group page.
Multicast IP Address	The unique multicast IP address that the paging number uses to broadcast audio paging messages to the idle IP phones that are associated with the paging number.
UDP Port Number	The UDP port used to broadcast audio paging messages to the idle IP phones that are associated with the paging number.
Group Members	The number of members (paging numbers) associated with the paging group.
Create button	Click this button to open the Create Paging Group dialog box in which you can create a new paging group. See Create or Edit a Paging Group Dialog Box, page 59-59.
Edit button	Click this button to open the Edit Paging Group dialog box in which you can modify the parameters that are configured on a selected paging group. See Create or Edit a Paging Group Dialog Box, page 59-59.

Table 59-18 Paging Groups Summary Page (continued)

Element	Description
Delete button	Click this button to delete selected paging groups. A confirmation dialog box opens. Click **Yes** in the confirmation dialog box to delete the selected paging group.

Create or Edit a Paging Group Dialog Box

Use the Create or Edit Paging Group dialog box to create a new paging group or to modify the parameters of a selected paging group.

How to Get to This Dialog Box

- Click **Configure > Unified Communications >Telephony Features > Paging Groups > Create**.
- Click **Configure > Unified Communications > Telephony Features > Paging Groups > Edit**.

Related Link

- Paging Groups, page 59-56
- Creating, Editing, and Deleting Paging Groups, page 59-56

Field Reference

Table 59-19 Create or Edit a Paging Group

Element	Description
Name **Note** This field is mandatory.	The group name corresponding to the paging group number that appears in caller-ID displays and directories. Once the paging group name is configured, it cannot be changed.
Number	The number that can be called to initiate a group page. Once the paging group number is configured, it cannot be changed.
Multicast IP address	The multicast IP address to use for the paging group number. When multiple paging groups are configured, each paging group must use a unique multicast IP address. **Note** IP phones do not support multicast at 224.x.x.x addresses.

Table 59-19 Create or Edit a Paging Group (continued)

Element	Description
UDP port number	The UDP port number to be used to broadcast paging messages to the idle IP phones that are associated with the paging group. The default port number is 2000. **Note** The UDP port number field is enabled only when you have specified a multicast IP address.

Table 59-19 Create or Edit a Paging Group (continued)

Element	Description
Associate Paging Numbers	Contains two panes: • Available Paging Numbers (left pane)—Lists all of the configured paging numbers that are available to be part of a paging group. • Selected Paging Numbers (right pane)—Lists the paging numbers that you added from the Available Paging Numbers pane into the Selected Paging Numbers pane. The paging numbers listed in the Selected Paging Numbers pane become part of the paging group. **Note** A maximum of 10 paging numbers can be grouped into a paging group. You can add or remove the paging numbers from the Selected Paging Numbers pane by using the arrow buttons or by using the drag and drop feature. • To add the paging number, do one of the following: – Use the arrow buttons—Select the paging numbers from the Available Paging Numbers list, and then click the > button. The paging number is added to the Selected Numbers list. To add all the paging numbers, click the >> button. – Use the drag and drop feature—Select the paging number from the Available Paging Numbers list, and then drag and drop it into the Selected Paging Numbers area. • To remove the paging number, do one of the following: – Use the arrow buttons—Select the paging numbers from the Selected Paging Numbers list, and then click the < button. The paging number is removed from the Selected Paging Numbers list. To remove all the paging numbers from the Selected Extensions list, click the << button. – Use the drag and drop feature—Select the paging numbers from the Selected Paging Numbers list, and then drag and drop it into the Available Paging Numbers area.
OK button	Click this button to apply the paging group configuration to the router.

Table 59-19 Create or Edit a Paging Group (continued)

Element	Description
Cancel button	Click this button to discard the configuration values that you entered.

Phone Templates

You can customize the display and order of soft keys that appear during various call states on individual IP phones. Using phone templates, you can delete soft keys that would normally appear or change the order in which the soft keys appear. For example, you might want to display the CFwdAll and Confrn soft keys on a manager's phone and remove these soft keys from a receptionist's phone.

You can also:

- Set preferred codec for calls with other phones on this router.
- Define blocked features.
- Enable Do Not Disconnect conference when conference initiator hangs-up. Connect remaining parties together directly using call transfer. This command is for adhoc software 3-party conference only.
- Always send media packets to this router.
- Enable Multicast Moh.
- Define night-service bell.
- Set audio paging dn group for phone.
- Define softkeys per state.
- Define IP phone speed-dial number.
- Transfer related configuration.
- Customized transfer-pattern configuration.
- Define IP phone type.
- Define URLs.

Note Ringing call state is not supported.

Note Phone softkey templates is supported with SCCP and SCCP and SIP endpoints but SIP phones are not listed.

Phone Template Reference

The following topics describe the window used to configure Phone Templates:

- Phone Templates page, page 59-63
- Creating or Editing a phone template, page 59-64
- Create or Edit Phone Template dialog box, page 59-66
- Associate Phones dialog box, page 59-71

Phone Templates page

Use the Phones Templates page to review and manage softkey templates.

How to get to this screen

Click **Configure > Unified Communications > Users, Phones and Extensions > Templates and Firmware > Phone Templates**.

Note Hlog softkey is available when huntgroup logout (Hlog) is enabled in the Telephony settings.

Note Flash softkey is available if FXO hookflash is enabled in the Telephony settings.

Note Phone templates are not available for SIP endpoints. One or both of the endpoints configured under **Unified Communications > Telephony Settings** have to be SCCP.

Related Links

- Create or Edit Phone Template dialog box, page 59-66
- Associate Phones dialog box, page 59-71

Field Reference

Table 59-20 Phone Templates

Element	Description
Template ID	Number from 1 to 20 that identifies the template.
Softkey Call States	The call states that are configured for this template. A call state with no softkeys configured does not appear in this column.
Associated Phones	The phones associated with this template.
Create button	Click to open the Create Softkey Template dialog box. See Create or Edit Phone Template dialog box, page 59-66.
Edit button	Click to open the Edit Softkey Template dialog box. See Create or Edit Phone Template dialog box, page 59-66.
Delete button	Click to open the Confirmation dialog box to delete the selected phone template.
Associate Phones button	Click to open the Associate Phones dialog box. See Associate Phones dialog box, page 59-71.

Creating or Editing a phone template

To create or edit a phone template, perform these steps:

Step 1 In the Configure tree, click **Unified Communications > Users, Phones and Extensions > Templates and Firmware > Phone Templates**. Cisco Configuration Professional displays the Phone Templates page.

Step 2 To edit an entry, choose an entry on the page. To add a template, skip this step.

Step 3 To display the Create Phone Template dialog box, click **Create**.

To display the Edit Phone Template page, click **Edit**.

Step 4 If you are editing a template, skip this step; the **Template ID** field is read only. If you are adding a template, enter the identification number in the **Template ID** field. The identification number range is from 1 to 20. There is no default.

Step 5 Click the Blocked Features tab, the Call Conference tab, the Codec tab, the Softkeys tab, and the Miscellaneous tab and choose the required options for each. More details about the options for the Softkeys tab follows.

Step 6 In the Softkeys tab, select the group of softkeys to modify. Not all softkeys are available for all call states.

Step 7 To select an available softkey, click a softkey name in the Available Softkeys column and drag it to the Selected Softkeys column. You can also select a softkey and click the right arrow to move it. Softkeys in the Selected Softkeys column, will be available on phones that use this template.

To move all available softkeys from the Available Softkeys column to the Selected Softkeys column, click the right double-arrow. To remove all available softkeys from the Selected Softkeys column, click the left double-arrow.

To remove a softkey from the Selected column, click the softkey name and drag it to the Available Softkeys column. You can also select the softkey name and click the left arrow to move it. Softkeys moved to the Available column will not be available on phones that use this template.

Step 8 The order of softkeys in the Selected column determines the order that the keys will be seen on phones. To move a softkey up the list of selected softkeys, select the softkey and click the up arrow.

To move a softkey down the list of selected softkeys, select the softkey and click the down arrow.

Create or Edit Phone Template dialog box

Use the Create or Edit Phone Template dialog box to create or change settings for call states and softkeys. This dialog box lets you select and order softkeys for multiple call states.

How to get to this screen

- Click **Configure > Unified Communications > Users, Phones and Extensions > Templates and Firmware > Phone Templates > Create**.
- Click **Configure > Unified Communications > Users, Phones and Extensions > Templates and Firmware > Phone Templates > Edit**.

Related Links

- Creating or Editing a phone template, page 59-64
- Phone Templates page, page 59-63

Field Reference

Table 59-21 Create or Edit Phone Template

Element	Description
Template ID drop-down list	Choose the template ID from the drop-down list. **Note** This is a mandatory field if you are creating a new phone template. This is a non-editable field if you are editing an existing phone template.
Blocked Features tab	
Answer a ringing phone in any pickup group by pressing the GpickUp softkey and then dialing the pickup group number check box	Check the check box to select this option. Uncheck the check box to deselect this option.
Join three or more parties in a telephone conversation check box	Check the check box to select this option. Uncheck the check box to deselect this option.
Place a call on hold at a special extension so it can be retrieved from any other place in the system check box	Check the check box to select this option. Uncheck the check box to deselect this option.

Table 59-21 Create or Edit Phone Template (continued)

Element	Description
Forward all incoming calls to a specified phone number check box	Check the check box to select this option. Uncheck the check box to deselect this option.
When connected to one party, shift the connection of the other party to a different number check box	Check the check box to select this option. Uncheck the check box to deselect this option.
Answer a call that is ringing on another phone check box	Check the check box to select this option. Uncheck the check box to deselect this option.
Call Conference tab	
The following options determine how the parties in a conference call will remain connected even when the conference initiator hangs up. These options are valid for adhoc three-party conferences only.	
The conference initiator can leave the conference and keep the other two parties connected check box	Check the check box to select this option. Uncheck the check box to deselect this option.
The conference initiator can press the confn softkey (IP phone) or hookflash (Analog Phone) to drop the last connected party from the conference check box	Check the check box to select this option. Uncheck the check box to deselect this option.
The conference initiator can hang up and leave the other parties connected if at least one of the remaining connected parties is local to the Cisco Unified CME system check box	Check the check box to select this option. Uncheck the check box to deselect this option.
Codec tab	
Use the following option to set preferred codec for calls with other phones on this router.	
Select codec type drop-down list	Choose the desired codec value from the drop-down list.
Softkeys tab	
Alert Call State tab, Connected Call State tab, Hold Call State tab, Idle Call State tab, Seized Call State tab	Click each tab to select softkeys from the available softkeys.
The various call states are explained below:	

Table 59-21 Create or Edit Phone Template (continued)

Element	Description
Alert Call State	A phone is in the alert call state when the remote point is being notified of an incoming call, and the status of the remote point is being relayed to the caller as either ringback or busy.
Connected Call State	A phone is in the connected call state when the connection to a remote point is established.
Hold Call State	A phone is in the hold call state when a connected party is still connected but there is temporarily no voice connection.
Idle Call State	A phone is in the idle call state before a call is made and after a call is complete.
Seized Call State	A phone is in the seized call state when a caller is attempting a call but it has not yet been connected.
Available Softkeys list	Lists the available softkeys. See Table 59-22 on page 59-70. Use the navigation arrows to move one or all available softkeys to the Selected Softkeys list. Use the same navigation arrows to remove softkeys from the list.
Selected Softkeys list	Lists the selected softkeys. Use the navigation arrows to move a selected item to the top of the list, end of the list, or one position up or down in the list.
Miscellaneous tab	
Always send the Media Packets (RTP) to this Cisco Unified CME router check box	Check the check box to select this option. Uncheck the check box to deselect this option.
Enable the multicast of the music on hold audio stream check box	Check the check box to select this option. Uncheck the check box to deselect this option.
Enable the IP phone to receive night-service bell notification check box	Check the check box to select this option. Uncheck the check box to deselect this option.

Table 59-21 Create or Edit Phone Template (continued)

Element	Description
Block call transfer to patterns defined under advanced telephony settings check box	Check the check box to select this option. Uncheck the check box to deselect this option.
Allow this phone to make blocked calls during after hours check box	Check the check box to select this option. Uncheck the check box to deselect this option.
OK button	Click OK to send your changes to the router.
Cancel button	Click Cancel to discard your changes.

The available softkeys are as follows:

Table 59-22 Available Softkeys

Softkey	Description
Acct	Short for "account code." Provides access to configured accounts.
Answer	Picks up incoming call.
Callback	Requests callback notification when a busy called line becomes free.
Cfwall	Forwards all calls to a target number.
Confrn	Short for "conference." Initiates ad-hoc conference or adds a new party to a conference call.
ConfList	Displays a list of conference participants.
DnD	Short for "do not disturb." Enables the do-not-disturb features.
EndCall	Ends the current call.
Flash	Short for "hookflash." Provides hookflash functionality for PSTN[1] services on calls connected to the PSTN via a foreign exchange office FXO[2] port.
GPickUP	Short for "group call pickup." Selectively picks up calls coming into a phone number that is a member of a pickup group.
HLog	Places the phone of an ephone-hunt group agent into the not-ready status or, if the phone is in the not-ready status, it places the phone into the ready status.
Hold	Places an active call on hold and resumes the call.
Join	Join an ad hoc conference.
Login	Provides PIN[3] access to restricted phone features.
MeetMe	Initiate a new MeetMe conference.
NewCall	Opens a line on a speakerphone to place a new call.
Park	Places an active call on hold so it can be retrieved from another phone in the system.
PickUp	Selectively picks up calls coming into another extension.
Redial	Redials the last number dialed.
Resume	Resumes the call.

Table 59-22 Available Softkeys (continued)

Softkey	Description
RmLstC	Removes the last caller from ad-hoc conference.
Select	Selects parties to be put into a conference call.
Trnsfer	Short for "call transfer." Transfers an active call to another extension.

1. PSTN = public switched telephone network
2. FXO = Foreign Exchange Office
3. PIN = Personal Identification Number

Associate Phones dialog box

Use this dialog box to associate a phone template with phones.

How to get to this page

- Click **Configure > Unified Communications > Users, Phones and Extensions > Templates and Firmware > Phone Templates > Associate Phones**.

How to use this page

To apply a phone template to a phone, complete the following tasks:

Step 1 In the Configure tree, click **Unified Communications > Users, Phones and Extensions > Templates and Firmware > Phone Templates**.

Step 2 In the Phone Templates page, choose the template to which you want to associate phones.

Step 3 To associate one or more phones with the template, click **Associate Phones**.

In the Associate Phones dialog box, select the phone to associate with the template, and click the left arrow. The phone you selected moves to the Selected column.

Note Analog phones are not listed.

Note If you chose one of the phone endpoints as SIP under **Unified Communications > Telephony Settings**, the phone is not displayed in the Available Phones list.

Step 4 To remove a phone from the Selected column, choose the phone, and click the right arrow. The phone moves to the Available column.

Step 5 When you have added all the phones that you want to associate with this template to the Selected column, click **OK**. You are prompted to restart the phone.

Step 6 Click **Yes** to restart the phone so the softkeys will be updated to the new configuration. Click **No** to associate the phone to the template without restarting the phone and updating the softkeys.

Related Links

- Phone Templates page, page 59-63
- Create or Edit Phone Template dialog box, page 59-66

Extension Templates

For information about how to use Cisco Configuration Professional (Cisco CP) to configure the Extension Templates feature, see the screencast at: http://www.cisco.com/en/US/docs/net_mgmt/cisco_configuration_professional/scrcst/ccpsc.html

Note You must have Internet access to view the screencast.

Note Extension templates are supported with SCCP and SCCP and SIP endpoints but SIP phones are not listed.

CHAPTER 60

Phone Firmware

Phone firmware files, also known as a phone load, are stored locally in Flash memory and provide code to enable phone displays and operations. These files are specialized for each phone type and protocol, SIP or SCCP, and are periodically revised. You must be sure to have the appropriate phone firmware files for the types of phones, protocol being used, and Cisco Manager Express (Cisco Unified CME) version at your site. You can use Cisco CP to configure and upload firmware to the phones.

This chapter contains the following sections:

- Configuring Phone Firmware, page 60-2
- Phone Firmware Reference, page 60-2

Configuring Phone Firmware

The Phone Firmware feature uploads a phone firmware file to the device Flash. It can configure the firmware existing on the Flash and allows you to remove or modify phone firmware association for a type of Cisco IP phone.

Note

- If you upload a phone firmware file that is already present in Flash, Cisco CP overwrites the file in Flash.
- If a phone firmware file is already configured for a particular phone type and you try to upload another firmware file for same phone type, Cisco CP uploads the firmware files, but it does not overwrite the existing firmware configured on the phone. You can associate phone firmware through the Phone Firmware Wizard and through the Edit button on the Phone Firmware page.
- If you attempt to upload a phone firmware to a Cisco 2800 series router with IOS version 12.4(11)T, the results are unpredictable and this is not recommended. We recommend that you upgrade the router to a more recent image.

You can download phone firmware files from Cisco.com.

Phone Firmware Reference

The following topics describe the window used to configure phone firmware, edit phone firmware, delete firmware, reset the phones, and display registered phones:

- Phone Firmware Page, page 60-3
- Edit button, page 60-4
- Edit Phone Firmware Settings dialog box, page 60-6
- Delete button, page 60-5
- Reset button, page 60-5
- Show Registered Phones button, page 60-5
- Registered Phones dialog box, page 60-6

Phone Firmware Page

Use this page to:

- Download phone firmware files from Cisco.com
- Launch wizard to configure phone firmware
- Associate phone firmware to a type of Cisco IP phone
- Delete selected phone firmware configuration
- Reset all phones
- Display the number of registered phones

Note

- If you upload a phone firmware file that is already present in Flash, Cisco CP overwrites the file in Flash.
- If a phone firmware file is already configured for a particular phone type and you try to upload another firmware file for same phone type, Cisco CP uploads the load files, but it does not overwrite the existing firmware configured on the phone. You can associate phone firmware through the Phone Firmware Wizard and through the Edit button on the Phone Firmware page.
- If you attempt to upload a phone firmware to a Cisco 2800 series router with IOS version 12.4(11)T, the results are unpredictable and this is not recommended. We recommend that you upgrade the router to a more recent image.

How to get to this page

- Click **Configure > Unified Communications > Users, Phones and Extensions > Templates and Firmware > Phone Firmware**.

Field Reference

Table 60-1 Phone Firmware page

Element	Description
Phone Model	Displays the model of the phone, for example 7905.
Phone Type	Displays the type of the phone, for example SIP.
Phone Firmware	Displays the phone load name, for example CP7905080001SCCP051117AS.BIN.
Filter	Enter keyword to filter the contents of the table. For example enter 7902 to display only the configured 7902 phone entries.
Edit button	Click to display the Edit Phone Firmware Settings dialog box.
Delete button	Click to remove phone firmware files from the Flash along with their configuration.
Reset button	Click to reboot all phones.
Show Registered Phones button	Click to display the Registered Phones dialog box with number of registered phones and total number of phones.
Guided Configuration—Right Pane	
Download Firmware link	Click to display the Download Software page from where you can select and download phone firmware.
Launch wizard button	Click to launch the Phone Firmware Wizard.
FAQ	Click the questions to see the help for each.

Edit button

Click the Edit button to edit phone firmware settings.

The Edit Phone Firmware Settings dialog box is displayed.

Delete button

Use the Delete button to remove phone firmware files from the Flash along with their configuration.

Step 1 Select single or multiple entries in the summary table and click **Delete**. A confirmation dialog box is displayed asking if you want to delete the selected phone firmware configurations.

Step 2 Click **Yes**. A confirmation dialog box is displayed asking if you want to delete firmware files from the device Flash, click **Yes** to delete the firmware files as well.

Click **No** to delete the configuration but not the firmware files.

Reset button

When you reset phones, you perform a complete reboot of all phones of a selected phone model. For example, if you selected 7905 phone model in the summary table, then all phones of model 7905 are reset. If a new phone firmware file is associated with a phone type, the file or files are downloaded to the phones.

Click the Reset button to be prompted to reset the phones. To reset the selected phones, click **Yes**. To exit the confirmation message window without resetting the phones, click **No**.

Note If the selected phone model does not have phones configured, clicking the Reset button has no effect.

Show Registered Phones button

Click this button to view the total number of phones and number of registered phones.

The Registered Phones dialog box dialog box is displayed.

Edit Phone Firmware Settings dialog box

In this dialog box, choose the firmware that you want a phone to use.

How to get to this page

- Click **Configure > Unified Communications > Users, Phones and Extensions > Templates and Firmware > Phone Firmware > Edit**.

Related Links

- Phone Firmware Page, page 60-3
- Registered Phones dialog box, page 60-6

How to use this screen

To update phone firmware file association for a particular type of Cisco IP phone, do the following:

Step 1 Select a phone type from the list in the Phone Firmware page, and click **Edit**.

Step 2 Select the phone firmware file from the Phone Firmware menu. The menu lists only those phone firmware files that are supported by the selected phone type and present in Flash.

Step 3 Check the Reset phones check box. To apply changes, all affected phones have to be reset.

Step 4 Click **OK** to apply your changes.

Step 5 Click **Cancel** to discard your changes.

Registered Phones dialog box

Use this dialog box to display the number of registered phones.

Related Links

- Reset button, page 60-5
- Registered Phones dialog box, page 60-6

How to get to this screen

- Click **Configure > Unified Communications > Users, Phones and Extensions > Templates and Firmware > Phone Firmware > Show Registered Phones**.

Step 1 Click **Show Registered Phones** to display a dialog box indicating number of registered phones and the total number of phones.

Step 2 Click **Refresh** to update the data for the registered phones.

Phone Firmware Wizard

Use this wizard to upload and configure phone firmware files.

How to get to this page

Click **Configure > Unified Communications > Users, Phones and Extensions > Templates and Firmware > Phone Firmware > Launch Wizard**.

See the appropriate link:

- Configure phone firmware available on the device flash radio button, page 60-7
- Upload phone firmware on the device flash and configure them radio button, page 60-11
- Upload phone firmware on the device flash without configuring them radio button, page 60-13

Configure phone firmware available on the device flash radio button

Use this option to configure phone firmware files present on the device flash.

How to get to this radio button

Click **Configure > Unified Communications > Users, Phones and Extensions > Templates and Firmware > Phone Firmware > Launch Wizard > Select Operation.**

Related Links

- Phone Firmware Wizard, page 60-7
- Upload phone firmware on the device flash and configure them radio button, page 60-11
- Upload phone firmware on the device flash without configuring them radio button, page 60-13
- Manual Phone Firmware Configuration dialog box, page 60-9

Configure Phone Firmware page

Use the Configure Phone Firmware page to view the phone type, phone model, and choose phone firmware file for a phone,

How to get to this page

Click **Configure > Unified Communications > Users, Phones and Extensions > Templates and Firmware > Phone Firmware > Launch Wizard > Select Operation > Configure phone firmware available on the device flash** radio button **> Next**.

Step 1 Select the phone firmware to apply to the phone model from the list.

The table lists Cisco CP recognized phone firmware files.

If a phone model has multiple phone firmware files, they are displayed in a drop-down list under Phone Firmware. You can choose any of the available phone firmware files from the drop-down list or skip phone firmware configuration by choosing Skip/None in the drop-down list.

Step 2 Check the Reset check box to perform a complete reboot of all phones of the selected phone model.

Note If the selected phone model does not have phones configured, clicking the Reset button has no effect.

Step 3 To configure new phone firmware files not given in the list, click the **Click here to manually configure phone firmware not listed in the above list** link.

The Manual Phone Firmware Configuration dialog box is displayed.

Finish page

How to get to this page

Click **Configure > Unified Communications > Users, Phones and Extensions > Templates and Firmware > Phone Firmware > Launch Wizard > Select Operation > Configure phone firmware available on the device flash** radio button **> Next > Configure Phone Firmware > Next**.

Use the Finish page to view the success or failure message for configuration of phone firmware files on the device Flash.

Manual Phone Firmware Configuration dialog box

Use this dialog box to manually configure new phone firmware files.

How to get to this page

Click **Configure > Unified Communications > Users, Phones and Extensions > Templates and Firmware > Phone Firmware > Launch Wizard > Select Operation > Configure phone firmware available on the device flash** radio button **> Next > Configure Phone Firmware > Click here to manually configure phone firmware not listed in above list** link.

Related Links

- Configure Phone Firmware page, page 60-8
- Configure phone firmware available on the device flash radio button, page 60-7
- Phone Firmware Wizard, page 60-7

Field Reference

Table 60-2 Manual Phone Firmware Configuration dialog box

Element	Description
Phone Type drop-down list	Choose the type of phone, SIP or SCCP. Based on endpoint selected under **Unified Communications > Telephony Settings,** you will see SCCP or/and SIP. For example, If SIP endpoint is selected then you will see only SIP not SCCP in this dialog box. **Note** This is a mandatory field.
Phone Model drop-down list	Choose the phone model. This is a mandatory field. The drop-down list has all SIP and SCCP phones supported by Cisco CP. From the drop-down list, choose Other to configure new phones not supported by Cisco CP. Enter the phone model in the field. **Note** This is a mandatory field.
Available files pane	Displays all available files on the device if Configure phone firmware available on the device flash option is selected from the Select Operation page. Displays content of zip and tar files when Upload phone firmware on the device flash and configure them option is selected from the Select Operation page. Click the required phone firmware files to select them. Click the Select button to move the selected files to the Associated firmware files pane. Click the Select All button to move all phone firmware files to the Associated firmware files pane.

Table 60-2 Manual Phone Firmware Configuration dialog box

Element	Description
Associated firmware files pane	Displays the selected phone firmware files. Click the required phone firmware file to select it. Click the Unselect button to move the selected file back to the Available files pane. Click the Unselect All button to move all phone firmware files back to the Available files pane.
Show only firmware files check box	Check this check box to display only phone firmware files in the Available files pane.
Load File drop-down list	This drop-down list gets automatically populated with the selected phone firmware files when they are moved to the Associated firmware files pane. Choose the load_file which will be used in load command. For example, load <phone_type> <load_file> Choose the required phone firmware file from the drop-down list. This is a mandatory field.
OK button	Click OK. The phone firmware file with associated phone model and type is displayed in the Configure Phone Firmware page.
Cancel button	Click Cancel to discard your changes.

Upload phone firmware on the device flash and configure them radio button

Use this option to upload phone firmware files on the device and configure them.

How to get to this radio button

Click **Configure > Unified Communications > Users, Phones and Extensions > Templates and Firmware > Phone Firmware > Launch Wizard > Select Operation.**

Related Links

- Phone Firmware Page, page 60-3
- Configure phone firmware available on the device flash radio button, page 60-7
- Upload phone firmware on the device flash without configuring them radio button, page 60-13

Field Reference

Table 60-3 Upload phone firmware on the device flash and configure them radio button

Element	Description
Phone firmware file field	Click Browse to select the phone firmware file from your PC. This is a mandatory field.
Device flash drop-down list	Choose the device flash where phone firmware files are to be copied from the drop-down list. This is a mandatory field.
Directory drop-down list	The drop-down list displays all directories available on the selected flash. Choose the directory on the device flash where the phone firmware file is to be saved. This is a mandatory field.
Back button	Click Back to go back to the previous page.
Next button	Click Next to go to the Configure Phone Firmware page, page 60-8.
Cancel button	Click Cancel to discard the changes you made and exit the wizard.

Finish page

Use the Finish page to view the success or failure message for upload and configuration of phone firmware files on the device Flash.

How to get to this radio button

Click **Configure > Unified Communications > Users, Phones and Extensions > Templates and Firmware > Phone Firmware > Launch Wizard > Select Operation > Upload phone firmware on the device flash and configure them radio button > Next.**

Upload phone firmware on the device flash without configuring them radio button

Use this option to upload phone firmware files on the device without configuring them.

How to get to this radio button

Click **Configure > Unified Communications > Users, Phones and Extensions > Templates and Firmware > Phone Firmware > Launch Wizard > Select Operation.**

Related Links

- Configure phone firmware available on the device flash radio button, page 60-7
- Upload phone firmware on the device flash and configure them radio button, page 60-11

Field Reference

Table 60-4 Upload phone firmware on the device flash without configuring them radio button

Element	Description
Phone firmware file field	Click Browse to select the phone firmware file from your PC. This is a mandatory field.
Device flash drop-down list	Choose the device flash where phone firmware files are to be copied from the drop-down list. This is a mandatory field.
Directory drop-down list	The drop-down list displays all directories available on the selected flash. Choose the directory on the device flash where the phone firmware file is to be saved. This is a mandatory field.
Back button	Click Back to go back to the previous page.
Next button	Click Next to go to the Finish page.
Cancel button	Click Cancel to discard the changes you made and exit the wizard.

Finish page

Use the Finish page to view the success or failure message for upload of phone firmware files on the device Flash without configuring them.

How to get to this radio button

Click **Configure > Unified Communications > Users, Phones and Extensions > Templates and Firmware > Phone Firmware > Launch Wizard > Select Operation > Upload phone firmware on the device flash without configuring them radio button > Next.**

FAQ

How do I upload firmware on device flash?

To upload firmware files from the PC to the device flash:

Step 1 Click **Launch wizard** on the Phone Firmware page.

The Phone Firmware wizard is launched with the Welcome page.

Step 2 Click **Next**.

The Select Operation page is displayed.

Step 3 Click the **Upload phone firmware files on the device flash without configuring them** radio button.

Step 4 Click **Browse** and select the firmware file.

Step 5 Choose the device flash slot on to which the firmware will be copied.

Step 6 Choose the directory on the flash slot selected in step 5 on to which firmware will be copied.

Step 7 Click **Next**.

Step 8 Click **Yes** in the confirmation window.

Once the upload is complete, the Finish page is displayed with the success or failure message.

How do I configure firmware on the device?

To configure firmware files already available on the device flash:

Step 1 Click **Launch wizard** on the Phone Firmware page.

The Phone Firmware wizard is launched with the Welcome page.

Step 2 Click **Next**.

The Select Operation page is displayed.

Step 3 Click the **Configure phone firmware files available on the device flash** radio button.

Step 4 Click **Next**.

The Configure Phone Firmware page is displayed with the list of all configurable firmware files on the device flash.

Step 5 If you do not see firmware files in the firmware summary table, add them manually. Click the **here** link available below the table to manually add firmware.

Step 6 Choose the appropriate firmware from the drop-down list which displays available firmware for a particular phone model under the Phone Firmware column.

Step 7 Select the Reset option to allow the phone to reset after the configuration is applied on the device.

Step 8 Click **Next** to apply the configuration.

Step 9 Click **Yes** in the confirmation window.

Once the configuration is applied, the Finish page is displayed with the success or failure message.

To configure firmware files available on the PC:

Step 1 Click **Launch wizard** on the Phone Firmware page.

The Phone Firmware wizard is launched with the Welcome page.

Step 2 Click **Next**.

The Select Operation page is displayed.

Step 3 Click the **Upload phone firmware files on the device flash and configure them** radio button.

Step 4 Click **Browse** and select the firmware file.

Step 5 Choose the device flash slot onto which the firmware will be copied.

Step 6 Choose the directory on the flash slot selected in Step 5 onto which the firmware file will be copied.

Step 7 Click **Next**.

The Configure Phone Firmware page is displayed with a list of all configurable firmware files on the device flash.

Step 8 If you do not see firmware files in the firmware summary table, add them manually. Click the **here** link available below the table to manually add firmware.

Step 9 Choose the appropriate firmware from the drop-down list that displays available firmware for a particular phone model under the Phone Firmware column.

Step 10 Select the Reset option to allow the phone to reset after the configuration is applied on the device.

Step 11 Click **Next** to apply the configuration.

Step 12 Click **Yes** in the confirmation window.

After the configuration is applied, the Finish page is displayed with a success or failure message.

How do I remove firmware from device flash?

To remove firmware from device flash:

Step 1 Select the firmware file or files to delete from the summary table.

Step 2 Click **Delete**.

Step 3 Click **Yes** in the confirmation window.

Step 4 Another confirmation window is displayed asking for user confirmation to allow deletion of files from the device flash. Click **Yes** to remove the firmware files from the flash. To avoid deleting the files, click **No**.

CHAPTER 61

Voicemail

This chapter explains how to configure Voicemail feature. It contains the following sections:

- Cisco Unity Express Initialization
- Configuring Voicemail
- Configuring the Call-in Number
- Launching Cisco Unity Express
- Configuring Module Settings

Cisco Unity Express Initialization

This section describes how to use Cisco CP to initialize a Cisco Unity Express (CUE) Module installed on the router.

This section contains the following sections:

- Initialization Procedure
- CUE Initialization Wizard Screen Reference
- Discovery Details Messages

Initialization Procedure

To complete the CUE module initialization process, complete the following tasks.

Step 1 Choose the device with the CUE module that you want to initialize from the Community Information screen, and click **Discover**. If not communities are configured, see the Community online help to learn how to configure communities.

Step 2 When the device is discovered, click **Discovery Details** and review the information in the displayed screen.

- If any of the messages in the "Discovery Details Messages" section on page 61-8 appear, rectify the problem that the message reports, and then rediscover the device before proceeding.
- If none of those messages appeared, go to the next step.

Step 3 The CUE module service engine can be given a private IP address if necessary. If you want to give the service engine a private IP address, do so before starting the wizard by completing these steps. If you don't need to give the service engine a private IP address and can use an unnumbered address, skip these steps and go to Step 4.

a. From the tools menu, choose **Telnet**.

b. In the displayed dialog, choose the device to which you need to connect, and click **OK**.

c. At the Cisco IOS command prompt, enter the command **config terminal**, as shown in the following example:

Router#**config termina**l

Router(config)#

d. Enter the **interface service-engine** command as shown in the following example:

Router(config)# **interface service-engine0/1**

Router(config-if)#

e. Enter the **ip address** command as shown in the following example:

f. Router(config-if)# **ip address 172.168.3.2 255.255.255.0**

g. Leave configuration mode by entering the command **end**.

h. Log off the router and close the Telnet window.

Step 4 Click **Configure** > **Interface Management** > **Module Configuration** > **CUE**.

Step 5 In the Service Engine Interface Configuration screen, do the following:

a. Choose an interface for an unnumbered IP address. If you gave the service engine a private IP address, this step is already completed.

b. Enter an IP address for Cisco Unity Express. This should be in the same subnet as the service engine IP address.

See Service Engine Configuration for more information.

Step 6 Click **Next**.

Step 7 In the Cisco Unity Express Module Configuration screen, provide the hostname, NTP server information, and other initialization parameters. See CUE Module Initialization for more information.

Step 8 Click **Next** to display the Initialization Confirmation screen. This screen describes the process that will occur when initialization starts, and informs you that the process cannot be halted once begun. If you want to return to any screen to change settings, click the **Back** button and do so, then return to this screen to start the initialization process.

Step 9 Click **Next** to start initialization.

Step 10 In the Cisco Unity Express Module Initialization screen, view the progress of initialization. Click **Next** when the process is complete.

Step 11 In the Complete screen, click **Finish** to close the wizard.

CUE Initialization Wizard Screen Reference

This section contains the following parts:

- Service Engine Configuration
- CUE Module Initialization
- Initialization Confirmation
- Cisco Unity Express Module Initialization
- Complete

Service Engine Configuration

In this screen, configure the service engine IP addresses.

How to get to this screen

Click **Configure > Interface Management > Module Configuration > CUE**.

Related Links

- Discovery Details Messages
- Initialization Procedure

Field Reference

Table 61-1 Service Engine Configuration

Element	Description
Service Engine IP address	This field appears if the Cisco IOS CLI has been used to configure the service engine with a private IP address. The IP address is displayed in this field. This field is read only.
Service Engine IP unnumbered interface	(Mandatory). If the service engine has not been configured with a private IP address, this field appears, and lists all available interfaces, including interfaces which are administratively shut down. You must choose an interface for the service engine from this list. If you choose an interface that is administratively shut down, an alert message is displayed asking you to select a different interface.
Cisco Unity Express IP address	(Mandatory). In this field, configure the CUE IP address. You must use an IP address that is in the same subnet as the IP address of the service engine. This is the case whether the service engine has a private IP address, or an unnumbered IP address.
Cisco Unity Express default gateway	This field displays the IP address of the service engine, whether it is a private IP address or an unnumbered IP address. This field is read only.

CUE Module Initialization

In this screen, enter the parameters to use when initializing the CUE module.

How to get to this screen

Click **Configure** > **Interface Management** > **Module Configuration** > **CUE**. Then click **Next** until you get to this screen.

Related Links

- Initialization Procedure
- Voicemail Settings

Field Reference

Table 61-2 CUE Module

Element	Description
Hostname	Enter the hostname for the CUE module. If you do not enter a hostname, the IP address entered in the Service Engine Configuration screen is used, and given the following a format where periods are replaced by dashes, and the letters se are prepended to the address. For example, an address of 10.1.10.1 would be formatted as follows: `se-10-1-10-1`
Domain Name	Enter the domain name for the CUE module.
Primary DNS Server	Enter the IP address of the DNS server that the CUE module will use.
Primary NTP Server	(Mandatory if enabled). This field is enabled if the NTP status on the router is synchronized. The default value is the IP address of the router. If the NTP status is not synchronized, this field is disabled, and the System Date and Time field is enabled.
Secondary NTP Server	Enter the IP address of the secondary NTP server. This field is enabled if the NTP status on the router is synchronized. Otherwise, the field is disabled.

Table 61-2 CUE Module (continued)

Element	Description
System Date and Time	(Mandatory if enabled). This field is enabled if the Primary NTP Server field is disabled. Synchronize with PC clock is checked by default, but you can uncheck it to enable the time field and enter the time manually. To choose the date, click the calendar icon and navigate to the correct date.
Continent	(Mandatory). Choose the continent in which the device is located.
Country	(Mandatory). Choose a country within the chosen continent. If no countries are available for the continent chosen, this field is disabled, but you can choose a time zone from the Time Zone field.
Time Zone	(Mandatory). Choose the time zone in which the device is located. If the country or continent chosen does not use time zones, then this field is disabled.
Administrative Username	(Mandatory). Enter a username for the administrator of the CUE module. The default value for this field is the username for the router.
Administrative Password	(Mandatory). Enter a password for the administrator of the CUE module. The default value for this field is the password for the router.
Skip GUI initialization wizard	Leave this box checked if you want to configure the CUE GUI initialization parameters manually. **Note** If you check **Skip GUI initialization wizard,** you must also check **Configure message waiting indicator** in the Voicemail Settings screen to properly configure both the CUE module and Cisco Communications Manager Express.

Initialization Confirmation

This screen informs you of the time that initialization can take, the results of the initialization process, and that once begun, the initialization process cannot be stopped.

How to get to this screen

Click **Configure** > **Interface Management** > **Module Configuration** > **CUE**. Then click **Next** until you get to this screen.

Related Links

- Initialization Procedure

To start initialization

To start initialization, click **Next**.

To return to configuration screens to review or make changes

To return to any of the screens in which you made settings, click **Back** until you reach the screen.

Cisco Unity Express Module Initialization

This screen displays a progress bar to report the progress of the initialization operation.

How to get to this screen

Click **Configure** > **Interface Management** > **Module Configuration** > **CUE**. Then click **Next** until you get to this screen.

Related Links

Initialization Procedure

Complete

This screen summarizes the results of the operation and enables you to close the wizard by clicking **Finish**.

How to get to this screen

Click **Configure > Interface Management > Module Configuration > CUE**. Then click **Next** until you get to this screen.

Related Links

- Initialization Procedure

Discovery Details Messages

During discovery, the following messages may be displayed in the Discovery Details window.

- **Unity Express module is not installed**. The Cisco Unity Express module is not installed on the device being discovered. All voicemail features are disabled in this case.
- **Unity Express module is not steady state**. The Cisco Unity Express module on the device being discovered is not reachable because the module is being shutdown or is already shutdown. All voicemail features are disabled in this state. You must restart the module and rediscover the device in order to configure voicemail features.
- **Unity Express module is in Offline mode**. The Cisco Unity Express module on the device being discovered is in offline mode. All Voicemail features are disabled. You must change the module to online mode and rediscover the device to configure voicemail features.
- **Unity Express module is in boot loader mode**. The Cisco Unity Express module on the device being discovered is in boot loader mode. All Voicemail features are disabled. You must bring the module to online mode and rediscover the device to configure voicemail features.
- **Unity Express is installed with CCM license**. The Cisco Unity Express module is installed with a Cisco Configuration Manager (CCM) license that is not supported by Cisco CP. You must upgrade the license to the latest version of Cisco Manager Express (Cisco Unified CME) and rediscover the device in order to configure voicemail features.
- **Unity Express version is not supported**. The supported versions of Cisco Unity Express module are versions 2.3, 3.0, and 3.1. Older releases are not supported.

- **Unity Express is reloading**. An attempt might have been made to reload the Cisco Unity Express module during discovery. You must until the Cisco Unity Express module reload is complete, and then rediscover the device in order to configure voicemail features.

Configuring Module Settings

For information about how to use Cisco Configuration Professional (Cisco CP) to configure Module Settings, see the screencast at: http://www.cisco.com/en/US/docs/net_mgmt/cisco_configuration_professional/scrcst/ccpsc.html.

Note You must have internet access to view the screencast.

Configuring Voicemail

Voicemail initial setup configuration specifies the capacity of the voice system as a whole, and default mailbox settings. Default mailbox settings can be overridden when configuring mailbox settings for specific users.

Voicemail Reference

The following topics describe the window used to configure voicemail:

- Voicemail Settings

Voicemail Settings

In the Mailbox Defaults screen, enter the system capacity settings and specify default values for individual voice mailboxes.

How to get to this screen

Click **Configure > Unified Communications > Voicemail > Voicemail Settings**.

Related Links

- Configuring Voicemail
- CUE Module Initialization

Field Reference

Table 61-3 Mailbox Defaults

Element	Description
System Wide	
System Capacity	The total number of voicemail minutes to store on the system. For AIM-CUE, enter a value from 1 to 840 minutes. For NM-CUE, enter a value from 1 to 6000 minutes. For NM-CUE-EC, enter a value from 1 to 18000 minutes. (The upper limit might vary, based on the type of Cisco Unity Express installed (AIM-CUE, NM-CUE, NME-CUE).)
Maximum Greeting Recording Size	The total number of seconds of greetings to store on the system. Enter a value from 10 to 3,600 seconds.
Play Caller ID of External Callers	Specify whether or not the system is to play the caller ID of an external caller by choosing one of the following: • Disable—Do not play the caller ID of external callers. • Enable—Play the caller ID of external callers when it is available.
Mailbox	
The values that you enter in the following fields are default values that can be overridden when configuring user mailboxes.	
Voice Mailbox Size	The default maximum number of seconds of stored messages allowed for voice mailboxes.
Maximum Caller Message Size	The default maximum size, in seconds, of a message that can be left by a caller in the voice-mail system.
Voice Mail Message Expiration	The default number of days to store messages. After a message has been stored for the specified number of days, the user can resave the message or delete it.
Message Waiting Indicator	

Table 61-3 Mailbox Defaults (continued)

Element	Description
This area of the screen is disabled in the following circumstances: • If the message waiting indicator (MWI) type is already configured for unsolicited notify. Cisco CP does not support this value. • If any **ephone-dn** command contains the **mwi on** or the **mwi off** keywords. • If the MWI type is configured as sub-notify, but Cisco Communications Manager Express is configured for TCP transport. It must be configured for UDP transport for this area of the screen to be enabled.	
Configure message waiting indicator	To configure the message waiting indicator (mwi) type to **sub-notify**, which will cause Subscribe and Notify messages to be used to relay incoming DTMF signals to Cisco Unity Express, check **Configure message waiting indicator**. This will configure MWI on both CUE module and Cisco Communications Manager Express.

Configuring the Call-in Number

The call-in number is the number (trigger) that is called to invoke a particular application. This can be your main auto-attendant number, or a temporary one. Without a call-in number, you cannot test or launch a script.

Note The Cisco Unity Express IP configuration window configures the Service Engine/Integrated Service Engine interface of Cisco unity express module. If Cisco Unity Express is not in a proper state, this feature is not available.

How to get to this screen

Click **Configure > Unified Communications > Voicemail > Unity Express IP Configuration**.

Call-in Number Reference

The following topics describe the window used to Call-in Number parameters:

- Configure the Call-in Numbers
- Edit or Create Cisco Unity Express Call-in Numbers

Configure the Call-in Numbers

Enter the call-in number.

How to get to this screen

Click **Configure > Unified Communications > Voicemail > Call-in Numbers**.

Related Links

- Edit or Create Cisco Unity Express Call-in Numbers

Field Reference

Table 61-4 Unity Express Call-in Number

Element	Description
Call-in Number	The number that is called for which a particular application needs to be invoked (trigger).
Application Name	The application configured.
Max Call-in Sessions	The maximum number of callers who can concurrently access the application at any given time. This parameter is limited by the number of ports on the Cisco Unity Express module.
Locale	The locale being used by the application. (This is not configurable.)
Status	Displays **Complete** if there is a dial peer configured. Displays **Incomplete** if there is no dial peer configured.

Edit or Create Cisco Unity Express Call-in Numbers

Enter the call-in number parameters.

How to get to this screen

- Click **Configure > Unified Communications > Voicemail > Call-in Numbers > Create**.

Field Reference

Table 61-5 Add CUE Application Trigger

Element	Description
Call-in number	Enter the call-in number. For Edit Call-in Number will be read-only. You can create more than one trigger for the same application. A duplicate call-in number is not allowed.
Application Name	Choose one of the applications. (ciscomwiapplication and msgnotification are not supported.)
Max Call-in Sessions	Enter the maximum number of call-in sessions for the application. The total number allowed is limited by the Usable System port of the module and by the application selected. If you selected the promptmgmt application the value for this field is 1.
Locale	This field is not editable. It displays the default value **systemDefault**.

Auto-complete

If an application is found that has a trigger but no dial-peer configured in Cisco Unified Call Manager Express, the status of the Call-in Number is **Incomplete**. You can use Auto-complete to create the dial peer for the application.

To create a dial-peer for this application, select the **Call-in Number** and click **Auto-complete**.

If the task is successful, the status changes from **Incomplete** to **Complete**.

Launching Cisco Unity Express

The Cisco Unity Express option opens the Cisco Unity Express Voice Mail (CUE) login window. You can open as many CUE windows as you want, but you must repeat the discovery process for the same router to synchronize the configuration with Cisco Configuration Professional.

Note The Cisco Unity Express IP configuration window configures the Service Engine/Integrated Service Engine interface of Cisco unity express module. If Cisco Unity Express is not in a proper state, this feature is not available.

Caution Do not make changes on the same router by using Cisco Configuration Professional and CUE simultaneously. The configurations might conflict.

Cisco Unity Express Reference

- Launch Cisco Unity Express

Launch Cisco Unity Express

You can launch the Cisco Unity Express application from within Cisco Configuration Professional.

Caution After configuring the device with Cisco Unity Express GUI, you must re-discover the device by using Cisco Configuration Professional before using Cisco Configuration Professional to add or modify Voicemail configurations.

How to get to this screen

Click **Configure > Unified Communications > Voicemail > Cisco Unity Express**.

Field Reference

Table 61-6 Launch Unity Express GUI

Element	Description
Cisco Unity Express IP	IP address of CUE service engine. This IP address must be routable to launch the CUE window. The field is auto-populated and it is not editable.
Launch Cisco Unity Express GUI	Launches the CUE window. It displays a user confirmation dialog.

Caution Do not make changes on the same router by using Cisco Configuration Professional and Cisco Unity Express simultaneously.

Related Link

- Launching Cisco Unity Express

CHAPTER 62

Media Resource Management and Transcoding

For information about how to use Cisco Configuration Professional (Cisco CP) to configure the Media Resource Management and Transcoding feature, see the screencast at: http://www.cisco.com/en/US/docs/net_mgmt/cisco_configuration_professional/scrcst/ccpsc.html.

Note You must have internet access to view the screencast.

PART 6

Configuring Utilities

This section provides information about how to configure Cisco CP utilities. I also provides information about viewing the running configuration, IOS show commands, and default rules.

CHAPTER 63

Utilities

This chapter provides information about Cisco Configuration Professional (Cisco CP) utilities and information about how to view the running configuration, IOS show commands, and default rules. The following sections provide more information:

- Understanding Utilities, page 63-1
- Utility Reference, page 63-2
- Understanding the View Menu Options, page 63-16
- View Reference, page 63-17

Understanding Utilities

Cisco CP provides the following utilities:

- Flash File Management—Manages the files in Flash memory. See Flash File Management, page 63-2.
- Software Upgrade—Manages the software image upgrade. See Software Upgrade Page, page 63-4.
- Configuration Editor—Allows you to edit the router configuration file. See Configuration Editor, page 63-8.
- Save Configuration to PC—Saves the device running configuration to a file on the PC. See Save Configuration to PC Page, page 63-9.
- Write to Startup Configuration—Writes from the running configuration to the startup configuration. See Write to Startup Configuration Page, page 63-9.

- Telnet—Opens the Telnet dialog box from where you can telnet into a selected device. See Telnet Page, page 63-10.
- Reload Device—Reloads the router. See Reload Device Page, page 63-11.
- Ping and Traceroute—Allows you to ping a remote host and traceroute the path of the packets on the network. See Understanding Ping and Traceroute, page 63-11.

Note The utilities are available under the Home, Configure, and Monitor tabs with at least one device discovered. In offline mode, the utilities are not available.

Utility Reference

This section describes the pages and dialog boxes you can use when working with the Cisco CP utilities and includes the following topics:

- Flash File Management, page 63-2
- Configuration Editor, page 63-8
- Save Configuration to PC Page, page 63-9
- Write to Startup Configuration Page, page 63-9
- Telnet Page, page 63-10
- Reload Device Page, page 63-11

Flash File Management

For information about how to use Cisco Configuration Professional (Cisco CP) to configure the Flash File Management utility, see the screencast at: http://www.cisco.com/en/US/docs/net_mgmt/cisco_configuration_professional/scrcst/ccpsc.html.

You must have Internet access to view the screencast.

Software Upgrade

The software upgrade feature allows you to upgrade the device software. You can download the software images from Cisco.com website and upgrade the software image on the device.

Managing Software Upgrade

Note Software Upgrade is supported only on Cisco CGS-2520-24TC and CGS-2520-16S-8PC series switches.

Prodedure

Use this procedure to upgrade the software image.

Step 1 Choose **Configure > Utilities > Software Upgrade**. The Software Upgrade dialog box opens. See Software Upgrade Page, page 63-4.

Step 2 Click the **Launch Wizard..** button. The Welcome page opens.

Step 3 From the Welcome page, click the **Next** button. The Download Image From CCO page opens.

Step 4 From the Download Image From CCO page, click the **Download From CCO** button.

Step 5 Download the image from CCO page.

Note If you do not have the CCO login account, register on the CCO page. If you already have a software image available in your Personal Computer (PC) or in the Remote TFTP server, then skip step 4 and step 5.

Step 6 After downloading the software image, click the **Next** button. The Save Existing Image and Config page opens.

Step 7 From the Save Existing Image and Config page, save the existing image on the flash and running configuration to a PC or to a remote TFTP server.

Step 8 After saving the existing software image, click the **Next** button. The Select and Upload Image page opens.

Step 9 From the Select and Upload Image page, browse and upload the image from your PC or enter the name of the software image that is available from a remote TFTP server. If the remote TFTP option is selected, enter the path of the TFTP server in the Remote TFTP text box.

Step 10 Browse and select the IOS Image Name.

Step 11 Click the **Finish** button to upload the selected image.

Step 12 Click the **Cancel** button to cancel the changes that you entered.

Software Upgrade Page

From the Software Upgrade page, click the **Launch Wizard..** button. The Welcome page opens. From the Welcome page, follow the instructions to upgrade the software image.

How to Get to This Page

Choose **Configure > Utilities > Software Upgrade**.

Related Topics

- Welcome Page, page 63-4
- Download Image From CCO Page, page 63-5
- Save Existing Image and Config Page, page 63-6
- Select and Upload Image Page, page 63-7
- Managing Software Upgrade, page 63-3
- Understanding Utilities, page 63-1

Welcome Page

From the Welcome page, click the **Next** button. The Download Image From CCO page opens. The Welcome page provides the instructions to upgrade the software image.

How to Get to This Page

Choose **Configure > Utilities > Software Upgrade**.Click the **Next** button until you get to this page.

Related Topics

- Software Upgrade, page 63-3
- Download Image From CCO Page, page 63-5
- Save Existing Image and Config Page, page 63-6
- Select and Upload Image Page, page 63-7
- Managing Software Upgrade, page 63-3
- Understanding Utilities, page 63-1

Field Reference

Table 63-1 Welcome Page

Element	Description
Next	Click the **Next** button to go the next page.
Cancel	Click the **Cancel** button to cancel the changes that you have entered.

Download Image From CCO Page

Use the Download Image From CCO page to download the software image from the Cisco.com site.

How to Get to This Page

Choose **Configure > Utilities > Software Upgrade**.Click the **Next** button until you get to this page.

Related Topics

- Software Upgrade, page 63-3
- Welcome Page, page 63-4
- Save Existing Image and Config Page, page 63-6
- Select and Upload Image Page, page 63-7

- Managing Software Upgrade, page 63-3
- Understanding Utilities, page 63-1

Field Reference

Table 63-2 Download Image From CCO Page

Element	Description
Download Form CCO	Click the **Download From CCO** button to download the software image. If you do not have CCO login account, register in the CCO page. If you already have an image available in your PC or in a Remote TFTP server, then skip this step.
Back	Click the **Back** button to go back to the previous page.
Next	Click the **Next** button to go the next page.
Cancel	Click the **Cancel** button to cancel the changes that you have entered.

Save Existing Image and Config Page

Use the Save Existing Image and Config page to save the existing image on the flash and running configuration to a PC or to a remote TFTP server.

How to Get to This Page

Choose **Configure > Utilities > Software Upgrade**.Click the **Next** button until you get to this page.

Related Topics

- Software Upgrade, page 63-3
- Welcome Page, page 63-4
- Download Image From CCO Page, page 63-5
- Select and Upload Image Page, page 63-7
- Managing Software Upgrade, page 63-3
- Understanding Utilities, page 63-1

Field Reference

Table 63-3 Save Existing Image and Config

Element	Description
Save to	Choose PC or Remote TFTP to save the existing image on the flash and running configuration to a PC or to a remote TFTP server.
Remote TFTP	Specify the remote TFTP path for the software image.
Save image	Click the **Save Image** button to save the software image.
Save running configuration	Click the **Save Running Configuration** button to save the running configuration.
Back	Click the **Back** button to go back to the previous page.
Next	Click the **Next** button to go the next page.
Cancel	Click the **Cancel** button to cancel the changes that you have entered.

Select and Upload Image Page

Use the Select and Upload Image page to upload the software image.

How to Get to This Page

Choose **Configure > Utilities > Software Upgrade**. Click the **Next** button until you get to this page.

Related Topics

- Software Upgrade, page 63-3
- Welcome Page, page 63-4
- Download Image From CCO Page, page 63-5
- Save Existing Image and Config Page, page 63-6
- Managing Software Upgrade, page 63-3
- Understanding Utilities, page 63-1

Field Reference

Table 63-4 Select and Upload Image Page

Element	Description
Upload image from	Browse and upload the image from your PC or enter the name of the software image that is available from a remote TFTP server. If the remote TFTP option is selected, enter the path of the TFTP server in the Remote TFTP text box.
ISO image name	Browse and select the IOS image name.
Back	Click the **Back** button to go back to the previous page.
Finish	Click the **Finish** button to upload the selected image.
Cancel	Click the **Cancel** button to cancel the changes that you have entered.

Configuration Editor

For information about how to use Cisco CP to work with the Configuration Editor utility, see the screencast at: http://www.cisco.com/en/US/docs/net_mgmt/cisco_configuration_professional/scrcst/ccpsc.html.

You must have Internet access to view the screencast.

Save Configuration to PC Page

From the Save Configuration to PC page, click the **Save Running Configuration to PC** button. The Save Location to Download from Local Host page opens. From the Save In drop-down list, select the location on your PC to save the running configuration file, and then click **Save**.

How to Get to This Page

Choose **Configure > Utilities > Save Configuration to PC**.

Related Topics

- Understanding Utilities, page 63-1

Write to Startup Configuration Page

From the Write to Startup Configuration page, click the **Confirm** button to copy the device running configuration to the startup configuration.

How to Get to This Page

Choose **Configure > Utilities > Write to Startup Configuration**.

Related Topics

- Understanding Utilities, page 63-1

Telnet Page

From the Telnet page, click the **Launch Telnet Window** button to open the Telnet window from where you can telnet to a selected device.

Note

- Cisco Security Agent or any other antivirus software that is installed on your PC might block Cisco CP from opening the Telnet command window. If this occurs, go to **Start > Run**, enter **cmd**, and then enter **telnet *<ip address>*** in the command window, to telnet to the device.
- Port 23 is used to telnet to discovered devices that have secure connection.
- Launching telnet from Cisco CP is not supported on a Windows 7 64-bit machine.

How to Get to This Page

Choose **Configure > Utilities > Telnet**.

Related Topics

- Understanding Utilities, page 63-1

Reload Device Page

From the Reload Device page, click the **Reload device** button to reload the device.

Note Reloading the device is a time consuming operation. Successful reload requires flash with IOS image or TFTP path pointing to IOS image.

How to Get to This Page

Choose **Configure > Utilities > Reload Device**.

Related Topics

- Understanding Utilities, page 63-1

Understanding Ping and Traceroute

The Cisco CGS 2520 switch supports the IP ping and traceroute features.

The following sections provide more information:

- Configuring Ping and Traceroute, page 63-14
- Ping and Traceroute Dialog Box, page 63-15

Note The following options are available on ISR and ISR-G2 devices:

- Basic ping
- Basic traceroute
- Advanced ping
- Layer 3 traceroute

Layer 2 IP traceroute and layer 2 MAC traceroute are not available on ISR and ISR-G2 devices.

Ping

The IP ping feature allows the switch to test the connectivity to the remote hosts. Ping sends an echo request packet to an address and waits for a reply.

Also, the Cisco CGS 2520 switch provides the Control Plane Security feature, which by default drops ping response packets received on User Network Interfaces (UNIs) or Enhanced Network Interfaces (ENIs). However, methods are available to ping successfully from the switch to a host connected to a UNI or ENI.

Control Plane Security does not drop ping response packets to or from the Network Node Interfaces (NNIs), and no special configuration is required to enable ping to or from hosts connected.

Layer 2 Traceroute

The Layer 2 traceroute feature allows the switch to identify the physical path that a packet takes from a source device to a destination device. The Layer 2 traceroute feature supports only unicast source and destination MAC addresses. It finds the path by using the MAC address tables of the switches in the path. When the switch detects a device in the path that does not support Layer 2 traceroute, the switch continues to send the Layer 2 trace queries and lets them time out.

Note Layer 2 traceroute feature is available only on NNIs.

The switch can only identify the path from the source device to the destination device. It cannot identify the path that a packet takes from source host to the source device or from the destination device to the destination host.

Layer 3 Traceroute

The Layer 3 traceroute feature allows the switch to identify the path that packets take through the network on a hop-by-hop basis.

To identify the next hop, traceroute sends an User Datagram Protocol (UDP) packet with a Time-to-Live (TTL) value of two. The first router decrements the TTL field value by one and sends the datagram to the next router. The second router receives a TTL value of one, discards the datagram, and returns the time-to-live-exceeded message to the source. This process continues until the TTL is incremented to a value that is large enough for the datagram to reach the destination host (or until the maximum TTL is reached).

Configuring Ping and Traceroute

Procedure

Use this procedure to ping the remote host and traceroute the path of the packets on the network.

Step 1 Choose **Configure > Utilities > Ping and Trace**. The Ping and Traceroute configuration dialog box opens. See Ping and Traceroute Dialog Box, page 63-15.

Step 2 To ping the remote host, do the following:

a. Enter the destination IP address or the hostname, and click the **Ping** button or click the **Advanced** button and check the **Ping** radio button.

b. From the Ping and Traceroute dialog box, enter the source IP address and the destination IP address of the switch.

c. Click the **Ping** button.

Step 3 To traceroute the path of the packets on the network, enter the destination IP address or the hostname, and click the **Traceroute** button or click the **Advanced** button and check the **Layer 3 Traceroute** or **Layer 2 Traceroute** radio button.

a. For the Layer 3 traceroute option, enter the destination IP address or the hostname, and click the **Traceroute** button.

b. For the Layer 2 traceroute option, if you check the IP check box, enter the source and destination IP address or the source and destination hostname, and click the **Traceroute** button.

c. For the Layer 2 traceroute, if you check the MAC check box, enter the source and destination MAC address or the source and destination hostname.

d. Select the Source Interface from the drop-down list.

e. Select the Destination Interface from the drop-down list.

f. Enter the VLAN ID. The VLAN ID range is 1 to 4094.

g. Click the **Traceroute** button.

Step 4 Click the **Basic** button to go back to the basic ping and trace dialog box.

Step 5 Click the **Clear** button to avoid the changes that you entered.

Ping and Traceroute Dialog Box

Use this page to the ping the remote host and traceroute the path of the packets on the network.

How to Get to This Page

Choose **Configure > Utilities > Ping and Traceroute**.

Related Topic

- Understanding Ping and Traceroute, page 63-11
- Configuring Ping and Traceroute, page 63-14
- Understanding Utilities, page 63-1

Field Reference

Table 63-5 Ping and Trace Dialog Box

Elements	Description
Destination	Specify the destination IP address.
Advanced	Click the advanced button to display more options. Displays the following options: • Ping • Layer 3 Traceroute • Layer 2 Traceroute
Ping radio button	Check this radio button to ping the remote host.
Layer 3 Traceroute radio button	Check Layer 3 Traceroute radio button to traceroute the Layer 3 path of the packets.
Layer 2 Traceroute radio button	Check the Layer 2 Traceroute radio button to traceroute the Layer 2 path of the packets.
IP radio button	Check the IP radio button to traceroute the path by providing the IP address.
MAC radio button	Check the MAC radio button to traceroute the path by providing the MAC address.
Source	Specify the source IP address.
Destination	Specify the destination IP address.

Table 63-5 Ping and Trace Dialog Box

Elements	Description
Source interface	Choose the source interface from the drop-down list.
Destination interface	Choose the destination interface from the drop-down list
VLAN	Specify the VLAN ID.
Ping	Click the **Ping** button to ping a remote host by providing the hostname or the IP address.
Traceroute	Click the **Traceroute** button to traceroute the path of the packets on the network.
Basic	Click the **Basic** button to go back to the basic ping and traceroute dialog box.
Clear	Click the **Clear** button to clear the changes that you entered.

Understanding the View Menu Options

Cisco CP allows you to view the following:

- Running Configuration—Displays the running configuration of a selected device. See Running Configuration Page, page 63-17.
- IOS Show Commands—Displays the results of the **show** command. You can either choose a **show** command from the drop-down list, or you can enter a **show** command in the field provided, and then click the **Show** button to display the results. See IOS Show Commands Page, page 63-17.
- Default Rules—Displays the default access list rule set. See Default Rules Page, page 63-19.

View Reference

This section describes the pages and dialog boxes you can use when working with the View left navigation pane menu items and includes the following topics:

- Running Configuration Page, page 63-17
- IOS Show Commands Page, page 63-17
- Default Rules Page, page 63-19

Running Configuration Page

Use the Running Configuration page to display the device running configuration. You can copy and paste the displayed text into an e-mail or a file for further analysis.

How to Get to This Page

Choose **Configure > Utilities > View > Running Configuration**.

Related Topics

- Understanding the View Menu Options, page 63-16
- IOS Show Commands Page, page 63-17
- Default Rules Page, page 63-19

IOS Show Commands Page

Use the IOS Show Commands page to display the results of the show command. You can either choose a show command from the drop-down list, or you can enter a show command in the field provided, and then click the **Show** button to display the results.

- You can choose one of the following show commands from the drop-down list:
  - **show flash**—Shows the contents of flash memory.
  - **show startup-config**—Shows the device startup configuration. This is the configuration that the device uses if it is restarted.

  - **show access-lists**—Shows the access lists configured on the device.
  - **show diag**—Shows hardware diagnostic information, such as hardware revision number, PCB serial number, and CLEI code.
  - **show interfaces**—Shows protocol and statistics information on all device interfaces.
  - **show version**—Shows the Cisco IOS version, the Cisco IOS image name, the configuration register settings, and a summary of interfaces and modules.
  - **show tech-support**—Shows the current software image, configuration, controllers, counters, stacks, interfaces, memory, and buffers.
  - **show environment**—Shows the status of electrical and mechanical elements of the device, such as fan status, input voltage status, and thermal status.
  - **show run**—Shows the configuration information currently running on the device.

- You can enter any show command that is supported by the device in the field provided. For example, enter:

```
show dial-peer voice
```

How to Get to This Page

Choose **Configure > Utilities > View > IOS Show Commands**.

Related Topics

- Understanding the View Menu Options, page 63-16
- Running Configuration Page, page 63-17
- Default Rules Page, page 63-19

Default Rules Page

Use the Default Rules page to display a list of all of the default rules configured by Cisco CP. This page is organized with a tree on the left side of the screen displaying options for Access Rules, Services, Firewall, VPN - IKE Policy, and VPN - Transform Sets. To view the default rules for these options, click the option in the tree, and the default rules for that option are displayed on the right.

How to Get to This Page

Choose **Configure > Utilities > View > Default Rules**.

Related Topics

- Understanding the View Menu Options, page 63-16
- Running Configuration Page, page 63-17
- IOS Show Commands Page, page 63-17
- More About IKE, page 97-21

Field Reference

Table 63-6 lists the elements on the Default Rules page.

Table 63-6 Default Rules Page

Element	Description
Access rules	Shows all of the default ACL[1] rules and a brief description of each, as shown in the following example: `SDM_DEFAULT_190ExtendedPermit IPSec VPN Pass-through` SDM_DEFAULT_190 is an extended access rule that is available to permit IPSec VPN traffic to pass through a configured firewall. Clicking on an access rule displays the rules defined for it, in detail. The Access Rules option is available when the ACL Editor is configured under **Configure > Router > ACL > ACL Editor**.

Table 63-6 Default Rules Page (continued)

Element	Description
Services	Shows the available Cisco CP services and the protocols that they use, as shown in the following example: `SDM_HTTPS tcp` The SDM_HTTPS service uses the TCP protocol. The Services option is available when the firewall is configured under **Configure > Security > Firewall > Firewall**.
Firewall	Shows default Application Security policies of Cisco CP. Choose the security policy to view from the list in the upper right corner of the window. • High Security—Prevents the use of Instant Messaging and Point-to-Point applications on the network. It monitors HTTP and e-mail traffic and drops traffic that does not comply with the protocol it uses. It returns other TCP and UPD traffic for sessions started inside the firewall. • Medium Security—Monitors the use of Instant Messaging and Point-to-Point applications, and HTTP and e-mail traffic. It returns other TCP and UPD traffic for sessions started inside the firewall. • Low Security—Does not monitor application traffic. It returns other TCP and UPD traffic for sessions started inside the firewall. The Services option is available when the firewall is configured under **Configure > Security > Firewall > Firewall**. **Note** Zone-based firewall rules are listed only when the firewall type selected is ZBF, otherwise classic firewall rules are displayed.
VPN–IKE Policy	Shows the default IKE[2] policies. For more information on IKE policies, see More About IKE. The VPN–IKE Policy option is available when the VPN is configured under **Configure > Security > VPN**.

Table 63-6 Default Rules Page (continued)

Element	Description
VPN–Transform Sets	Shows the default IPSec[3] transform sets. The VPN–Transform Sets option is available when the VPN is configured under **Configure > Security > VPN**.

1. ACL = Access Control List.
2. IKE = Internet Key Exchange.
3. IPSec = IP Security.

This Feature Not Supported

This window appears when a Cisco CP feature is not supported. This may be because the device is running a Cisco IOS image that does not support the feature or because Cisco CP is being run on a PC and cannot support the feature.

PART 7

Managing Modules

This section provides information about how to manage modules.

CHAPTER 64

WAN Optimization

Cisco's Wide Area Application Services (WAAS) is a WAN optimization and application acceleration solution that enables branch office server consolidation, improves performance for centralized applications, and provides remote users with LAN-like access to applications, storage, and content across the WAN.

Note The terms WAAS module and WAN Optimization module are used interchangeably in this document.

The following sections provide more information:

- Understanding WAAS, page 64-2
- Configuring a WAN Optimization Module Interface, page 64-3
- WAN Optimization Module Setup Wizard Page, page 64-5
- WAAS Central Manager, page 64-16

Understanding WAAS

The WAAS solution has three major components:

- WAAS Modules—WAAS modules are of the following two types:
  - Wide Area Application Services Network Module (WAAS-NM)—The WAAS-NM for the Cisco Integrated Services Routers (ISR) is a powerful WAN optimization and application acceleration solution that enables branch office server consolidation, improves performance for centralized applications, and provides remote users with LAN-like access to applications, storage, and content across the WAN. The WAAS-NMs are designed for deployment as edge devices. See the Cisco CP release notes for the supported WAAS-NMs:

    http://www.cisco.com/en/US/products/ps9422/prod_release_notes_list.html

Note The network module is also referred to as the integrated service engine (ISE) on the Cisco IOS CLI. The network module is a standalone Wide Area Application Engine (WAE) with its own startup and run-time configurations that are independent of the Cisco IOS configuration on the router.

  - Wide Area Application Services Service Module (WAAS-SM)—See the Cisco CP release notes for the supported WAAS-SMs:

    http://www.cisco.com/en/US/products/ps9422/prod_release_notes_list.html

- Web Cache Communication Protocol (WCCP)—WCCP is a Cisco protocol that specifies interactions between one or more routers or Layer 3 switches, and one or more application appliances, web caches, and caches of other protocols. The purpose of the interaction is to establish and maintain the transparent redirection of selected types of traffic flowing through a group of routers to a group of appliances. Any type of TCP traffic can be redirected.
- WAAS Central Manager (WCM)—The WCM provides a centralized mechanism for configuring features, reporting, and monitoring thousands of Cisco WAE nodes. The WCM can be accessed from a web browser, allowing management from anywhere in the world. Access to the WCM is secured and encrypted with Secure Sockets Layer (SSL), and users can be authenticated through a local database or a third-party authentication service such as RADIUS, TACACS, or Microsoft Active Directory.

Related Topics

- Configuring a WAN Optimization Module Interface, page 64-3
- WAN Optimization Module Setup Wizard Page, page 64-5
- WAAS Central Manager, page 64-16

Configuring a WAN Optimization Module Interface

You must have a WAAS module installed on the router to configure WAAS.

To configure IP settings on the installed WAAS modules, see the Module Configuration screencast at:

http://www.cisco.com/en/US/docs/net_mgmt/cisco_configuration_professional/scrcst/ModCfg/Modconfig_skin.swf

Related Topics

- Understanding WAAS, page 64-2
- WAN Optimization Module Setup Wizard Page, page 64-5
- WAAS Central Manager, page 64-16

WAN Optimization Reference

This section describes the pages and dialog boxes you can use when working with WAAS and includes the following topics:

- WAN Optimization Module Setup Wizard Page, page 64-5
- WAAS Central Manager, page 64-16

WAN Optimization Module Setup Page

See the following topics as appropriate:

- WAN Optimization Module Setup Wizard Page, page 64-5
- WAAS Central Manager, page 64-16

WAN Optimization Module Setup Wizard Page

Use this page to launch the WAN Optimization Module Setup wizard.

Note Choose the router with the WAAS module installed, from the Select Community Member drop-down list. The WAN Optimization feature is displayed in the left pane only if the router has a WAAS module installed with Cisco WAAS software version 4.1.1 or later and the module is in online state.

How to Get to this page

Click **Configure > Interface Management > Module Configuration > WAAS**.

Related Topics

- Understanding WAAS, page 64-2
- Configuring a WAN Optimization Module Interface, page 64-3
- Login Credentials Dialog Box, page 64-7
- WAN Optimization Module Setup Wizard—Welcome Page, page 64-8
- WAN Optimization Module Setup Wizard—Module Configuration page, page 64-9
- WAN Optimization Module Setup Wizard—Configure Interception Method, page 64-11
- WAN Optimization Module Setup Wizard—Select License, page 64-13
- WAN Optimization Module Setup Wizard—Summary, page 64-15
- WAAS Central Manager, page 64-16

Field Reference

Table 64-1 WAN Optimization Module Setup wizard

Element	Description
Select Module	Choose the module you want to configure on the router from the drop-down list. If only one module is present on the router, drop-down list is disabled.
Launch Wizard	Click the **Launch Wizard** button to configure the selected module on the router.

Login Credentials Dialog Box

Use the Login Credentials dialog box to provide the username and password to log in to the module. This dialog box is displayed if the default username and password for the module has changed.

How to Get to This Page

Click **Configure > Interface Management > Module Configuration > WAAS > Launch Wizard**.

Related Topics

- WAN Optimization Module Setup Wizard Page, page 64-5
- WAN Optimization Module Setup Wizard—Welcome Page, page 64-8

Table 64-2 Login Credentials Dialog Box

Element	Description
Username	Enter the username.
Password	Enter the password.

WAN Optimization Module Setup Wizard—Welcome Page

Use the welcome page to inform yourself about the available options and data required to complete the wizard.

How to Get to This Page

Click **Configure > Interface Management > Module Configuration > WAAS > Launch Wizard**.

Related Topics

- Understanding WAAS, page 64-2
- Configuring a WAN Optimization Module Interface, page 64-3
- WAN Optimization Module Setup Wizard Page, page 64-5
- WAN Optimization Module Setup Wizard—Module Configuration page, page 64-9
- WAN Optimization Module Setup Wizard—Configure Interception Method, page 64-11
- WAN Optimization Module Setup Wizard—Select License, page 64-13
- WAN Optimization Module Setup Wizard—Summary, page 64-15
- WAAS Central Manager, page 64-16

WAN Optimization Module Setup Wizard—Module Configuration page

Use this page to view and configure the host name, domain name, DNS IP address, NTP server IP address, time zone, WCM, and management interface.

How to Get to This Page

Click **Configure > Interface Management > Module Configuration > WAAS > Launch Wizard**.

Related Topics

- Understanding WAAS, page 64-2
- Configuring a WAN Optimization Module Interface, page 64-3
- WAN Optimization Module Setup Wizard Page, page 64-5
- WAN Optimization Module Setup Wizard—Welcome Page, page 64-8
- WAN Optimization Module Setup Wizard—Configure Interception Method, page 64-11
- WAN Optimization Module Setup Wizard—Select License, page 64-13
- WAN Optimization Module Setup Wizard—Summary, page 64-15
- WAAS Central Manager, page 64-16

Field Reference

Table 64-3 WAN Optimization Module Configuration

Element	Description
Host name	Module host name is displayed, if configured, otherwise the router's host name is displayed by default, if configured.
Domain name	Module domain name is displayed, if configured, otherwise the router's domain name is displayed by default, if configured.
Domain Name Server	Module domain name server is displayed, if configured, otherwise the router's domain name server is displayed by default, if configured.
Network Time Protocol Server	You need to enter the NTP server IP address.

Table 64-3 WAN Optimization Module Configuration (continued)

Element	Description
Time Zone	Configured time zone is displayed, if configured, otherwise the router-configured time zone is displayed by default, if configured.
WAAS Central Manager	You need to enter the WCM IP address to which the module is to be registered.
Management Interface	You need to choose Internal (via router) or External (via Faceplace connector) interface from the drop-down list, to communicate with the WCM. If external management interface is selected, enter the external interface IP address, choose the subnet mask from the drop-down list, and enter the module default gateway.

WAN Optimization Module Setup Wizard—Configure Interception Method

Use this page to configure the interception method WCCP Version 2.

How to Get to this Page

Click **Configure > Interface Management > Module Configuration > WAAS > Launch Wizard**.

Related Topics

- Understanding WAAS, page 64-2
- Configuring a WAN Optimization Module Interface, page 64-3
- WAN Optimization Module Setup Wizard Page, page 64-5
- WAN Optimization Module Setup Wizard—Welcome Page, page 64-8
- WAN Optimization Module Setup Wizard—Module Configuration page, page 64-9
- WAN Optimization Module Setup Wizard—Select License, page 64-13
- WAN Optimization Module Setup Wizard—Summary, page 64-15
- WAAS Central Manager, page 64-16

Field Reference

Table 64-4 WAN Optimization Select Interception Method

Element	Description
LAN Interface(s)	Select the Layer 3 interfaces to which TCP promiscuous mode service 61 is to be configured.

Table 64-4 WAN Optimization Select Interception Method (continued)

Element	Description
WAN Interface(s)	Select the Layer 3 interfaces to which TCP promiscuous mode service 62 is to be configured.
Router IP Address	Enter the router's IP address and click **Add** to add it to the list.
Router List	The router's IP address is displayed in the Router List. You can add a maximum of 4 routers for intercepting traffic with WCCP. Select the router's IP address from the Router List and click **Delete** if you want to remove it from the list.

WAN Optimization Module Setup Wizard—Select License

Use this page to choose the license.

Only valid and applicable licenses are displayed. If no license is configured, the default license is shown as selected.

The three licenses are Transport, Enterprise, and Enterprise and Video.

How to Get to this Page

Click **Configure > Interface Management > Module Configuration > WAAS > Launch Wizard**.

Related Links

- Understanding WAAS, page 64-2
- Configuring a WAN Optimization Module Interface, page 64-3
- WAN Optimization Module Setup Wizard Page, page 64-5
- WAN Optimization Module Setup Wizard—Welcome Page, page 64-8
- WAN Optimization Module Setup Wizard—Module Configuration page, page 64-9
- WAN Optimization Module Setup Wizard—Configure Interception Method, page 64-11
- WAN Optimization Module Setup Wizard—Summary, page 64-15
- WAAS Central Manager, page 64-16

Field Reference

Table 64-5 Select License

Element	Description
Transport	Cisco WAAS Transport license provides the WAN optimization features of Cisco WAAS. The WAN optimization features are DRE[1], LZ[2] compression, and TFO[3]. The features optimize application delivery to the branch office.
Enterprise	Cisco WAAS Enterprise license provides Cisco WAAS Transport license functions and application-specific accelerations for protocols. The license functions and accelerations include Common Internet File System CIFS[4], Messaging API MAPI[5], HTTP, SSL, NFS[6], and Windows print services. These facilitate application acceleration, WAN optimization, and IT consolidation.
Enterprise and Video	Cisco WAAS Video license provides Cisco WAAS Enterprise license functions and video application accelerator.

1. DRE = Data Redundancy Elimination.
2. LZ = Lempel-Ziv.
3. TFO = transport flow optimization.
4. CIFS = Common Internet File System.
5. MAPI = Messaging API
6. NFS = Network File System

You can select Transport or Enterprise or both Enterprise and Video.

Note NME-WAE-302 supports only Transport license. The following licenses are not supported on WAAS modules:

- Enterprise and Virtual blade
- Enterprise, Video, and Virtual blade

WAN Optimization Module Setup Wizard—Summary

Use this page to see the configuration summary and apply your changes to the WAAS module.

1. Click **Finish** to apply your changes to the WAAS module.
2. Click **Yes** in the confirmation dialog box.

How to Get to this Page

Click **Configure > Interface Management > Module Configuration > WAAS > Launch Wizard**.

Related Topics

- Understanding WAAS, page 64-2
- Configuring a WAN Optimization Module Interface, page 64-3
- WAN Optimization Module Setup Wizard Page, page 64-5
- WAN Optimization Module Setup Wizard—Welcome Page, page 64-8
- WAN Optimization Module Setup Wizard—Module Configuration page, page 64-9
- WAN Optimization Module Setup Wizard—Configure Interception Method, page 64-11
- WAN Optimization Module Setup Wizard—Select License, page 64-13
- WAAS Central Manager, page 64-16

WAAS Central Manager

Use this page to launch the WCM.

Note The Launch WAAS Central Manager button is displayed if the WAAS module was registered with the WCM as described in WAN Optimization Module Setup Wizard—Module Configuration page, page 64-9.

Note After the WAAS module is registered with the WCM, we recommend that you perform configuration modifications from the WCM GUI.

How to Get to this Page

Click **Configure > Interface Management > Module Configuration > WAAS > Launch WAAS Central Manager**.

Related Topics

- Understanding WAAS, page 64-2
- Configuring a WAN Optimization Module Interface, page 64-3
- WAN Optimization Module Setup Wizard Page, page 64-5
- WAN Optimization Module Setup Wizard—Welcome Page, page 64-8
- WAN Optimization Module Setup Wizard—Module Configuration page, page 64-9
- WAN Optimization Module Setup Wizard—Configure Interception Method, page 64-11
- WAN Optimization Module Setup Wizard—Select License, page 64-13
- WAN Optimization Module Setup Wizard—Summary, page 64-15

CHAPTER 65

WAAS Express Registration

The WAAS Express feature in Cisco Configuration Professional allows you to perform the following operations:

- Enable secure HTTP server on your router
- Enable evaluation or permanent license for WAAS Express on your router
- Install digital certificate for WCM on your router
- Register your router with the WAAS central Manager (WCM)

The following sections provide more information:

- WAAS Express Registration Basic Workflow, page 65-1
- Understanding WAAS Express, page 65-2
- Registering WAAS Express, page 65-2
- WAAS Express Registration Reference, page 65-4

WAAS Express Registration Basic Workflow

1. Enable evaluation license or permanent license.
2. Launch wizard to register with the WCM.

Understanding WAAS Express

Cisco WAAS Express is a small-footprint, cost-effective, IOS-based software solution integrated into the 88x, 89x, and Integrated Services Router (ISR) G2 to offer bandwidth optimization and application acceleration capabilities.

It increases remote user productivity, reduces WAN bandwidth costs, and offers investment protection by interoperating with existing Cisco WAAS infrastructure.

Cisco WAAS Express provides network transparency, improves deployment flexibility with on-demand service enablement, and integrates with native IOS-based services such as security, Netflow, and QoS.

The software is fully interoperable with WAAS on SM-SRE modules, WAAS appliances, and can be managed by a common WAAS Central Manager.

The WAAS Central Manager manages WAAS Express devices, which are Cisco routers deployed with the WAAS Express software. The WAAS Express software implements a subset of the WAAS appliance functionality, providing only basic optimization with no application acceleration. The WCM navigation menu displays a subset of the full menu when a WAAS Express device is selected as the context.

Registering WAAS Express

Procedure

Use this procedure to register the router with the WCM.

Step 1 From the Register with WCM page, click **Enable Evaluation License** to enable evaluation license or click **Enable Permanent License** to enable permanent license.

If you clicked the Enable Evaluation License button:

1. A Confirmation dialog box is displayed where you can review the End User License Agreement (EULA).
2. Check the Accept check box to accept the terms of the agreement.
3. Click **OK**.

If you clicked the Enable Permanent License button:

The Product License Registration page is displayed. Follow the instructions on the page to obtain a permanent license.

Note The Launch Wizard button to register the router with the WCM is active only after you have enabled a license.

Step 2 Click the Launch Wizard button.

The WAAS Express Registration wizard Welcome page is displayed.

Use this page to view the information you need to complete the wizard.

Step 3 Click **Next**.

The WAAS Central Manager page is displayed.

Step 4 Enter the IP address of the WAAS Central Manager. You can obtain this address from you network administrator.

Step 5 Click **Next**.

You will see a busy cursor while the WCM certificate is being obtained.

If Cisco CP is unable to obtain the certificate from WCM, the WCM Certificate page is displayed.

Use this page to view the steps to get the WCM certificate.

Step 6 Click **Next**.

If domain name is not configured on the router, the Domain Name Configuration page is displayed.

Step 7 Enter the domain name.

Step 8 Click **Next**.

The Digital Certificate page is displayed.

Step 9 Choose an existing self-signed digital certificate on the router, or create a new self-signed digital certificate, from the Digital Certificate drop-down list.

If you choose to create a new certificate:

1. Enter a name for the certificate in the Name field
2. Enter the size of the RSA key pair used in the certificate in the Key Size field. The range is between 512 and 2048.

Step 10 Click **Next**.

The WCM Login Credentials page is displayed.

Step 11 Click **This Router** radio button to have the WCM log in as a local user using user credentials configured on the router.

Or

Click **An external AAA server** radio button to have the WCM log in using the user credentials configured on an external AAA server.

If you clicked **This Router** radio button:

1. Check the **To create new user enter credentials below** check box to create a new user.
2. Enter the username for the new user in the Username field.
3. Enter the password for the new user in the Password field.
4. Enter the password again in the Confirm Password field.

If you clicked **An external AAA server** radio button:

1. From the Authentication List drop-down list, choose the default option or choose an existing method for the WCM to validate itself when logging in.
2. From the Authorization List drop-down list, choose the default option or choose an existing method for the WCM to validate itself when logging in.

Step 12 Click **Finish**.

The Status dialog box is displayed with the registration status of the device with the WCM.

WAAS Express Registration Reference

The following topics describe the WAAS Express Registration pages and dialog boxes used to register the router with the WCM:

- Register with WCM page, page 65-5
- WAAS Express Registration wizard, page 65-7

Register with WCM page

Use this page to enable the WAAS license and launch the wizard to register the router with the WAAS Central Manager (WCM).

How to Get to this page

Click **Configure > Router > WAAS Express > Register with WCM**.

Related Topics

- WAAS Express Registration wizard, page 65-7
- EULA Confirmation dialog box, page 65-6
- Status dialog box, page 65-6

Field Reference

Table 65-1 Register with WCM page

Element	Description
Prerequisites	
Enable Evaluation License button	Click this button to display the EULA confirmation dialog box.
Enable Permanent License button	Click this button to display the Product License Registration page.
If permanent license is enabled, a message is displayed saying it is enabled. If evaluation license is enabled, the Enable Permanent License button is displayed. One of the licenses has to be enabled to register the router with the WCM.	
Register this router with WAAS Central Manager	
Launch Wizard button	Click this button to launch the WAAS Express Registration wizard. Evaluation license or Permanent license has to be enabled for this button to be active.
Status button	Click this button to display the Status dialog box with the registration status of the device with the WCM.

EULA Confirmation dialog box

Use this dialog box to review and accept the terms of the agreement.

How to Get to this page

Click **Configure > Router > WAAS Express > Register with WCM > Enable Evaluation License**.

Related Topics

- Register with WCM page, page 65-5
- Registering WAAS Express, page 65-2

Field Reference

Table 65-2 EULA Confirmation dialog box

Element	Description
Accept check box	Check this check box to accept the terms of the EULA.
OK button	Click the OK button to accept the changes you have made.
Cancel button	Click the Cancel button to cancel the operation.

Status dialog box

Use this dialog box to view the registration status of the device with the WCM.

How to Get to this page

Click **Configure > Router > WAAS Express > Register with WCM > Status**.

or

Click **Configure > Router > WAAS Express > Register with WCM > Launch Wizard > Finish**.

Related Topics

- Register with WCM page, page 65-5
- WAAS Express Registration wizard, page 65-7

Field Reference

Table 65-3 Status dialog box

Element	Description
Registration Status	*Display only.* Displays the registration status of the device with the WCM: Success, Failure, or Status not updated. Status not updated is displayed when there is a delay in receiving the registration status from the WCM. You can view the updated status by clicking the Status button on the Register with WCM page.
Close button	Click this button to close the Status dialog box.

WAAS Express Registration wizard

Use this wizard to register the router with the WCM.

How to Get to this page

Click **Configure > Router > WAAS Express > Register with WCM > Launch Wizard**.

See the following topics:

- WAAS Express Registration wizard—Welcome page, page 65-8
- WAAS Express Registration wizard—WAAS Central Manager page, page 65-8
- WAAS Express Registration wizard—WCM Certificate page, page 65-8
- WAAS Express Registration wizard—Domain Name Configuration page, page 65-9
- WAAS Express Registration wizard—Digital Certificate page, page 65-9

- WAAS Express Registration wizard—WCM Login Credentials page, page 65-10

WAAS Express Registration wizard—Welcome page

Use this page to view the information you need to complete the wizard.

You need the IP address and username of the WCM.

You are also informed that Cisco CP will configure a self-signed certificate if one is not already present, configure HTTPS service, and open HTTP Access List during the registration.

Related Topics

- WAAS Express Registration wizard—WAAS Central Manager page, page 65-8
- WAAS Express Registration wizard, page 65-7

WAAS Express Registration wizard—WAAS Central Manager page

Use this page to enter the IP address of the WCM.

Related Topics

- WAAS Express Registration wizard—WCM Certificate page, page 65-8
- WAAS Express Registration wizard, page 65-7

WAAS Express Registration wizard—WCM Certificate page

Note This page is displayed if Cisco CP is unable to obtain the certificate from WCM.

Use this page to view the steps to get the WCM certificate:

Step 1 Log in to WCM device using telnet.

Step 2 Run the **show crypto certificate-detail admin** command.

Step 3 Copy the contents between ---BEGIN CERTIFICATE--- and ---END CERTIFICATE--- from the command output and paste it in the text box.

Related Topics

- WAAS Express Registration wizard—Domain Name Configuration page, page 65-9
- WAAS Express Registration wizard, page 65-7

WAAS Express Registration wizard—Domain Name Configuration page

Note This page is displayed if the domain name is not configured on the router.

Use this page to enter the domain name.

Related Topics

- WAAS Express Registration wizard—Digital Certificate page, page 65-9
- WAAS Express Registration wizard, page 65-7

WAAS Express Registration wizard—Digital Certificate page

Use this page to create a new self-signed certificate, or choose an existing self-signed certificate to enable secure HTTP service for the WCM to communicate with the router.

Related Topics

- WAAS Express Registration wizard—WCM Login Credentials page, page 65-10
- WAAS Express Registration wizard, page 65-7

Field Reference

Table 65-4 Digital Certificate page

Element	Description
Digital Certificate drop-down list	Choose an existing certificate or choose Create New to create a new certificate.
Name field	Enter a name for the self-signed certificate. This field is displayed only if you chose Create New from the Digital Certificate drop-down list.
Key Size field	Enter the size of the RSA key pair used in the certificate. The range is between 512 and 2048. This field is displayed only if you chose Create New from the Digital Certificate drop-down list.

WAAS Express Registration wizard—WCM Login Credentials page

Use this page to configure a local user on the router, or a user on an external AAA server, for the WCM to log in to the router. WCM logs in to the router to configure and monitor it.

Related Topics

- WAAS Express Registration wizard, page 65-7
- Status dialog box, page 65-6

Field Reference

Table 65-5 WCM Login Credentials page

Element	Description
This Router radio button	Click this radio button to have the WCM log in as a local user using user credentials configured on the router.
An external AAA server radio button	Click this radio button to have the WCM log in using the user credentials configured on an external AAA server.

Table 65-5 WCM Login Credentials page (continued)

Element	Description
Following users are configured on the router field	*Display only.* Displays the names of existing users. This field is displayed if you clicked the This Router radio button.
To create new user enter credentials below check box	Check this check box to create a new user. This check box is displayed if you clicked the This Router radio button.
Username field	Enter the username. This field is displayed if you clicked the This Router radio button.
Password field	Enter the password. This field is displayed if you clicked the This Router radio button.
Confirm Password field	Enter the password again for confirmation. This field is displayed if you clicked the This Router radio button.
Authentication List drop-down list	Choose the default option or choose an existing method for the WCM to validate itself when logging in. This drop-down list is displayed if you clicked the An external AAA server radio button.
Authorization List drop-down list	Choose the default option or choose an existing method for the WCM to validate itself when logging in. This drop-down list is displayed if you clicked the An external AAA server radio button.

CHAPTER 66

Application Extension Platform

For information about how to use Cisco Configuration Professional (Cisco CP) to configure the Application Extension Platform (AXP) feature, see the screencast at:
http://www.cisco.com/en/US/docs/net_mgmt/cisco_configuration_professional/scrcst/ccpsc.html.

Note You must have internet access to view the screencast.

CHAPTER 67

Network Module Management

If the router has network modules that are managed by other applications, such as an IPS sensor, Cisco Configuration Professional (Cisco CP) provides a means for you to launch those applications.

This chapter contains the following sections:

- AIM Module Management
- Switch Module Interface Selection
- Managing the IPS Sensor

AIM Module Management

If a Cisco AIM Module is installed on the router, this window displays basic status information for it. If the AIM Module has been configured, you will also be able to start the Intrusion Detection Device Manager (IDM) software on the module, and select the router interfaces that you want the module to monitor from this window.

If Cisco CP detects that the AIM module has not been configured, it prompts you to open a session to the module so that you can configure it. You can use Telnet or SSH for this session.

AIM Network Module Control Buttons

Cisco CP enables you to issue a number of basic commands to the AIM Network Module from this window.

Reload

Click to reload the AIM network module operating system.

Reset

Click to perform a reset of the AIM network module hardware You should only use the Reset button to recover from Failed state, or after you have shutdown the IDS Network Module.

Shutdown

Click to shutdown the AIM Network Module. You should always perform a shutdown before you to remove the module from the router.

Launch IDM

Click to start the software on the AIM module. When you launch the IDM software, Cisco CP displays a dialog box that asks you for the IP address of the IDS module's external Fast Ethernet interface. When Cisco CP obtains the correct address, it opens an IDM window. For more information on this dialog box, refer to IP Address Determination.

For more information on how to run the IDM application, refer to the documents at the following link:

http://www.cisco.com/univercd/cc/td/doc/product/iaabu/csids/csids10/index.htm

Refresh

Click to refresh the status display.

IDS Network Module Status

This area shows the general status of the AIM Network Module. It contains the following types of information.

- Service Module–The name of the network module.
- State–The state of the network module. Possible states are: Steady state, Shutdown, and/or Failed.
- Software Version–The version of software running on the module.
- Model–The model number of the network module.
- Memory–The amount of memory available on the network module.

IDS NM Monitoring Interface Settings

This area of the window shows which router interfaces have traffic sent to the IDS network module for monitoring.

	A check mark icon next to the interface name indicates that the IDS network module is monitoring the traffic on that interface.
	A red icon with an X next to the interface name indicates that the IDS network module is not monitoring the traffic on that interface.

Configure

Click to add or remove interfaces from this list. When you click **Configure**, Cisco CP verifies that the AIM Network Module has been configured, and that the router has all the configuration settings necessary to communicate with the IDS Network Module. If any configurations are not in place, Cisco CP displays a checklist showing you what has been configured and what has not been configured. You can click on the items that have not been configured to complete the configuration, and then have Cisco CP reverify that these items have been configured so that you can then add or remove interfaces from the AIM Network Module Interface Settings list.

AIM Sensor Interface IP Address

Cisco CP must communicate with the AIM using the IP address of the module's internal Fast Ethernet interface. This window appears when Cisco CP cannot detect this IP address, and enables you to supply one without leaving Cisco CP to do so. If the IDS network module has been configured with a static IP address, or configured as IP unnumbered to another interface with an IP address, this window will not appear.

Entering an IP address in this window may create a new loopback interface. Loopback interfaces can be displayed in the Interfaces and Connections window. The IP address you enter will only be seen by the router. Therefore, it can be any address you want to use.

IP Address

Enter an IP address to use for the sensor interface. Cisco CP will do the following:

- Create a loopback interface. The number 255 is used if available, if not, another number will be used. This loopback interface will be listed in the Interfaces and Connections window.
- Configure the loopback interface with the IP address you enter.
- Configure the IDS network module IP unnumbered to the loopback interface.
- If the IDS network module has already been configured IP unnumbered to an existing loopback interface, but the interface does not have a valid IP address, the loopback interface is given the IP address you enter in this window.

IP Address Determination

Cisco CP displays this window when it needs to determine the IP address of an AIM that you are attempting to manage. This is typically the IP address of the interface. Cisco CP can use the address it used the last time the management application was run, it can attempt to discover the IP address, or it can accept an address that you provide in this window.

Select a method, and click **OK**. If the method you choose fails, you can select another method.

Use Cisco CP last known IP Address

Click to have Cisco CP use the IP address that it used the last time that the management application was run. If the IP address has not been changed since the management application was last run, and you do not want Cisco CP to attempt discovery of the address, use this option.

Let Cisco CP discover IP address

Click to have Cisco CP attempt to discover the IP address. You can use this option if you do not know the IP address, and you are not sure that the last address Cisco CP used to contact the AIM is still correct.

Specify

If you know the network module's IP address, choose this option, and enter the address. Cisco CP will remember the address, and you can select **Use Cisco CP last known IP Address** the next time you start the network module.

Configuration Checklist

This window is displayed when you have clicked **Configure** to specify the router interfaces whose traffic is to be analyzed, but the router lacks a configuration setting required for the two devices to communicate. It shows which configuration settings are needed, and in some cases, allows you to complete the configuration from within Cisco CP.

- A check mark icon in the Action column means the configuration setting has been made.
- An X icon in the Action column means that the configuration setting must be made in order for the router to be able to communicate with the network module.

Sensor Interface

- If this row contains an X icon in the Action column, the sensor interface has not been configured with an IP address. Double-click the row and enter an IP address for the sensor in the dialog displayed. The sensor IP address is the address that Cisco CP and the router use when communicating with the network module. This IP address can be a private address; no hosts other than the router it is installed in will be able to reach the address.

Date & Time

- If this row contains an X icon in the Action column, the router's clock settings have not been configured. Double-click on this row, and enter time and date settings in the Date and Time Properties window.

IP CEF Setting

If this row contains an X icon in the Action column, Cisco Express Forwarding (CEF) has not been enabled on the router. Double-click on this row, and click **Yes** to enable IP CEF on the router.

NM Initial Setup

If this row contains an X icon in the Action column, Cisco CP has detected that the network module's default IP address has not been changed. Double-click on this row, and Cisco CP will prompt you to open a session to the module and complete configuration.You can use Telnet or SSH for this session.

For more information on configuring the network module, refer to the documents at the following link.

http://www.cisco.com/univercd/cc/td/doc/product/iaabu/csids/csids10/index.htm

Refresh

After you have fixed configuration settings, you can click this button to refresh the checklist. If an X icon remains in the Action column, a configuration setting has still not been made.

Interface Monitoring Configuration

In this screen, specify which interfaces are to be monitored by the IPS sensor. Additionally, display a dialog that enables you to choose or create an ACL that specifies the traffic that is to be monitored.

How to get to this screen

In the navigation pane, click **Configure > Security > Advanced Security > Intrusion Prevention > IPS Sensor > Configure**.

Related Links

- IPS Sensor Configuration Checklist
- Monitoring Settings

Field Reference

Table 67-1 Interface Monitoring Configuration

Element	Description
Monitoring Mode	Choose one of the following: • Promiscuous—To create a separate stream of traffic that will be directed to the IPS sensor for inspection, choose **Promiscuous**. • Inline—To direct all specified traffic to the IPS sensor before it is sent to the router, choose **Inline**.
Interface and Traffic columns	These columns display the configured interfaces and the number of any ACL that is associated with the interface. To specify that the traffic on an interface is to be inspected, check the box next to the interface name.
Traffic	To display a dialog that enables you to choose or create an ACL that specifies which traffic is to be inspected on the interface, or to clear the association between an interface and an ACL, choose the interface, and click **Traffic**.

Network Module Login

Enter the username and password required to login to the network module. These credentials may not be the same credentials required to log in to the router.

Switch Module Interface Selection

This window is displayed when there is more than one switch module installed on the router, and allows you to select the one that you want to manage. Click the radio button next to the switch module that you want to manage, and then click **OK**.

Managing the IPS Sensor

If there is an AIM-IPS-K9, or NME-IPS-K9IPS sensor on the router, you can configure it from the IPS Sensor tab.

To configure the IPS sensor, complete the following steps:

Step 1 From the navigation panel, click **Configure > Security > Intrusion Prevention**.

Step 2 In the Intrusion Prevention System window, click **IPS Sensor**.

Step 3 In the IPS Sensor screen, manage and configure the IPS sensor. You can reload, reset, and shut down the IPS sensor,. You can also make failover settings, launch the IDM application, and configure interface settings. For more information, see Sensor Failover Settings.

IPS Sensor Reference

This section contains the following help topics:

- IPS Sensor
- Sensor Failover Settings
- IPS Sensor Configuration Checklist
- Interface Monitoring Configuration
- Monitoring Settings

IPS Sensor

In this screen, manage the IPS sensor, make failover settings, and configure ACLs for the monitored interfaces.

How to get to this screen

In the navigation pane, click **Configure > Security > Advanced Security > Intrusion Prevention > IPS Sensor**.

Related Links

- Sensor Failover Settings
- Interface Monitoring Configuration
- Monitoring Settings

Field Reference

Table 67-2 IPS Sensor

Element	Description
IPS Sensor Management	
Reload	To reload the software on the IPS sensor, click **Reload**.
Reset	To reset the IPS sensor and clear accumulated statistics, click **Reset**.
Shutdown	To shut down the IPS sensor, click **Shutdown**.
Launch IDM	To start the software used to configure the IPS sensor, click **Launch IDM**.
Failover Settings	To specify what the router is to do when the IPS sensor is not operating, click **Failover Settings**, and make settings in the displayed dialog.
Refresh	To refresh the information displayed in this screen, click **Refresh**.
Module Status Area—Depending on the type of module, the name of Module Status area changes.	
Contents	For AIM-IPS and NME-IPS modules, this area is called IPS Sensor Status—Displays basic information for the router IPS sensor and its possible values. For NM-CIDS modules, this area is called IDS Network Module Status—Displays basic information for the router IPS sensor and its possible values.
Interface Settings Area—Depending on the type of module, the name of the Interface Settings area changes.	

Table 67-2 IPS Sensor (continued)

Element	Description
Configure button	To have the IPS sensor monitor traffic on a router interface, and to specify the traffic that the sensor is to monitor, click **Configure**, and make specifications in the displayed dialog.
	For AIM-IPS and NME-IPS modules, the Interface Settings area is called Interface Settings for IPS Monitoring—Displays the configured router interfaces, indicates if traffic on the interface is being monitored, the monitor mode, and the traffic that is being monitored on the interface. For NM-CIDS modules, the Interface Settings area is called IDS NM Monitoring Interface Status—Displays the configured router interfaces and indicates if traffic on the interface is being monitored.

Sensor Failover Settings

In this screen, specify how the router is to handle traffic if the IPS sensor goes down, and whether the router is to automatically reboot the sensor when it goes down.

How to get to this screen

In the navigation pane, click **Configure > Security > Advanced Security > Intrusion Prevention > IPS Sensor > Failover Settings**.

Related Links

- IPS Sensor

Field Reference

Table 67-3 Sensor Failover Settings

Element	Description
Traffic Handling on Failure	
Drop All Traffic	To cause the router to drop all traffic when the IPS sensor fails, check **Drop All Traffic**.

Table 67-3 Sensor Failover Settings (continued)

Element	Description
Pass Traffic Through Without Inspection	To cause the router to allow all traffic when the IPS sensor fails, check **Pass Traffic Through Without Inspection**.
Sensor Reboot Settings	
Enable Automatic Reboot	To cause the router to automatically reboot the sensor when it goes down, click **Enable Automatic Reboot**.

IPS Sensor Configuration Checklist

This screen displays the IPS sensor configuration items that are being checked prior to display of the router interfaces. This screen automatically closes when the configuration checklist is complete, and the Interface Monitoring Configuration screen is displayed.

How to get to this screen

In the navigation pane, click **Configure > Security > Advanced Security > Intrusion Prevention > IPS Sensor > Configure**.

Related Links

- IPS Sensor
- Interface Monitoring Configuration

Field Reference

Table 67-4 IPS Sensor Configuration Checklist

Element	Description
Sensor Interface	The sensor interface to the router is being checked.
Date and Time	The date and time settings on the sensor are being checked.
IP CEF Settings	The IP Cisco Express Forwarding settings are being checked.
Sensor Initial Setup	The initial sensor setup is being checked.

Interface Monitoring Configuration

In this screen, specify which interfaces are to be monitored by the IPS sensor. Additionally, display a dialog that enables you to choose or create an ACL that specifies the traffic that is to be monitored.

How to get to this screen

In the navigation pane, click **Configure > Security > Advanced Security > Intrusion Prevention > IPS Sensor > Configure**.

Related Links

- IPS Sensor Configuration Checklist
- Monitoring Settings

Field Reference

Table 67-5 Interface Monitoring Configuration

Element	Description
Monitoring Mode	Choose one of the following: • Promiscuous—To create a separate stream of traffic that will be directed to the IPS sensor for inspection, choose **Promiscuous**. • Inline—To direct all specified traffic to the IPS sensor before it is sent to the router, choose **Inline**.
Interface and Traffic columns	These columns display the configured interfaces and the number of any ACL that is associated with the interface. To specify that the traffic on an interface is to be inspected, check the box next to the interface name.
Traffic	To display a dialog that enables you to choose or create an ACL that specifies which traffic is to be inspected on the interface, or to clear the association between an interface and an ACL, choose the interface, and click **Traffic**.

Monitoring Settings

In this screen, associate or dissociate an ACL from and interface.

How to get to this screen

In the navigation pane, click **Configure > Security > Advanced Security > Intrusion Prevention > IPS Sensor > Configure > Edit**.

Related Links

- Interface Monitoring Configuration

Field Reference

Table 67-6 Monitoring Settings

Element	Description
Traffic	In this field, enter the name or number of an ACL that defines the traffic that is to be inspected. If you cannot remember the name or number, or if there are no ACLs configured, you c an click the button to the right of the field to display a dialog that enables you to choose or configure an ACL.
Button	Clicking this button displays the following options: • Select an existing rule (ACL)—Display a dialog that lists the ACLs that you can choose to associate with the interface. • Create a new rule (ACL) and select—Display a dialog that enables you to create an ACL and associate it with the interface. • None. Clear rule association—Dissociate the current ACL from the interface.

CHAPTER 68

Video Surveillance

This chapter describes how to use Cisco CP to initialize a Video Management module, Video Gateway module, and Integrated Storage System (ISS) module installed on the router.

The following sections provide more information:

- Video Management Initialization Wizard Screen Reference, page 68-1
- Video Gateway Initialization Wizard Screen Reference, page 68-7
- Integrated Storage System Initialization Wizard Screen Reference, page 68-12

Video Management Initialization Wizard Screen Reference

This section describes the pages and dialog boxes you can use when working with video modules and includes the following topics:

- Initialization Page, page 68-2
- Module Initialization Wizard—Service Engine Configuration, page 68-2
- Module Initialization Wizard—Module Configuration Page, page 68-3
- Module Initialization Wizard—Confirmation Page, page 68-5
- Module Initialization Wizard—Module Initialization Page, page 68-5
- Module Initialization Wizard—Complete Page, page 68-6

Initialization Page

Use this page to launch the Module Initialization wizard.

How to get to this screen

Click **Configure > Applications > Video Surveillance > Video Management**.

Related Links

- Video Management Initialization Wizard Screen Reference, page 68-1
- Module Initialization Wizard—Service Engine Configuration, page 68-2

Field Reference

Table 68-1 Initialization

Element	Description
Launch Wizard	Click the **Launch Wizard** button to launch the wizard.

Module Initialization Wizard—Service Engine Configuration

Use this screen to configure the service engine IP addresses.

How to get to this screen

Click **Configure > Applications > Video Surveillance > Video Management > Initialization.**

Related Links

- Video Management Initialization Wizard Screen Reference, page 68-1
- Initialization Page, page 68-2
- Module Initialization Wizard—Module Configuration Page, page 68-3

Field Reference

Table 68-2 Service Engine Configuration

Element	Description
Service Engine IP address	This field appears if the Cisco IOS CLI has been used to configure the service engine with a private IP address. The IP address is displayed in this field. This field is read only.
Service Engine IP unnumbered interface	(Mandatory). If the service engine has not been configured with a private IP address, this field appears, and lists all available interfaces, including interfaces which are administratively shut down. You must choose an interface for the service engine from this list. If you choose an interface that is administratively shut down, an alert message is displayed asking you to select a different interface.
Module IP address	(Mandatory). In this field, configure the module's IP address. You must use an IP address that is in the same subnet as the IP address of the service engine. This is the case whether the service engine has a private IP address, or an unnumbered IP address.
Module Default Gateway	This field displays the IP address of the service engine, whether it is a private IP address or an unnumbered IP address. This field is read only.

Module Initialization Wizard—Module Configuration Page

Use this page to enter the parameters to use when initializing the video module.

How to get to this screen

Click **Configure > Applications > Video Surveillance > Video Management > Initialization**.

Related Links

- Video Management Initialization Wizard Screen Reference, page 68-1
- Module Initialization Wizard—Service Engine Configuration, page 68-2
- Module Initialization Wizard—Confirmation Page, page 68-5

Field Reference

Table 68-3 Module Configuration

Element	Description
Hostname	Enter the hostname for the video module. You can enter a maximum of 51 characters. If you do not enter a hostname, the IP address entered in the Service Engine Configuration screen is used, and given the following format where periods are replaced by dashes, and the letters are prepended to the address. For example, an address of 10.1.10.1 would be formatted as follows: `se-10-1-10-1`
Domain Name	Enter the domain name for the video module.
Primary DNS Server	Enter the IP address of the DNS server that the video module will use.
Primary NTP Server	(Mandatory if enabled). This field is enabled if the NTP status on the router is synchronized. The default value is the IP address of the router. If the NTP status is not synchronized, this field is disabled, and the System Date and Time field is enabled.
Secondary NTP Server	Enter the IP address of the secondary NTP server. This field is enabled if the NTP status on the router is synchronized. Otherwise, the field is disabled.
System Date and Time	(Mandatory if enabled). This field is enabled if the Primary NTP Server field is disabled. Synchronize with PC clock is checked by default; but, you can uncheck it to enable the time field and enter the time manually. To choose the date, click the calendar icon and navigate to the correct date.
Continent	(Mandatory). Choose the continent on which the device is located.
Country	(Mandatory). Choose a country within the chosen continent. If no countries are available for the continent chosen, this field is disabled; but, you can choose a time zone from the Time Zone field.
Time Zone	(Mandatory). Choose the time zone in which the device is located. If the country or continent chosen does not use time zones, then this field is disabled.

Module Initialization Wizard—Confirmation Page

Use this page to inform yourself of the time that initialization can take and to understand that once begun, the initialization process cannot be stopped.

How to get to this screen

Click **Configure > Applications > Video Surveillance > Video Management > Initialization**.

Related Links

- Video Management Initialization Wizard Screen Reference, page 68-1
- Module Initialization Wizard—Module Configuration Page, page 68-3
- Module Initialization Wizard—Module Initialization Page, page 68-5

To start initialization

To start initialization, click **Next**.

To return to configuration screens to review or make changes

To return to the previous page to change the settings, click **Back**.

Module Initialization Wizard—Module Initialization Page

Use this page to view the progress of the initialization operation.

How to get to this screen

Click **Configure > Applications > Video Surveillance > Video Management > Initialization**.

Related Links

- Video Management Initialization Wizard Screen Reference, page 68-1
- Module Initialization Wizard—Confirmation Page, page 68-5
- Module Initialization Wizard—Complete Page, page 68-6

Module Initialization Wizard—Complete Page

Use this page to see the summary of the results of the operation and close the wizard by clicking **Finish**.

How to get to this screen

Click **Configure > Applications > Video Surveillance > Video Management > Initialization**.

Related Links

- Video Management Initialization Wizard Screen Reference, page 68-1
- Module Initialization Wizard—Module Initialization Page, page 68-5

Video Gateway Initialization Wizard Screen Reference

This section describes the pages and dialog boxes you can use when working with video modules and includes the following topics:

- Initialization Page, page 68-7
- Module Initialization Wizard—Service Engine Configuration, page 68-8
- Module Initialization Wizard—Module Configuration Page, page 68-9
- Module Initialization Wizard—Confirmation Page, page 68-11
- Module Initialization Wizard—Module Initialization Page, page 68-11
- Module Initialization Wizard—Complete Page, page 68-12

Initialization Page

Use this page to launch the Module Initialization wizard.

How to get to this screen

Click **Configure > Applications > Video Surveillance > Video Gateway**.

Related Links

- Video Gateway Initialization Wizard Screen Reference, page 68-7
- Module Initialization Wizard—Service Engine Configuration, page 68-8

Field Reference

Table 68-4 Initialization

Element	Description
Module Location	Choose the module location from the drop-down list.
Launch Wizard	Click the **Launch Wizard** button to launch the wizard.

Module Initialization Wizard—Service Engine Configuration

Use this screen to configure the service engine IP addresses.

How to get to this screen

Click **Configure > Applications > Video Surveillance > Video Gateway > Initialization.**

Related Links

- Video Gateway Initialization Wizard Screen Reference, page 68-7
- Initialization Page, page 68-7
- Module Initialization Wizard—Module Configuration Page, page 68-9

Field Reference

Table 68-5 Service Engine Configuration

Element	Description
Service Engine IP address	This field appears if the Cisco IOS CLI has been used to configure the service engine with a private IP address. The IP address is displayed in this field. This field is read only.
Service Engine IP unnumbered interface	(Mandatory). If the service engine has not been configured with a private IP address, this field appears, and lists all available interfaces, including interfaces which are administratively shut down. You must choose an interface for the service engine from this list. If you choose an interface that is administratively shut down, an alert message is displayed asking you to select a different interface.
Module IP address	(Mandatory). In this field, configure the module's IP address. You must use an IP address that is in the same subnet as the IP address of the service engine. This is the case whether the service engine has a private IP address, or an unnumbered IP address.
Module Default Gateway	This field displays the IP address of the service engine, whether it is a private IP address or an unnumbered IP address. This field is read only.

Module Initialization Wizard—Module Configuration Page

Use this page to enter the parameters to use when initializing the video module.

How to get to this screen

Click **Configure > Applications > Video Surveillance > Video Gateway > Initialization**.

Related Links

- Video Gateway Initialization Wizard Screen Reference, page 68-7
- Module Initialization Wizard—Service Engine Configuration, page 68-8
- Module Initialization Wizard—Confirmation Page, page 68-11

Field Reference

Table 68-6 Module Configuration

Element	Description
Module Location	The module location you chose in the Initialization page is displayed.
Hostname	Enter the hostname for the video module. You can enter a maximum of 51 characters. If you do not enter a hostname, the IP address entered in the Service Engine Configuration screen is used, and given the following format where periods are replaced by dashes, and the letters are prepended to the address. For example, an address of 10.1.10.1 would be formatted as follows: `se-10-1-10-1`
Domain Name	Enter the domain name for the video module.
Primary DNS Server	Enter the IP address of the DNS server that the video module will use.
Primary NTP Server	(Mandatory if enabled). This field is enabled if the NTP status on the router is synchronized. The default value is the IP address of the router. If the NTP status is not synchronized, this field is disabled, and the System Date and Time field is enabled.

Table 68-6 Module Configuration (continued)

Element	Description
Secondary NTP Server	Enter the IP address of the secondary NTP server. This field is enabled if the NTP status on the router is synchronized. Otherwise, the field is disabled.
System Date and Time	(Mandatory if enabled). This field is enabled if the Primary NTP Server field is disabled. Synchronize with PC clock is checked by default; but, you can uncheck it to enable the time field and enter the time manually. To choose the date, click the calendar icon and navigate to the correct date.
Continent	(Mandatory). Choose the continent on which the device is located.
Country	(Mandatory). Choose a country within the chosen continent. If no countries are available for the continent chosen, this field is disabled; but, you can choose a time zone from the Time Zone field.
Time Zone	(Mandatory). Choose the time zone in which the device is located. If the country or continent chosen does not use time zones, then this field is disabled.
Administrative Username	(Mandatory). Enter a username for the administrator of the module. The default value of this field is the username of the router.
Administrative Password	(Mandatory). Enter a password for the administrator of the module. The default value of this field is the password of the router.

Module Initialization Wizard—Confirmation Page

Use this page to inform yourself of the time that initialization can take and to understand that once begun, the initialization process cannot be stopped.

How to get to this screen

Click **Configure > Applications > Video Surveillance > Video Gateway > Initialization**.

Related Links

- Video Gateway Initialization Wizard Screen Reference, page 68-7
- Module Initialization Wizard—Module Configuration Page, page 68-9
- Module Initialization Wizard—Module Initialization Page, page 68-11

To start initialization

To start initialization, click **Next**.

To return to configuration screens to review or make changes

To return to the previous page to change the settings, click **Back**.

Module Initialization Wizard—Module Initialization Page

Use this page to view the progress of the initialization operation.

How to get to this screen

Click **Configure > Applications > Video Surveillance > Video Gateway > Initialization**.

Related Links

- Video Gateway Initialization Wizard Screen Reference, page 68-7
- Module Initialization Wizard—Confirmation Page, page 68-11
- Module Initialization Wizard—Complete Page, page 68-12

Module Initialization Wizard—Complete Page

Use this page to see the summary of the results of the operation and close the wizard by clicking **Finish**.

How to get to this screen

Click **Configure > Applications > Video Surveillance > Video Gateway > Initialization**.

Related Links

- Video Gateway Initialization Wizard Screen Reference, page 68-7
- Module Initialization Wizard—Module Initialization Page, page 68-11

Integrated Storage System Initialization Wizard Screen Reference

This section describes the pages and dialog boxes you can use when working with video modules and includes the following topics:

- Initialization Page, page 68-13
- Module Initialization Wizard—Service Engine Configuration, page 68-13
- Module Initialization Wizard—Module Configuration Page, page 68-14
- Module Initialization Wizard—Confirmation Page, page 68-16
- Module Initialization Wizard—Module Initialization Page, page 68-16
- Module Initialization Wizard—Complete Page, page 68-17

Initialization Page

Use this page to launch the Module Initialization wizard.

How to get to this screen

Click **Configure > Applications > Video Surveillance > Integrated Storage System**.

Related Links

- Integrated Storage System Initialization Wizard Screen Reference, page 68-12
- Module Initialization Wizard—Service Engine Configuration, page 68-13

Field Reference

Table 68-7 Initialization

Element	Description
Module Location	Choose the module location from the drop-down list.
Launch Wizard	Click the **Launch Wizard** button to launch the wizard.

Module Initialization Wizard—Service Engine Configuration

Use this screen to configure the service engine IP addresses.

How to get to this screen

Click **Configure > Applications > Video Surveillance > Integrated Storage System > Initialization.**

Related Links

- Integrated Storage System Initialization Wizard Screen Reference, page 68-12
- Initialization Page, page 68-13
- Module Initialization Wizard—Module Configuration Page, page 68-14

Field Reference

Table 68-8 Service Engine Configuration

Element	Description
Service Engine IP address	This field appears if the Cisco IOS CLI has been used to configure the service engine with a private IP address. The IP address is displayed in this field. This field is read only.
Service Engine IP unnumbered interface	(Mandatory). If the service engine has not been configured with a private IP address, this field appears, and lists all available interfaces, including interfaces which are administratively shut down. You must choose an interface for the service engine from this list. If you choose an interface that is administratively shut down, an alert message is displayed asking you to select a different interface.
Module IP address	(Mandatory). In this field, configure the module's IP address. You must use an IP address that is in the same subnet as the IP address of the service engine. This is the case whether the service engine has a private IP address, or an unnumbered IP address.
Module Default Gateway	This field displays the IP address of the service engine, whether it is a private IP address or an unnumbered IP address. This field is read only.

Module Initialization Wizard—Module Configuration Page

Use this page to enter the parameters to use when initializing the video module.

How to get to this screen

Click **Configure > Applications > Video Surveillance > Integrated Storage System > Initialization**.

Related Links

- Integrated Storage System Initialization Wizard Screen Reference, page 68-12
- Module Initialization Wizard—Service Engine Configuration, page 68-13
- Module Initialization Wizard—Confirmation Page, page 68-16

Field Reference

Table 68-9 Module Configuration

Element	Description
Module Location	The module location you chose in the Initialization page is displayed.
Hostname	Enter the hostname for the video module. You can enter a maximum of 51 characters. If you do not enter a hostname, the IP address entered in the Service Engine Configuration screen is used, and given the following format where periods are replaced by dashes, and the letters are prepended to the address. For example, an address of 10.1.10.1 would be formatted as follows: `se-10-1-10-1`
Domain Name	Enter the domain name for the video module.
Primary DNS Server	Enter the IP address of the DNS server that the video module will use.
Primary NTP Server	(Mandatory if enabled). This field is enabled if the NTP status on the router is synchronized. The default value is the IP address of the router. If the NTP status is not synchronized, this field is disabled, and the System Date and Time field is enabled.
Secondary NTP Server	Enter the IP address of the secondary NTP server. This field is enabled if the NTP status on the router is synchronized. Otherwise, the field is disabled.
System Date and Time	(Mandatory if enabled). This field is enabled if the Primary NTP Server field is disabled. Synchronize with PC clock is checked by default; but, you can uncheck it to enable the time field and enter the time manually. To choose the date, click the calendar icon and navigate to the correct date.
Continent	(Mandatory). Choose the continent on which the device is located.
Country	(Mandatory). Choose a country within the chosen continent. If no countries are available for the continent chosen, this field is disabled; but, you can choose a time zone from the Time Zone field.

Table 68-9 Module Configuration (continued)

Element	Description
Time Zone	(Mandatory). Choose the time zone in which the device is located. If the country or continent chosen does not use time zones, then this field is disabled.

Module Initialization Wizard—Confirmation Page

Use this page to inform yourself of the time that initialization can take and to understand that once begun, the initialization process cannot be stopped.

How to get to this screen

Click **Configure > Applications > Video Surveillance > Integrated Storage System > Initialization**.

Related Links

- Integrated Storage System Initialization Wizard Screen Reference, page 68-12
- Module Initialization Wizard—Module Configuration Page, page 68-14
- Module Initialization Wizard—Module Initialization Page, page 68-16

To start initialization

To start initialization, click **Next**.

To return to configuration screens to review or make changes

To return to the previous page to change the settings, click **Back**.

Module Initialization Wizard—Module Initialization Page

Use this page to view the progress of the initialization operation.

How to get to this screen

Click **Configure > Applications > Video Surveillance > Integrated Storage System > Initialization**.

Related Links

- Integrated Storage System Initialization Wizard Screen Reference, page 68-12
- Module Initialization Wizard—Confirmation Page, page 68-16
- Module Initialization Wizard—Complete Page, page 68-17

Module Initialization Wizard—Complete Page

Use this page to see the summary of the results of the operation and close the wizard by clicking **Finish**.

How to get to this screen

Click **Configure > Applications > Video Surveillance > Integrated Storage System > Initialization**.

Related Links

- Integrated Storage System Initialization Wizard Screen Reference, page 68-12
- Module Initialization Wizard—Module Initialization Page, page 68-16

PART 8

Managing Licenses

This section provides information about how to manage licenses.

CHAPTER 69

License Management

License Dashboard Screencast

For information about how to use Cisco Configuration Professional (Cisco CP) to configure licenses, see the screencast at: http://www.cisco.com/en/US/docs/net_mgmt/cisco_configuration_professional/scrcst/ccpsc.html.

Note You must have internet access to view the screencast.

PART 8

Monitoring the Router

This section provides information about how to monitor the router.

CHAPTER 70

Viewing Router Information

The Cisco Configuration Professional (Cisco CP) Monitor mode lets you view a current snapshot of information about your router, the router interfaces, the firewall, and any active VPN connections. You can also view any messages in the router event log.

Note The Monitor window is not dynamically updated with the latest information. To view any information that has changed since you brought up this window, you must click **Update**.

Monitor mode works by examining the router log and by viewing the results of Cisco IOS **show** commands. For Monitor mode functions that are based on log entries, such as firewall statistics, logging must be enabled. Logging is enabled by default by Cisco CP, but you can change that setting using the **Router > Logging** window. In addition, individual rules may need configuration so that they generate log events. For more information, see the help topic How Do I View Activity on My Firewall?

If you want to:	Do this:
View graphs of CPU or memory usage.	From the toolbar, click **Monitor > Router > Overview**. The Overview page includes graphs of CPU usage and memory usage.
View information about router interfaces.	From the toolbar, click **Monitor**, and then in the left frame, click **Router > Interface Status**. From the Select Interface field select the interface for which you want to view information, then in the Available Items group, select the information you want to view. Then click **Show Details**.
View messages in the router event log.	From the toolbar, click **Monitor**, and then in the left frame, click **Router > Logging**.
View information about the firewall.	From the toolbar, click **Monitor**, and then in the left frame, click **Security > Firewall Status**.
View information about VPN Connections	From the toolbar, click **Monitor**, and then in the left frame, click **Security > VPN Status**. Then select the tab for IPSec Tunnels, DMVPN Tunnels, Easy VPN Servers, or IKE SAs.

Overview

The Monitor mode Overview screen displays an overview of your router activity and statistics, and serves as a summary of the information contained on the other Monitor mode screens. It contains the information described in this help topic.

Note If you do not see feature information described in this help topic on the Overview screen, the Cisco IOS image does not support the feature. For example, if the router is running a Cisco IOS image that does not support security features, the Firewall Status, and VPN status sections do not appear on the screen.

Launch Wireless Application Button

If the router has radio interfaces, you can click this button to monitor and configure radio interfaces. The Monitor Overview window provides interface status information for these interfaces, but radio interfaces are not listed in the Monitor Interface Status window.

This button does not appear if the router does not have radio interfaces.

Update Button

Retrieves current information from the router, updating statistics displayed by this screen.

Resource Status

Shows basic information about your router hardware and contains the following fields:

CPU Usage

Shows the percentage of CPU usage.

Memory Usage

Shows the percent of RAM usage.

Flash Usage

Shows the available flash over the amount of flash installed on the router.

Interface Status

Shows basic information about the interfaces installed on the router and their status.

Note Only interface types supported by Cisco CP are included in these statistics. Unsupported interfaces will not be counted.

Total Interface(s) Up

The total number of enabled (up) interfaces on the router.

Total Interface(s) Down

The total number of disabled (down) interfaces on the router.

Interface

The interface name.

IP

The IP address of the interface.

Status

The status of the interface, either Up, or Down.

Bandwidth Usage

The percent of interface bandwidth being used.

Description

Available description for the interface. Cisco CP may add descriptions such as $FW_OUTSIDE$ or ETH_LAN.

Firewall Status Group

Shows basic information about the router resources and contains the following fields:

Number of Attempts Denied

Shows the number of log messages generated by connection attempts (by protocols such as Telnet, HTTP, ping, and others) rejected by the firewall. Note that in order for a log entry to be generated by a rejected connection attempt, the access rule that rejected the connection attempt must be configured to create log entries.

Firewall Log

If enabled, shows the number of firewall log entries.

QoS

The number of interfaces with an associated QoS policy.

VPN Status Group

Shows basic information about the router resources and contains the following fields:

Number of Open IKE SAs

Shows the number of IKE Security Associations (SAs) connections currently configured and running.

Number of Open IPSec Tunnels

Shows the number of IPSec Virtual Private Network (VPN) connections currently configured and running.

No. of DMVPN Clients

If the router is configured as a DMVPN hub, the number of DMVPN clients.

No. of Active VPN Clients

If the router is configured as an EasyVPN Server, this field shows the number of Easy VPN Remote clients.

NAC Status Group

Shows a basic snapshot of Network Admission Control (NAC) status on the router.

No. of NAC enabled interfaces field

The number of router interfaces on which NAC is enabled.

No. of validated hosts field

The number of hosts with posture agents that have been validated by the admissions control process.

Log Group

Shows basic information about the router resources and contains the following fields:

Total Log Entries

The total number of entries currently stored in the router log.

High Severity

The number of log entries stored that have a severity level of 2 or lower. These messages require immediate attention. Note that this list will be empty if you have no high severity messages.

Warning

The number of log entries stored that have a severity level of 3 or 4. These messages may indicate a problem with your network, but they do not likely require immediate attention.

Informational

The number of log entries stored that have a severity level of 6 or higher. These information messages signal normal network events.

Interface Status

The Interface Status screen displays the current status of the various interfaces on the router, and the numbers of packets, bytes, or data errors that have travelled through the selected interface. Statistics shown on this screen are cumulative since the last time the router was rebooted, the counters were reset, or the selected interface reset.

Monitor Interface and Stop Monitoring Button

Click this button to start or stop monitoring the selected interface. The button label changes based on whether Cisco CP is monitoring the interface or not.

Test Connection Button

Click to test the selected connection. A dialog appears that enables you to specify a remote host to ping through this connection. The dialog then reports on the success or failure of the test. If the test fails, information about why the test may have failed is given, along with the steps you need to take to correct the problem.

Interface List

Select the interface for which you want to display statistics from this list. The list contains the name, IP address and subnet mask, the slot and port it is located in, and any Cisco CP or user description entered.

Note Ethernet subinterfaces are not listed in the UI. Instead, the corresponding main interface of the configured Ethernet subinterface is listed. Also, the Ethernet subinterface packet count is not shown in **show interface** <sub-interface-name>. It is shown only on the main interface (**show interface** <main interface>).

Select Chart Types to Monitor Group

These check boxes are the data items for which Cisco CP can show statistics on the selected interface. These data items are as follows:

- Packet Input—The number of packets received on the interface.
- Packet Output—The number of packets sent by the interface.
- Bandwidth Usage—The percent of bandwidth used by the interface, shown as a percentage value. Here is how bandwidth percentage is computed:

  Bandwidth percentage=(Kbps/bw) * 100,

  where

  bits per second= ((change in input+change in output) * 8) / poll interval

  Kbps= bits per second/1024

  bw=bandwidth capacity of the interface

  Because the differences in bytes input and bytes output can only be computed after the second view interval, the bandwidth percentage graph shows the correct bandwidth usage starting with the second view interval. See the View Interval section of this topic for polling intervals and view intervals.

- Bytes Input—The number of bytes received on the interface.
- Bytes Output—The number of bytes sent by the interface.
- Errors Input—The number of errors occurring while receiving data on the interface.
- Errors Output—The number of errors occurring while sending data from the interface.
- Packets flow—The number of packets in the flow for the chosen interface. This data item appears only if configured under **Configure > Interfaces and Connections > Edit > Application Service** for the chosen interface.
- Bytes flow—The number of bytes in the flow for the chosen interface. This data item appears only if configured under **Configure > Interfaces and Connections > Edit > Application Service** for the chosen interface.
- Total flow—The total number flows, from sources and destinations, for the chosen interface. This data item appears only if configured under **Configure > Interfaces and Connections > Edit > Application Service** for the chosen interface.

Note If the router Cisco IOS image does not support Netflow, the flow counters will not be available.

To view statistics for any of these items:

Step 1 Select the item(s) you want to view by checking the associated check box(es).

Step 2 Click **Monitor Interface** to see statistics for all selected data items.

Interface Status Area

View Interval

This pull-down field selects both the amount of data shown for each item and the frequency with which the data is updated. It has the following options

Note The polling frequencies listed are approximations and may differ slightly from the listed times.

- Real-time data every 10 sec. This option will continue polling the router for a maximum of two hours, resulting in approximately 120 data points.
- 10 minutes of data polled every 10 sec.
- 60 minutes of data, polled every 1 minute.
- 12 hours of data, polled every 10 minutes.

Note The last three options will retrieve a maximum of 60 data points. After 60 data points have been retrieved, Cisco CP will continue to poll data, replacing the oldest data points with the newest ones.

Show Table/Hide Table

Click this button to show or hide the performance charts.

Reset button

Click this button to reset the interface statistic counts to zero.

Chart Area

This area shows the charts and simple numerical values for the data specified.

Note The last three options will retrieve a maximum of 30 data points. After 30 data points have been retrieved, Cisco CP will continue to poll data, replacing the oldest data points with the newest ones.

Environment

For information about how to use Cisco Configuration Professional (Cisco CP) to monitor the router environment, see the screencast at: http://www.cisco.com/en/US/docs/net_mgmt/cisco_configuration_professional/scrcst/ccpsc.html.

Note You must have internet access to view the screencast.

Logging

Cisco CP offers the following logs:

- Syslog—The router log.
- Firewall Log— If a firewall has been configured on the router, this log records entries generated by that firewall.
- Application Security Log—If an application firewall has been configured on the router, this log records entries generated by that firewall.
- SDEE Message Log—If SDEE has been configured on the router, this log records SDEE messages.

To open a log, click the tab with the log's name.

Syslog

The router contains a log of events categorized by severity level, like a UNIX syslog service.

Note It is the router log that is displayed, even if log messages are being forwarded to a syslog server.

Logging Buffer

Shows whether or not the logging buffer and syslog logging are enabled. The text "Enabled" is displayed when both are enabled. The logging buffer reserves a specified amount of memory to retain log messages. The setting in this field is not preserved if your router is rebooted. The default settings for these fields are for the logging buffer to be enabled with 4096 bytes of memory.

Logging Hosts

Shows the IP address of any syslog hosts where log messages are being forwarded. This field is read-only. To configure the IP addresses of syslog hosts, use the **Monitor > Router > Logging** window.

Logging Level (Buffer)

Shows the logging level configured for the buffer on the router.

Number of Messages in Log

Shows the total number of messages stored in the router log.

Select a Logging Level to View

From this field, select the severity level of the messages that you want to view in the log. Changing the setting in this field causes the list of log messages to be refreshed.

Log

Displays all messages with the severity level specified in the Select a Logging Level to View field. Log events contains the following information:

- Severity Column

  Shows the severity of the logging event. Severity is shown as a number from 1 through 7, with lower numbers indicating more severe events. The descriptions of each of the severity levels are as follows:

  - 0 - emergencies

    System unusable

  - 1- alerts

    Immediate action needed

  - 2 - critical

    Critical conditions

  - 3 - errors

    Error conditions

  - 4 - warnings

    Warning conditions
  - 5 - notifications

    Normal but significant condition
  - 6 - informational

    Informational messages only
  - 7 - debugging

    Debugging messages
- Time Column

  Shows the time that the log event occurred.
- Description Column

  Shows a description of the log event.

Update Button

Updates the window with current information about log details and the most current log entries.

Clear Log Button

Erases all messages from the log buffer on the router.

Search Button

Opens a search window. In the search window, enter text in the Search field and click the **Find** button to display all entries containing the search text. Searches are *not* case sensitive.

Firewall Log

The log entries shown in the top part of this window are determined by log messages generated by the firewall. In order for the firewall to generate log entries, you must configure individual access rules to generate log messages when they are invoked. For instructions on configuring access rules to cause log messages, see the help topic How Do I View Activity on My Firewall?

In order for firewall log entries to be collected, you must configure logging for the router. Go to **Router > Logging**. Click **Edit**, and configure logging. To obtain firewall logging messages, you must configure a logging level of debugging (7).

Firewall Log

The firewall log is displayed if the router is configured to maintain a log of connection attempts denied by the firewall.

Number of Attempts Denied by Firewall

Shows the number of connection attempts rejected by the firewall.

Attempts Denied by Firewall Table

Shows a list of connection attempts denied by the firewall. This table includes the following columns:

- Time column

  Shows the time that each denied connection attempt occurred.

- Description column

  Contains the following information about the denied attempt: log name, access rule name or number, service, source address, destination address, and number of packets. An example follows:

```
%SEC-6-IPACCESSLOGDP: list 100 denied icmp 171.71.225.148->10.77.158.140 (0/0), 3 packets
```

Update Button

Polls the router and updates the information shown on the screen with current information.

Search Button

Opens a search window. Choose a search type from the **Search** menu and enter the appropriate text in the Search field, then click the **Find** button to display matching log entries.

The search types are:

- Source IP Address—The IP address of the origin of the attack.

  A partial IP address can be entered.

- Destination IP Address—The IP address of the target of the attack.

  A partial IP address can be entered.

- Protocol—The network protocol used in the attack.
- Text—Any text found in the log entry.

Searches are *not* case sensitive.

View Top Attacks

From the View drop-down menu, choose one of the following ways to display information on top attacks:

- Top Attack Ports—Top attacks by target port.
- Top Attackers—by attacker IP address.

The top-attacks table below the View drop-down menu displays the top attack entries. If you choose Top Attack Ports from the View drop-down menu, the top-attacks table displays entries with the following columns:

- Port Number—The target port.
- Number of attacks—The number of attacks against the target port.
- Number of packets denied—The number of packets denied access to the target port.
- View Details—A link that opens a window containing the full log of attacks against the chosen port.

If you choose Top Attackers from the View drop-down menu, the top-attacks table displays entries with the following columns:

- Attacker's IP Address—The IP address from which the attacks are coming.

- Number of attacks—The number of attacks that have come from the IP address.
- Number of packets denied—The number of packets that have come from the IP address and were denied access.
- View Details—A link that opens a window containing the full log of the attacks from the chosen IP address.

Monitoring Firewall with a "Non-Administrator View" User Account

Firewall monitoring requires that Logging to Buffer be enabled on the router. If Logging to Buffer is not enabled, log in to Cisco CP using an Administrator view account or a non-view based user account with privilege level 15 and configure logging.

To configure logging in Cisco CP, go to **Router > Logging**.

Application Security Log

If logging has been enabled, and you have specified that alarms be generated when the router encounters traffic from applications or protocols that you have specified, those alarms are collected in a log that can be viewed from this window.

In order for Application Security log entries to be collected, you must configure logging for the router. Go to **Router > Logging**. Click **Edit**, and configure logging. To obtain firewall logging messages, you must configure a logging level of **informational (6)**, or higher. If you have already configured logging for **debugging(7)**, the log will contain application security log messages.

The following is example log text:

```
*Sep  8 12:23:49.914: %FW-6-DROP_PKT: Dropping im-yahoo pkt
128.107.252.142:1481 => 216.155.193.139:5050
*Sep  8 12:24:22.762: %FW-6-DROP_PKT: Dropping im-aol pkt
128.107.252.142:1505 => 205.188.153.121:5190
*Sep  8 12:26:02.090: %FW-6-DROP_PKT: Dropping im-msn pkt
128.107.252.142:1541 => 65.54.239.80:1863
*Sep  8 11:42:10.959: %APPFW-4-HTTP_PORT_MISUSE_IM: Sig:10006 HTTP
Instant Messenger detected - Reset - Yahoo Messenger from
10.10.10.2:1334 to 216.155.194.191:80
*Sep  8 12:27:54.610: %APPFW-4-HTTP_STRICT_PROTOCOL: Sig:15 HTTP
protocol violation detected - Reset -  HTTP Protocol not detected from
10.10.10.3:1583 to 66.218.75.184:80
```

```
*Sep  8 12:26:14.866: %FW-6-SESS_AUDIT_TRAIL_START: Start im-yahoo
session: initiator (10.10.10.3:1548) -- responder (66.163.172.82:5050)
*Sep  8 12:26:15.370: %FW-6-SESS_AUDIT_TRAIL: Stop im-yahoo session:
initiator (10.10.10.3:1548) sent 0 bytes -- responder
(66.163.172.82:5050) sent 0 bytes
*Sep  8 12:24:44.490: %FW-6-SESS_AUDIT_TRAIL: Stop im-msn session:
initiator (10.10.10.3:1299) sent 1543 bytes -- responder
(207.46.2.74:1863) sent 2577 bytes
*Sep  8  11:42:01.323: %APPFW-6-IM_MSN_SESSION: im-msn un-recognized
service session initiator 14.1.0.1:2000 sends 1364 bytes to responder
207.46.108.19:1863
*Sep  8  11:42:01.323: %APPFW-6-IM_AOL_SESSION: im-aol text-chat
service session initiator 14.1.0.1:2009 sends 100 bytes to responder
216.155.193.184:5050
```

Update Button

Updates the screen with current information about log details and the most current log entries.

Search Button

Opens a search window. In the search window, enter text in the Search field and click the **Find** button to display all entries containing the search text. Searches are *not* case sensitive.

SDEE Message Log

This window lists the SDEE messages received by the router. SDEE messages are generated when there are changes to IPS configuration.

SDEE Messages

Choose the SDEE message type to display:

- All— SDEE error, status, and alert messages are shown.
- Error—Only SDEE error messages are shown.
- Status—Only SDEE status messages are shown.
- Alerts—Only SDEE alert messages are shown.

Update Button

Click to check for new SDEE messages.

Search Button

Opens a search window. Choose a search type from the **Search** menu and enter the appropriate text in the Search field, then click the **Find** button to display matching log entries.

The search types are:

- Source IP Address
- Destination IP Address
- Text

Searches are *not* case sensitive.

Time

The time the message was received.

Type

Types are Error, Status, and Alerts. Click SDEE Message Text to see possible SDEE messages.

Description

Available description.

Traffic Status

This window displays a tree of traffic types that can be monitored on an interface. Before any traffic type can be monitored, it must be enabled on at least one interface.

You can choose one of the following traffic types from the Traffic Status tree:

- Netflow Top Talkers
- QoS

- Application/Protocol Traffic

  This type uses Network-based application recognition (NBAR) to monitor traffic.

Netflow Top Talkers

If Netflow statistics have been enabled for at least one interface in **Configure > Interfaces and Connections > Edit Interface/Connection**, you can view Netflow statistics. Choose **Top N Traffic Flows > Top Protocols** or **Top N Traffic Flows > Top Talkers** (high-traffic sources) from the Traffic Status tree.

Note If the router Cisco IOS image does not support Netflow, the Netflow choices will not be available in the Traffic Status tree.

Top Protocols

This window displays a table with the following columns:

- Protocol—Protocol being examined.
- Total Flows—Total number of flows associated with that protocol.
- Flows/Sec—Active flows per second for the protocol.
- Packets/Flow—Packets transmitted per flow.
- Bytes/Packet—Bytes per transmitted packet.
- Packets/Sec—Packets transmitted per second.

Update Button

Updates the window with current information about the flows.

Top Talkers

This window displays a table with the following columns:

- **Source IP Address**—Source IP address of the top talker.

Select a source IP address to see more information in **Flow status for the source address**.

- **Packets**—Total number of packets received from the source IP address.
- **Bytes**—Total number of bytes received from the source IP address.
- **Flows**—Number of flows associated with the source IP address.

Note If Netflow top talkers is not enabled in **Configure > Router > NetFlow**, then statistics for the top ten talkers are displayed.

Flow status for the source address

This table displays the following information about the flow associated with the selected source IP address:

- **Destination IP Address**—Target IP address of the top talker.
- **Protocols**—Protocols used in the packets exchanged with the destination IP address.
- **Number of Packets**—Number of packets exchanged with the destination IP address.

Update Button

Updates the window with current information about the flows.

QoS

The QoS Status window allows you to monitor the performance of the traffic on QoS configured interfaces (see Associating a QoS Policy With an Interface). This window also allows you to monitor bandwidth utilization and bytes-sent for interfaces with no QoS configuration. Monitoring inbound traffic on QoS interfaces shows the statistics only at a protocol level. Protocol-level statistics for non-QoS interfaces are collected for traffic in both directions.

This window allows you to monitor the following statistics:

- Bandwidth utilization for Cisco CP defined traffic types
  - Bandwidth utilization per class under each traffic type

  - Bandwidth utilization for protocols under each class

  Bandwidth utilization is shown in Kbps.

- Total incoming and outgoing bytes for each traffic type
  - Incoming and outgoing bytes for each class defined under the traffic type
  - Incoming and outgoing bytes for each protocol for each class

  If the value is more than 1,000,000, then the graph may show the bytes as a multiple of 10^6. If the value is more than 1,000,000,000, then the graph may show the bytes as a multiple of 10^9.
- Packets dropped statistics for each traffic type

Interface—IP/Mask—Slot/Port—Description

This area lists the interfaces with associated QoS policies, their IP addresses and subnet masks, slot/port information if applicable, and available descriptions.

Select the interface that you want to monitor from this list.

View Interval

Select the interval at which statistics should be gathered:

- Now—Statistics are gathered when you click **Start Monitoring**.
- Every 1 minute—Statistics are gathered when you click **Start Monitoring**, and refreshed at 1-minute intervals.
- Every 5 minutes—Statistics are gathered when you click **Start Monitoring**, and refreshed at 5-minute intervals.
- Every 1 hour—Statistics are gathered when you click **Start Monitoring**, and refreshed at 1-hour intervals.

Start Monitoring

Click to start monitoring QoS statistics.

Select QoS Parameters for Monitoring

Select the traffic direction and type of statistics you want to monitor.

Direction

Click either **Input** or **Output**.

Statistics

Select one of the following

- Bandwidth
- Bytes
- Packets dropped

All Traffic—Real-Time—Business-Critical—Trivial

Cisco CP displays statistics for all traffic classes in bar chart form, based on the type of statistic you selected. Cisco CP displays a message instead of a bar chart if there are not adequate statistics for a particular traffic type.

Associating a QoS Policy With an Interface

Step 1 Go to **Interfaces and Connections > Edit Interface/Connection**.

Step 2 From the Interface List, choose the interface to which you want to associate a QoS policy.

Step 3 Click the **Edit** button.

Step 4 Click the **Application Service** tab.

Step 5 Choose a QoS policy from the **Inbound** drop-down list to associate with inbound traffic on the interface.

Step 6 Choose a QoS policy from the **Outbound** drop-down list to associate with outbound traffic on the interface.

Application/Protocol Traffic

This window allows you to monitor application and protocol traffic using Network-based application recognition (NBAR), a protocol and application discovery feature. NBAR is used to classify packets for more efficient handling of network traffic through a specific interface.

Note If the router Cisco IOS image does not support NBAR, this status window will not be available.

Enable NBAR

To display the status of NBAR for a specific interface, NBAR must first be enabled on that interface. To enable NBAR, follow these steps:

Step 1 Go to **Interfaces and Connections > Edit Interface/Connection**.

Step 2 Choose the interface for which you want to enable NBAR from the Interface List.

Step 3 Click the **Edit** button.

Step 4 Click the **Application Service** tab.

Step 5 Check the **NBAR** check box.

NBAR Status

The NBAR status table displays the following statistics for the interface you choose from the **Select an Interface** drop-down list:

- Input Packet Count—The number of packets of the protocol shown incoming to the chosen interface.
- Output Packet Count—The number of packets of the protocol shown outgoing from the chosen interface.
- Bit rate (bps)—The speed, in bits per second, of traffic passing through the interface.

Firewall Status

This window displays the following statistics about the firewall configured on the router:

- Number of Interfaces Configured for Inspection—The number of interfaces on the router that are configured to have traffic inspected by a firewall.

- Number of TCP Packets Count—The total number of TCP packets transmitted through the interfaces configured for inspection.
- Number of UDP Packets Count—The total number of UDP packets transmitted through the interfaces configured for inspection.
- Total number of active connections—The count of current sessions.

The Firewall Status window also displays active firewall sessions in a table with the following columns:

- Source IP Address—The IP address of the packet's origin host.
- Destination IP Address—The IP address of the packet's destination host.
- Protocol—The network protocol being examined.
- Match Count—The number of packets matching the firewall conditions.

Update button

Click this button to refresh the firewall sessions in the table and display the most current data from the router.

Zone-Based Policy Firewall Status

If the router runs a Cisco IOS image that supports the Zone-Based Policy Firewall feature, you can display the status of the firewall activity for each zone pair configured on the router.

Firewall Policy List Area

The firewall policy list area displays the policy name, source zone, and destination zone for each zone pair. The following table contains sample data for two zone pairs.

Zone Pair Name	Policy Name	Source Zone	Destination Zone
wan-dmz-in	pmap-wan	zone-wan	zone-dmz
wan-dmz-out	pmap-dmz	zone-dmz	zone-wan

In this sample table there is a zone pair configured for traffic inbound to the DMZ, and traffic outbound from the DMZ.

Choose the zone pair that you want to display firewall statistics for.

View Interval

Choose one of the following options to specify how data should be collected:

- Real-time data every 10 sec—Data is reported every 10 seconds. Each tick mark on the horizontal axis of the Dropped Packets and Allowed Packets graph represents 10 seconds.
- 60 minutes of data polled every 1 minute—Data is reported every 1 minute. Each tick mark on the horizontal axis of the Dropped Packets and Allowed Packets graph represents 1 minute.
- 12 hours of data polled every 12 minutes—Data is reported every 12 minutes. Each tick mark on the horizontal axis of the Dropped Packets and Allowed Packets graph represents 12 minutes.

Monitor Policy

Click **Monitor Policy** to collect firewall data for the selected policy.

Stop Monitoring

Click **Stop Monitoring** to stop collecting firewall data.

Statistics Area

This area displays the firewall statistics for the selected zone pair. Control the display in this area by clicking on nodes in the tree on the left hand side. The following sections describe what you see when you click on each of the nodes.

Active Sessions

Clicking **Active Sessions** displays the traffic type, source IP address, and destination IP address for traffic that is inspected in the chosen zone pair.

Dropped Packets

For the chosen zone pair, clicking **Dropped Packets** displays a graph showing the cumulative number of dropped packets against the time interval chosen in the View Interval list. Data is collected on the traffic configured to be dropped and logged in the Layer 4 policy map.

Allowed Packets

For the chosen zone pair, clicking **Allowed Packets** displays a graph showing the cumulative number of allowed packets against the time interval chosen in the View Interval list. Data is collected on the traffic configured with the pass action in the Layer 4 policy map.

VPN Status

This window displays a tree of VPN connections that are possible on the router. You can choose one of the following VPN categories from the VPN connections tree:

- IPSec Tunnels
- DMVPN Tunnels
- Easy VPN Server
- IKE SAs
- SSL VPN Components

To view statistics on an active VPN category, choose it from the VPN connections tree.

IPSec Tunnels

This group displays statistics about each IPSec VPN that is configured on the router. Each row in the table represents one IPSec VPN. The columns in the table and the information they display are as follows:

- Interface column

  The WAN interface on the router on which the IPSec tunnel is active.

- Local IP column

The IP address of the local IPSec interface.

- Remote IP column

  The IP address of the remote IPSec interface.

- Peer column

  The IP address of the remote peer.

- Tunnel Status

  The current status of the IPSec tunnel. Possible values are:

  - Up—The tunnel is active
  - Down—The tunnel is inactive due to an error or hardware failure.

- Encapsulation Packets column

  The number of packets encapsulated over the IPSec VPN connection.

- Decapsulation Packets column

  The number of packets decapsulated over the IPSec VPN connection.

- Send Error Packets column

  The number of errors that have occurred while sending packets.

- Receive Error Packets column

  The number of errors that have occurred while receiving packets.

- Encrypted Packets column

  The number of packets encrypted over the connection.

- Decrypted Packets column

  The number of packets decrypted over the connection.

Monitor Tunnel Button

Click to monitor the IPSec tunnel chosen in the IPSec Tunnel table. See Monitoring an IPSec Tunnel.

Test Tunnel.. Button

Click to test a selected VPN tunnel.The results of the test will be shown in another window.

Update button

Click this button to refresh the IPSec Tunnel table and display the most current data from the router.

Monitoring an IPSec Tunnel

To monitor an IPSec tunnel, follow these steps:

Step 1 Choose the tunnel you want to monitor in the IPSec Tunnel table.

Step 2 Choose the types of information you want to monitor by checking the check boxes under **Select Item to Monitor**.

Step 3 Choose the time interval for the real-time graphs using the **View Interval** drop-down list.

DMVPN Tunnels

This group displays the following statistics about Dynamic Multi-point VPN (DMVPN) tunnels. Each row reflects one VPN tunnel.

- Remote Subnet column

  The network address of the subnet to which the tunnel connects.

- Remote Tunnel IP column

  The IP address of the remote tunnel. This is the private IP address given the tunnel by the remote device.

- IP Public Interface of Remote Router column

  IP address of the public (outside) interface of the remote router.

- Status column

  The status of the DMVPN tunnel.

- Expiration column

  The time and date when the tunnel registration expires and the DMVPN tunnel will be shut down.

Monitor Tunnel Button

Click to monitor the DMVPN tunnel chosen in the DMVPN Tunnel table. See Monitoring a DMVPN Tunnel.

Update button

Click this button to refresh the DMVPN Tunnel table and display the most current data from the router.

Reset Button

Click to reset statistics counters for the tunnel list. Number of packets encapsulated and decapsulated, number of sent and received errors, and number of packets encrypted and decrypted are set to zero.

Monitoring a DMVPN Tunnel

To monitor a DMVPN tunnel, follow these steps:

Step 1 Choose the tunnel you want to monitor in the DMVPN Tunnel table.

Step 2 Choose the types of information you want to monitor by checking the check boxes under **Select Item to Monitor**.

Step 3 Choose the time interval for the real-time graphs using the **View Interval** drop-down list.

Easy VPN Server

This group displays the following information about each Easy VPN Server group:

- Total number of server clients (in upper right corner)
- Group Name
- Number of client connections

Group Details Button

Clicking **Group Details** shows the following information about the selected group.

- Group Name
- Key
- Pool Name
- DNS Servers
- WINS Servers
- Domain Name
- ACL
- Backup Servers
- Firewall-R-U-There
- Include local LAN
- Group lock
- Save password
- Maximum connections allowed for this group
- Maximum logins per user

Client Connections in this Group

This area shows the following information about the selected group.

- Public IP address
- Assigned IP address
- Encrypted Packets
- Decrypted Packets
- Dropped Outbound Packets
- Dropped Inbound Packets
- Status

Update button

Click this button to display the most current data from the router.

Disconnect button

- Choose a row in the table and click Disconnect to drop the connection with the client.

IKE SAs

This group displays the following statistics about each active IKE security association configured on the router:

- Source IP column

  The IP address of the peer originating the IKE SA.

- Destination IP column

  The IP address of the remote IKE peer.

- State column

  Describes the current state of IKE negotiations. The following states are possible:

  - MM_NO_STATE—The Internet Security Association and Key Management Protocol (ISAKMP) SA has been created but nothing else has happened yet.
  - MM_SA_SETUP—The peers have agreed on parameters for the ISAKMP SA.
  - MM_KEY_EXCH—The peers have exchanged Diffie-Hellman public keys and have generated a shared secret. The ISAKMP SA remains unauthenticated.
  - MM_KEY_AUTH—The ISAKMP SA has been authenticated. If the router initiated this exchange, this state transitions immediately to QM_IDLE and a Quick mode exchange begins.
  - AG_NO_STATE—The ISAKMP SA has been created but nothing else has happened yet.
  - AG_INIT_EXCH—The peers have done the first exchange in Aggressive mode but the SA is not authenticated.
  - AG_AUTH—The ISAKMP SA has been authenticated. If the router initiated this exchange, this state transitions immediately to QM_IDLE and a Quick mode exchange begins.

  - QM_IDLE—The ISAKMP SA is idle. It remains authenticated with its peer and may be used for subsequent Quick mode exchanges.
- Update button—Click this button to refresh the IKE SA table and display the most current data from the router.
- Clear button—Select a row in the table and click Clear to clear the IKE SA connection.

SSL VPN Components

Clicking the VPN Status button in the monitoring window causes the router to begin monitoring SSL VPN activity. This window displays the data gathered for all SSL VPN contexts configured on the router.

By default, this data is refreshed every 10 seconds. If 10 seconds is too short an interval for you to view data before the next refresh, you can select an auto-refresh interval of **Real-time data every minute**.

Choose a context in the SSL VPN tree to view data for that context and data for the users who are configured for the context.

System Resources

The percentage of CPU and memory resources that SSL VPN traffic is using across all contexts is shown in this area.

Number of Connected Users

This graph shows the number of active users over time. The peak number of active users since monitoring began is displayed at the top of the graph area. The time that monitoring began is shown in the lower left-hand corner of the graph, and the current time is shown centered under the graph.

Tabbed Area

This area of the window displays gathered statistics in a series of tabs for easier viewing.

Click any of the links below for a description of the data the tab displays.

User Sessions

URL Mangling

Port Forwarding

CIFS

Full Tunnel

Note If a feature such as port forwarding or full tunnel has not been configured on the router, no data will be shown in the tab for that feature.

Some statistics are collected anew each time the router refreshes monitoring data. Other statistics, such as peak number of active users statistics, are collected at refresh time, but compared against the same data collected when monitoring began. Monitoring of all VPN activity, including SSL VPN, begins when you click the **VPN Status** button.

SSL VPN Context

This window shows the same types of information as the SSL VPN Components window but only shows the data gathered for the chosen context. For a description of the information displayed, click SSL VPN Components.

User Sessions

This tab displays the following information about SSL VPN user sessions.

- Active user sessions—The number of SSL VPN user sessions, of all traffic types, active since monitoring data was refreshed.
- Peak user sessions—The highest number of active SSL VPN user sessions since monitoring began.
- Active user TCP connections—The number of TCP-based SSL VPN user sessions active since monitoring data was refreshed.
- Session alloc failures—The number of session allocation failures that have occurred since monitoring began.
- VPN Session timeout—The number of VPN session timeouts that have occurred since monitoring began.

- User cleared VPN Sessions—The number of VPN sessions that have been cleared by users since monitoring began.
- AAA pending requests—The number of AAA requests that have been pending since monitoring data was refreshed.
- Peak time— The longest user session recorded since monitoring began.
- Terminated user sessions—The number of users sessions that have terminated since monitoring began.
- Authentication failures—The number of sessions that have failed to be authenticated since monitoring began.
- VPN Idle timeout—The number of VPN idle timeouts that have occurred since monitoring began.
- Exceeded context user limit—The number of times, since monitoring began, that a user has attempted to initiate a session when the context session limit had already been reached.
- Exceeded total user limit—The number of times, since monitoring began, that a user has attempted to initiate a session when the total session limit had already been reached.

URL Mangling

This tab displays data about URL mangling activities. For more information, refer to the command reference available at the following link:

http://www.cisco.com/en/US/products/hw/switches/ps708/products_command_reference_chapter09186a0080419245.html#wp1226849

Port Forwarding

This tab displays data gathered about port forwarding activities. For more information, refer to the command reference at the following link:

http://www.cisco.com/en/US/products/hw/switches/ps708/products_command_reference_chapter09186a0080419245.html#wp1226849

CIFS

This tab displays data gathered about CIFS requests, responses, and connections. For more information refer to the command reference available at the following link:

http://www.cisco.com/en/US/products/hw/switches/ps708/products_command_reference_chapter09186a0080419245.html#wp1226849

Full Tunnel

This tab displays information about full tunnel connections between SSL VPN clients and servers on the corporate intranet.

- Active tunnel connections—The number of active full tunnel connections since data was last refreshed. Data can be refreshed every 10 seconds, or every minute.
- Active connections peak time—The full tunnel connection of the longest duration since monitoring began.
- Peak active tunnel connections—The highest number of active full tunnel connections since monitoring began.
- Tunnel connection attempts failed—The number of full tunnel connection attempts that have failed since monitoring began.
- Tunnel connection attempts succeeded— The number of full tunnel connections successfully established since monitoring began.

Server:

- IP packets sent to server—The number of IP packets from full-tunnel clients that the router forwarded to servers on the corporate intranet.
- IP traffic sent to server in bytes—The amount of IP traffic, in bytes, forwarded from full-tunnel clients to servers on the corporate intranet.
- IP packets received from server—The number of IP packets that the router has received from servers with full-tunnel connections to clients.
- IP traffic received from server in bytes—The amount of IP traffic, in bytes, received from servers on the corporate intranet with full-tunnel connections to clients.

User List

This window displays user information for the context chosen in the SSL VPN Components tree. Because there can be multiple group polices configured for the context, each using their own URL list and server lists, this screen provides valuable information about how individual users are using their SSL VPN connections.

You can control individual use of the SSL VPN in this window by choosing a user and clicking the **Disconnect** button.

User List Area

This area lists all active users in all groups configured for this context. This area displays the following information:

- User Login Name—The username that is authenticated with the AAA server.
- Client IP address—The user's assigned SSL VPN IP address for this session. This IP address is drawn from the address pool configured for this context.
- Context—The SSL VPN context under which the group policy for this user has been configured.
- No. of connections—The number of active connections for the user. For example, the user might have a connection to a mail server, and might also be browsing files on another server in the network.
- Created—The time at which the session was created.
- Last used—The time at which the user last sent traffic over any active connection.
- Cisco Secure Desktop—True or False. Indicates whether Cisco Secure Desktop has been downloaded to the user's PC.
- Group name—The name of the group policy under which the user is configured. The group policy specifies the URL list, the services available to the users, the WINS servers available to resolve server names, and the servers that the users can see when browsing files on the corporate intranet.
- URL list name—The name of the URL list that appears on the user's portal page. The URL list is configured for the group to which the user belongs. See Group Policy: Clientless Tab for more information.

- Idle timeout—The number of seconds that a session can remain idle before the router terminates it. This value is configured for the group to which the user belongs. See Group Policy: General Tab for more information.
- Session timeout—The maximum number of seconds that a session can remain active before being terminated. This value is configured for the group to which the user belongs. See Group Policy: General Tab for more information.
- Port forwarding list name—This value is configured for the group to which the user belongs. See Group Policy: Thin Client Tab for more information.
- WINS Name Service list name—This value is configured for the group to which the user belongs. See Group Policy: Clientless Tab for more information.

IPS Status

This window appears if the router is using a Cisco IOS image that supports IPS version 4.x or earlier. This window displays a table of IPS signature statistics, grouped by signature type. The following statistics are shown:

- **Signature ID**—Numerical signature identifier.
- **Description**—Description of the signature.
- **Risk Rating**—A a value between 0 and 100 that represents a numerical quantification of the risk associated with a particular event on the network.
- **Action**—The action that is to be taken when a packet matches a signature.
- **Source IP Address**—The IP address of the packet's origin host.
- **Destination IP Address**—The IP address of the packet's destination host.
- **Hits**—Number of matching packets.
- **Drop Counts**—Number of matching packets dropped.

To sort the signatures, click the column head with the name of signature statistic you want to sort by.

Note If you sort the signatures, the signatures may no longer be grouped by type. To restore the grouping of signatures by type, click the **Update** button.

Total Active Signatures

Displays the total number of signatures available that are active on your router.

Total Inactive Signatures

Displays the total number of signatures available that are inactive on your router.

Update Button

Click to check for and include the latest signature statistics.

Clear Button

Click to set all signature statistic counters to 0.

SDEE Log

Click to view SDEE messages. You can also view these messages by clicking **Monitor > Router > Logging > SDEE Message Log**.

IPS Signature Statistics

This window is displayed if the router is using an IOS IPS 5.x configuration. Statistics are displayed for each enabled signature in the IOS IPS configuration. The top of the window displays signature totals to provide a snapshot of the signature configuration. The following totals are provided:

- Total Signatures
- Total Enabled Signatures
- Total Retired Signatures
- Total Compiled Signatures

Update and Clear Buttons

Click **Update** to check for and include the latest signature statistics. Click **Clear** to set all signature statistic counters to 0.

SDEE Log

Click to view SDEE messages. You can also view these messages by clicking **Monitor > Router > Logging > SDEE Message Log**.

Signature List Area

The Signature ID, Description, number of hits, and drop count is shown for all signatures. If packet arrives that matches a signature, the source and destination IP addresses are listed as well.

IPS Alert Statistics

The IPS Alert Statistics window displays alert statistics in a color-coded format for easy recognition. The top part of the screen displays a legend that explains the use of colors in the display.

Note The IPS Alert Statistics window displays only IPS signatures having alarm counts. The IPS Signature Statistics window displays IPS signatures having drop counts.

Color	Explanation
RED	The event that generated the alert has a high Risk Rating (RR) in the range of 70 to 100.
MAGENTA	The event that generated the alert has a medium Risk Rating (RR) in the range of 40 to 69.
BLUE	The event that generated the alert has a low Risk Rating (RR) in the range of 0 to 39.

By clicking on a column heading, you sort the display based on the values of that parameter. For example, by clicking on the **Signature ID** heading, you sort the display in ascending or descending numerical order of signature IDs. Each column is described in the following list:

- **Signature ID**—Numerical signature identifier.

- **Description**—Description of the signature.
- Risk Rating—A value between 0 and 100 that represents a numerical quantification of the risk associated with a particular event on the network.
- Event Action—The action that IOS IPS is to take when an event matching the signature occurs.
- Source IP Address—The IP address from which the packet originated.
- Destination IP Address—The IP address to which the packet was addressed. If the packet is malicious, the Destination IP address can be considered the target.
- Hits—Number of matching packets.
- Drop Count—The number of matching packets dropped.
- Engine—The signature engine associated with the signature.

NAC Status

If NAC is configured on the router, Cisco CP can display snapshot information about the NAC sessions on the router, the interfaces on which NAC is configured, and NAC statistics for the selected interface.

The top row in the window displays the number of active NAC sessions, the number of NAC sessions being initialized, and a button that allows you to clear all active and initializing NAC sessions

The window lists the router interfaces with associated NAC policies.

```
FastEthernet0/0    10.10.15.1/255.255.255.0   0
```

Clicking on an interface entry displays the information returned by posture agents installed on the hosts in the subnet for that interface. An example of the interface information follows:

```
10.10.10.5      Remote EAP Policy      Infected       12
```

10.10.10.1 is the host's IP address. Remote EAP Policy is the type of authentication policy that is in force. The host's current posture is Infected, and it has been 12 minutes since the host completed the admissions control process.

Note This area of the window contains no data if no posture information is returned by the hosts on the selected subnet.

The authentication types are:

- **Local Exception Policy**—An exception policy that is configured on the router is used to validate the host.
- **Remote EAP Policy**—The host returns a posture, and an exception policy assigned by an ACS server is used.
- **Remote Generic Access Policy**—The host does not have a posture agent installed, and the ACS server assigns an agentless host policy.

The posture agents on the hosts may return the following posture tokens:

- **Healthy**—The host is free of known viruses, and has the latest virus definition files.
- **Checkup**—The posture agent is determining if the latest virus definition files have been installed.
- **Quarantine**—The host does not have the latest virus definition files installed. The user is redirected to the specified remediation site that contains instructions for downloading the latest virus definition files.
- **Infected**—The host is infected with a known virus. The user is redirected to a remediation site to obtain virus definition file updates.
- **Unknown**—The host's posture is unknown.

802.1x Authentication Status

802.1x Authentication on Interfaces Area

Interface

802.1x Authentication

Reauthentication

802.1x Clients Area

Client MAC Address

Authentication Status

Interface

Traffic Monitoring

For information about how to use Cisco Configuration Professional (Cisco CP) to configure the Traffic Monitoring feature, see the screencast at: http://www.cisco.com/en/US/docs/net_mgmt/cisco_configuration_professional/scrcst/ccpsc.html.

Note You must have internet access to view the screencast.

Traffic Volume

For information about how to use Cisco Configuration Professional (Cisco CP) to configure the Traffic Monitoring feature, see the screencast at: http://www.cisco.com/en/US/docs/net_mgmt/cisco_configuration_professional/scrcst/ccpsc.html.

Note You must have internet access to view the screencast.

Custom Traffic Classifier

Custom traffic classifier is used to group protocols and show grouped protocols as one entry in the graph. For example HTTP and HTTPS can be classified as Web.

To create a custom classifier:

Step 1 Create a new properties file, for example, custom.properties under CCP\Installed Directory\CiscoCP\webapps\ROOT\Counterpoint\assets\data.

Step 2 Add entries in the properties file to group protocols. The entries have to be in the form of <tcp or udp>-<portno> = <Group Name>.

For example to group HTTP and HTTPS as Web, the entries are added as:

tcp-80 = Web

tcp-443 = Web

Step 3 Add entry to newly created properties file in classifiers.properties for it to reflect in the Traffic Volume user interface:

custom = custom.properties

Step 4 Refresh the user interface to view the newly added custom grouping in Traffic Classifier.

PART 10

Configuring Switches

This section provides information about how to configure switches.

CHAPTER 71

IP Address

An IP address is a unique 32 bit number assigned to each machine connected to the Internet. IP addresses are denoted as four decimal numbers (also called octets), and are separated by dots. This format of representing an IP address is known as "dotted quad" or "dotted decimal" notation.

An IP address consists of two parts, one identifying the network and one identifying the host in the network. In the class system, the class of the address determines which part belongs to the network address, and which part belongs to the host address. IP addresses have been classified into five classes (described in Table 71-1).

Table 71-1 shows the list of classes with the start address and end address range information.

Table 71-1 Cisco CP—IP Address Classes

Class	Start Address	End Address
A	0.0.0.0	127.255.255.255
B	128.0.0.0	191.255.255.255
C	192.0.0.0	223.255.255.255
D	224.0.0.0	239.255.255.255
E	240.0.0.0	255.255.255.255

In Cisco CP, you can use this IP Address feature to assign the IP address along with the subnet mask to the selected VLAN.

Related Topics

- Assign IP Address, page 71-2
- IP Address Reference, page 71-3

Assign IP Address

Procedure

Use this procedure to assign the IP address to the selected VLAN using Cisco CP.

Step 1 Choose **Configure > Switch > IP Address**. The IP Address Summary page opens. See IP Address Summary Page, page 71-3 for more information.

Step 2 Choose the VLAN from the **VLAN** drop-down menu to assign the IP address for the selected VLAN ID.

Step 3 Enter the IP address in the **IP Address** field.

Step 4 Enter the subnet mask in the **Subnet Mask** field.

Step 5 Enter the default gateway IP address in the **Default Gateway** field. See IP Address Summary Page, page 71-3 for more information.

Note The Gateway address cannot be the same as the IP address assigned to the VLAN.

Step 6 Click **Apply**. The Deliver Configure to Device dialog box opens.

Step 7 Click **Deliver** in the Deliver dialog box to deliver the configuration changes to the device.

Related Topic

- IP Address Reference, page 71-3

IP Address Reference

This section describes the summary page that you can use when working with IP Address feature and includes the following topic:

- IP Address Summary Page, page 71-3

IP Address Summary Page

Use this IP Address Summary page to apply the IP address to the selected VLAN using Cisco CP.

How to Get to This Page

Choose **Configure > Switch > IP Address**.

Field Reference

Table 71-2 IP Address Summary Page

Element	Description
IP Address	
VLAN	Choose the VLAN ID from the **VLAN** drop-down menu to assign the IP address.
IP Address	Enter the IP address.
Subnet Mask	Enter the Subnet Mask.
Default Gateway	
Default Gateway	Enter the default gateway IP address.
Apply button	Click this button to apply the changes.

CHAPTER 72

Port

A port is a physical entity used to connect devices in a network. Packets are sent and received through these ports within the devices. The physical characteristics (duplex, speed, portfast, Auto-MDIX, and so on) can be configured on a port.

Note The HWIC and NM modules related screens are available at **Configure > Interface Management > Ports > Port**. The SM and NME modules related screens are available at **Configure > Switching Module > Ports > Port**.

Related Topics

- Configuring Port, page 72-1
- Runtime Status, page 72-12

Configuring Port

By default, all ports on a switch are enabled and the port parameters are set with initial values. Use the Port window to view and modify their parameters.

When certain parameters (speed, duplex and so on) are set to auto, it negotiates with the other end of the port.

An auto negotiation mismatch can occur under the following conditions:

- When a manually set duplex parameter is different from the one that is set on the attached port.

- When a port is set to auto negotiate, and the attached port is set to full duplex with no auto negotiation.

A mismatch on Fast Ethernet ports reduce performance or link errors. On Gigabit Ethernet ports, the link does not come up, and statistics are not reported.

To correct mismatched port settings, follow one of the guidelines:

- Set both the ports to auto negotiate with speed and duplex.
- Manually set the speed and duplex parameters for the ports on both ends of the connection.

Note To connect to a remote Fast Ethernet device that does not auto negotiate, you should explicitly set the duplex on the local device to a value, other than Auto. Speed negotiation works even if the other device does not auto negotiate. To connect to a remote Gigabit Ethernet device that does not auto negotiate, disable auto negotiation on the local device and set the duplex and flow control parameters to be compatible with the remote device.

Related Topics

- How to Edit a Port, page 72-2
- Port Reference, page 72-4

How to Edit a Port

Procedure

Use this procedure to edit the existing parameters of a port.

Step 1 Choose **Configure > Switching Module > Ports > Port** or **Configure > Interface Management > Ports > Port** or **Configure > Switching > Ports > Port**.

The Port Summary Page opens. See Port Summary Page, page 72-4 for more information.

Step 2 Select the interface to edit the parameters, and click **Edit**. The Edit Port dialog box opens with previously set parameters. See Edit Port Dialog Box, page 72-7 for more information.

Step 3 The selected interface name is displayed in the **Interface Name** field.

Note You can select multiple interfaces to edit the parameters. When you select multiple interfaces, the Edit Port dialog box does not display the interface name in the **Interface Name** field.

Step 4 Enter the description for the selected interface in the **Description** field.

Step 5 Click **enable** or **disable** radio button to administratively enable or disable the port. See Edit Port Dialog Box, page 72-7 for more information.

Step 6 Select the type of duplex mode from the **Duplex** drop-down menu such as : auto, or half, or full. See Edit Port Dialog Box, page 72-7 for more information.

Step 7 Select the type of speed setting from the **Speed** drop-down menu. See Edit Port Dialog Box, page 72-7 for more information.

Step 8 In the **Port Fast** field, choose **enable** or **disable** for the selected port from the drop-down menu; otherwise select **enable when static access**, only for static-access ports.

Step 9 Choose **off**, **desire** or **on** from the **Flow control (Receive)** drop-down menu. See Edit Port Dialog Box, page 72-7 for more information.

Step 10 Choose **on** or **off** mode from the **Auto MDIX** drop-down menu. See Edit Port Dialog Box, page 72-7 for more information.

Step 11 Choose **auto-select**, **rj45** or **sfp** from the **Media Type** from the drop-down menu. See Edit Port Dialog Box, page 72-7 for more information.

Note The **Media type** setting is applicable only for Gigabit Ethernet.

Step 12 Click **OK**. The Deliver Configuration to Device dialog box opens.

Step 13 Click **Deliver** in the Deliver dialog box to deliver the configuration changes to the device.

Related Topics

- Port Reference, page 72-4
- Runtime Status, page 72-12

Port Reference

This section describes the summary pages and the dialog boxes you can use when modifying the parameters of the ports and includes the following topics:

- Port Summary Page, page 72-4
- Edit Port Dialog Box, page 72-7

Port Summary Page

Use this summary page to view the port parameters and modify the same for the selected port.

How to Get to This Page

Choose **Configure > Switching Module > Ports > Port** or **Configure > Interface Management > Ports > Port** or **Configure > Switching > Ports > Port**.

Note For the HWIC and NM modules, the Port Summary page does not display the router interfaces. Also, the Flow Control (Receive), Auto MDIX, and Media type displays as not applicable.

Related Topics

- Edit Port Dialog Box, page 72-7
- Configuring Port, page 72-1

Field Reference

Table 72-1 Cisco CP—Port Summary page

Elements	Description
Port	Identifies the port: Fast Ethernet, Gigabit Ethernet, the module or slot number (0, 1, or 2), and the port number.
Description	Displays the description of the port.

Table 72-1 Cisco CP—Port Summary page (continued)

Elements	Description
Status	Displays one of the following status: • Enable • Disable
EtherChannel number	Displays the EtherChannel number.
Duplex	Displays the Duplex setting for the port. Displays one of the following option: • Auto • Half • Full
Speed	Displays the speed type of the port. Displays one of the following type: • auto • 10 • 100 • 1000 • auto 10 • auto 100 • auto 10 100 • auto 10 100 1000
PortFast	Displays the status of the PortFast. Displays one of the following status: • enable • disable • enable when static access

Table 72-1 Cisco CP—Port Summary page (continued)

Elements	Description
Flow Control (Receive)	Displays the status of the Flow Control. Displays one of the following status: • on • off • desired
Auto MDIX	Displays the status of the Auto MDIX. Displays one of the following status: • On • Off
Media type	Displays the Media type status. Displays one of the following status: • auto-select • rj45 • sfp **Note** The **Media Type** is set only on Gigabit Ethernet ports.
Edit button	Click this button to edit the selected interface. You can select multiple interfaces to edit the parameters. When you select multiple interfaces, the Edit Port dialog box does not display the interface name in the **Interface Name** field.

Table 72-2 shows the link states that result from auto-MDIX settings with correct and incorrect cabling.

Table 72-2 Link Conditions and Auto-MDIX Settings

Local Side Auto-MDIX	Remote Side Auto-MDIX	With Correct Cabling	With Incorrect Cabling
On	On	Link up	Link up
On	Off	Link up	Link up

Table 72-2 Link Conditions and Auto-MDIX Settings

Local Side Auto-MDIX	Remote Side Auto-MDIX	With Correct Cabling	With Incorrect Cabling
Off	On	Link up	Link up
Off	Off	Link up	Link down

Related Topic

- Edit Port Dialog Box, page 72-7

Edit Port Dialog Box

Use this dialog box to modify the parameters of the selected ports using Cisco CP.

How to Get to This Page

1. Choose **Configure > Switching Module > Ports > Port** or **Configure > Interface Management > Ports > Port** or **Configure > Switching > Ports > Port**.
2. Click **Edit**.

Note Tunnel is not applicable for the HWIC and NM modules.

Related Topics

- Port Summary Page, page 72-4
- Configuring Port, page 72-1

Field Reference

Table 72-3 Edit Port Dialog box

Elements	Description
InterfaceName	Displays the name of the selected interface. When you select multiple interfaces, the Edit Port dialog box does not display the interface name in the **Interface Name** field.
Description	Enter a text or description for the selected interface. **Note** Special characters are allowed; however, don't use "?". Also, don't leave empty space.
Status	Click one of the following radio button to perform the selected action: • **Enable—**Administratively enables the port. • **Disable**—Administratively disables the port.
Duplex	Choose one of the following option from the drop-down menu: • **Auto**—Enables the interface to auto negotiate duplex with the connected device. • **Half**—Either can send or receive the packets. • **Full**—Packets are sent and received simultaneously.

Table 72-3 Edit Port Dialog box (continued)

Elements	Description
Speed	Choose one of the following option from the drop-down menu: • **Auto**—Enables the interface to auto negotiate the speed with the connected device. **Note** The default setting for Fast ethernet is 10/100-Mbps and Gigabit ethernet is 10/100/1000-Mbps ports. • **10**—Ports run at a forced speed of 10 Mbps. • **100**—Ports run at a forced speed of 100 Mbps. • **1000**—Ports run at a forced speed of 1000Mbps. • **Auto 10**—Ports auto negotiate and advertise a speed of about 10 Mbps to the other end of the link. • **Auto 100**—Ports auto negotiate and advertise a speed of 100 Mbps to the other end of the link. • **Auto 10 100**—Ports auto negotiate and advertise speeds 10 and 100 Mbps to the other end of the link. • **Auto 10 100 1000**—Ports auto negotiate and advertise speeds of 10, 100, and 1000 Mbps to the other end of the link. **Note** **1000** and **Auto 10 100 1000** are applicable only for Gigabit Ethernet ports.

Table 72-3 Edit Port Dialog box (continued)

Elements	Description
Port fast	Choose one of the following option from the drop-down menu: • **Enable—**When the Port Fast is enabled, the interface goes to forwarding state immediately bypassing the listening and learning states. Also, in the spanning-tree feature, this port will converge quickly irrespective of the port type. That means, the port fast characteristics will be applicable to port only if they are “access” or “trunk”. • **Disable**—When the Port Fast is disabled, the interface transits to listening state, learning state and then to forwarding state. If port fast is disable, it is disabled for all type of port. • **Enable with static access**—When the PortFast is set to “Enable when static access”**,** all the static access ports are configured to port fast. Also, in the spanning-tree protocol feature, this port will converge quickly only if the port type is “access”. If the port is trunk, then the port fast characteristic will not be applicable to this ports.
Flow control (Receive)	Set the ability of the interface to receive pause frames to **on**, **off**, or **desired**. By default, the state is **off**. • **Receive on (or desired)**—Port cannot send the pause frames but can operate with an attached device that is required to or can send pause frames; the port can receive pause frames. • **Receive off**—Flow control does not operate in either direction. In case of congestion, no indication is given to the link partner, and no pause frames are sent or received by either device.

Table 72-3 Edit Port Dialog box (continued)

Elements	Description
Auto MDIX	Choose one of the following option from the drop-down menu: • **On**—Interface automatically detects the required cable connection type (straight through or crossover) and configures the connection appropriately. • **Off**—Straight-through cables must be used to connect to the devices such as servers, workstations, or routers and crossover cables to connect to other switches or repeaters. **Note** By default, the Auto-MDIX is **On**. When the Auto-MDIX is on, you must set the interface speed and duplex to **auto** so that the feature operates correctly. Auto-MDIX is supported on all 10/100 and 10/100/1000-Mb/s interfaces. See Table 72-2 for more information.
Media type	Choose one of the following option from the drop-down menu: • **Auto-select**—Speed and duplex is set to auto and Auto-MDIX displays as Not Applicable. • **rj45**—Speed, duplex and the Auto-MDIX values can be configured. • **sfp**—Speed and duplex is set to auto and auto-MDIX displays as Not Applicable.
OK button	Click this button to save the Changes.
Cancel button	Click this button to avoid saving the changes that you entered.

Runtime Status

Use this page to view the actual runtime status of the ports like speed, duplex, ethernet link status and Auto-MDIX.

How to Get to This Page

1. Choose **Configure > Switching Module > Ports > Port** or **Configure > Interface Management > Ports > Port** or **Configure > Switching > Ports > Port**.
2. Choose **Runtime Status**.

Note For the HWIC and NM modules, the runtime status displays the status of all the ports on the modules except the router interfaces.

Related Topics

- Refreshing the Runtime Status Page, page 72-12
- Runtime Status Summary Page, page 72-13

Refreshing the Runtime Status Page

Procedure

Use this procedure to refresh the page.

Step 1 Choose **Configure > Switching Module> Ports > Port > Runtime Status** or **Configure > Interface Management > Ports > Port > Runtime Status** or **Configure > Switching > Ports > Port > Runtime Status**.

Step 2 Click **Refresh**. The page refreshes and updates the runtime status of the ports.

Related Topic

- Runtime Status Summary Page, page 72-13

Runtime Status Summary Page

Use this page to view the runtime status of the ports.

How to Get to This Page

Choose **Configure > Switching Module > Ports > Port > Runtime Status** or **Configure > Interface Management > Ports > Port > Runtime Status or Configure > Switching > Ports > Port > Runtime Status**.

Field Reference

Table 72-4 Cisco CP—Runtime status of Port

Element	Description
Interface	Identifies the port: Fast Ethernet, Gigabit Ethernet, the module or slot number (0, 1, or 2), and the port number.
Description	Displays the description of the interface.
Ethernet link	Displays the port state. Displays one of the following status: • disabled • notconnected • connected
Duplex	Displays the duplex status of the port. Displays one of the following: • auto • half • full
Speed	Displays the runtime status of the port speed.
Auto MDIX	Displays whether automatic medium-dependent interface crossover (auto-MDIX) is enabled or disabled on the port. **Note** For the HWIC and NM modules, Auto MDIX displays as not applicable.
Refresh button	Refreshes the page.

CHAPTER 73

EtherChannel

A group of Fast or Gigabit Ethernet port acts as a single logical port for high-bandwidth connections between switches, or between switches and servers. If a port within an EtherChannel fails, the previously carried traffic over the failed port, transfers to the remaining ports within the EtherChannel. You can create, edit, or delete an EtherChannel using Cisco CP.

Related Topics

- EtherChannel Overview, page 73-1
- Configuring EtherChannel, page 73-4

EtherChannel Overview

The EtherChannel provides fault-tolerant high-speed links between switches, routers, and servers. It consists of individual Fast or Gigabit Ethernet links bundled into a single logical link. The EtherChannel provides full-duplex bandwidth of up to 800 Mbps between your switch and another switch, or a host for the Fast EtherChannel on a switch with 24 Fast Ethernet ports. For a Gigabit EtherChannel, you can configure up to 8 Gbps (8 ports of 1 Gbps), depending on the number of supported Gigabit Ethernet interfaces.

Note Only Network Node Interfaces (NNIs) and Enhanced Network Interfaces (ENIs) support Link Aggregation Control Protocol (LACP) or Port Aggregation Protocol (PAgP).

Each EtherChannel has up to eight compatible configured Ethernet ports. All ports in every EtherChannel must be configured as either Layer 2 or Layer 3 ports. The number of EtherChannels are limited to 48 on a switch.

You can configure an EtherChannel in one of the following modes: PAgP, LACP, or On mode. PAgP and LACP are available only on NNIs and ENIs. You can configure both ends of the EtherChannel in following mode:

- If you configure one end of an EtherChannel in PAgP or LACP mode, the system negotiates with the other end of the channel to determine which ports should become active. Incompatible ports are suspended.
- If you configure an EtherChannel in the On-mode, no negotiations take place. The switch forces all compatible ports to become active in the EtherChannel. The other end of the channel (on the other switch) must also be configured in the on mode; otherwise, packet loss can occur.

Related Topics

- Load Balancing and Forwarding Methods, page 73-2
- Configuring EtherChannel, page 73-4
- EtherChannel Reference, page 73-7

For more information on PAgP and LACP, see:

http://www.cisco.com/en/US/docs/switches/connectedgrid/cgs2520/software/release/12_2_53_ex/configuration/guide/swethchl.html

Load Balancing and Forwarding Methods

EtherChannel balances different traffic load across the links in a channel. EtherChannel load balancing can use MAC addresses or IP addresses, source or destination addresses, or both source and destination addresses. The selected mode applies to all EtherChannels configured on the switch.

- **Source MAC address—**The traffic distribution depends on the source MAC address of the incoming packets. Packets from different hosts use different ports in the channel; packets from the same host use the same port in the channel.

- **Destination MAC address**—The traffic distribution depends on the destination host MAC address of the incoming packets. Packets directed to different destinations are sent on different ports in the channel; packets directed to the same destination are sent on the same port.
- **Source-Destination MAC address**—The traffic distribution depends on both the source and destination MAC addresses of the incoming packets.

Note Use this forwarding method if it is not clear whether source-MAC or destination-MAC address forwarding is preferable on a switch.

- **Source IP address**—The traffic distribution is based on the source IP address of the incoming packets. Packets from different IP addresses use different ports in the channel; packets from the same IP address use the same port in the channel.
- **Destination IP address**—The traffic distribution is based on the destination IP address of the incoming packets. Packets going to the same destination IP address are sent on the same port in the channel; packets going to different destination IP addresses are sent on different ports in the channel.
- **Source-Destination IP address**—The traffic distribution is based on both the source and destination IP addresses of the incoming packets.

Note Use this forwarding method if it is not clear whether source IP or destination IP address forwarding is preferable on a switch.

Different load-balancing methods have different advantages, and the choice of a particular load-balancing method should be based on the position of the switch in the network and the kind of traffic that needs to be load-distributed.

Related Topics

- EtherChannel Overview, page 73-1
- Configuring EtherChannel, page 73-4
- EtherChannel Reference, page 73-7

Configuring EtherChannel

Before you begin:

- Make sure that the ports are correctly configured. For more information, see the "EtherChannel Configuration Guidelines, page 73-4".
- After you configure an EtherChannel, configuration changes applied to the port-channel interface apply to all the physical ports assigned to the port-channel interface, and configuration changes applied to the physical port affect only the port to which you apply the configuration.

Related Topics

- EtherChannel Configuration Guidelines, page 73-4
- Creating, Editing and Deleting an EtherChannel, page 73-5
- EtherChannel Reference, page 73-7

EtherChannel Configuration Guidelines

Following are the guidelines to avoid configuration problems:

- Do not try to configure more than 48 EtherChannels on the switch.
- Configure a PAgP EtherChannel including only NNIs or only ENIs.
- Configure a LACP EtherChannel including only NNIs or only ENIs.
- Configure all ports in an EtherChannel to operate at the same speeds and duplex modes.
- On UNIs, the EtherChannel mode must always be configured to ON.
- All ports in an EtherChannel must be the same type, either UNI, NNI, or ENI. You cannot mix port types in an EtherChannel.
- Do not configure a port to be a member of more than one EtherChannel group.
- Do not configure an EtherChannel in both the PAgP and LACP modes. Individual EtherChannel groups can run either PAgP or LACP, but they cannot inter operate.

Note PAgP and LACP are only available on NNIs and ENIs.

- Do not configure a secure port as part of an EtherChannel or configure any ports under EtherChannel as a secure port.
- Do not configure a port that is an active or a not-yet-active member of an EtherChannel as an 802.1x port. If you try to enable 802.1x on an EtherChannel port, an error message appears, and 802.1x is not enabled.l
- For Layer 2 EtherChannels:
  - Assign all ports in the EtherChannel to the same VLAN, or configure them as . Ports with different native VLANs cannot form an EtherChannel
  - An EtherChannel supports the same allowed range of VLANs on all the ports in a trunking Layer 2 EtherChannel. If the allowed range of VLANs is not the same, the ports do not form an EtherChannel even when PAgP is set to the auto or desirable mode.

Related Topics

- Creating, Editing and Deleting an EtherChannel, page 73-5
- EtherChannel Reference, page 73-7

Creating, Editing and Deleting an EtherChannel

Procedure

Use this procedure to create, edit, and delete an EtherChannel.

Step 1 Choose **Configure > Switching > Ports > EtherChannel**. The EtherChannel Summary Page opens. See EtherChannel Summary Page, page 73-7.

Step 2 To create a EtherChannel, do the following:

a. Click **Create**. The Create EtherChannel window opens. See Create or Edit EtherChannel Dialog Box, page 73-9, page 73-8 for more information.

b. Enter the number in the EtherChannel Number filed in the range between 1 to 48. See Create or Edit EtherChannel Dialog Box, page 73-9, page 73-8 for more information.

c. Choose **Layer 2**, to have the EtherChannel and all the ports in this layer configured as Layer 2 EtherChannel.

d. Choose **Layer 3**, to have the EtherChannel and all the ports in this layer configured as Layer 3 EtherChannel.

e. Select the type of mode from the **Mode** drop-down menu for the selected port. See Create or Edit EtherChannel Dialog Box, page 73-9, page 73-8 for more information.

f. Click the **Priority cells** for the selected ports, and enter a PAgP or LACP priority.

g. Click **OK**. The Deliver Configuration to Device dialog box opens.

h. Click **Deliver** in the Deliver dialog box to deliver the configuration changes to the device.

Step 3 To edit an EtherChannel, do the following:

a. Select the EtherChannel from the EtherChannel Summary Page and then click **Edit**.

b. Enter the number in the EtherChannel Number filed in the range from 1 to 48. See Create or Edit EtherChannel Dialog Box, page 73-9, page 73-8 for more information.

c. Choose **Layer 2**, to have the EtherChannel and all the ports in this layer configured as Layer 2 EtherChannel.

d. Choose **Layer 3**, to have the EtherChannel and all the ports in this layer configured as Layer 3 EtherChannel.

e. Select the type of mode from the drop-down menu. See Create or Edit EtherChannel Dialog Box, page 73-9, page 73-8 for more information.

f. Click the **Priority cells** for the selected ports, and enter a PAgP or LACP priority.

g. Click **OK**. The Deliver Configuration to Device dialog box opens.

h. Click **Deliver** in the Deliver dialog box to deliver the configuration changes to the device.

Step 4 To delete an EtherChannel, do the following:

a. Choose the EtherChannel to delete, and click **Delete**. A confirmation dialog box opens.

b. Click **Yes** in the confirmation dialog box.

Related Topics

- EtherChannel Reference, page 73-7
- Configuring EtherChannel, page 73-4

EtherChannel Reference

This section describes the pages and dialog boxes that you can use when working with EtherChannel and includes the following topics:

- EtherChannel Summary Page, page 73-7
- Create or Edit EtherChannel Dialog Box, page 73-9, page 73-8

EtherChannel Summary Page

Use this page to create new EtherChannel, or to modify the parameters of the existing EtherChannels, and to delete an EtherChannel using Cisco CP.

How to Get to This Page

Choose **Configure > Switching > Ports > EtherChannel**.

Related Topics

- Create or Edit EtherChannel Dialog Box, page 73-9, page 73-8
- EtherChannel Overview, page 73-1
- Configuring EtherChannel, page 73-4

Load Balance

Choose an appropriate option from the Load Balance drop-down menu. See Load Balancing and Forwarding Methods, page 73-2 for more information.

- **Source MAC address—**Load distribution is based on the source-MAC address of the incoming packet.
- **Destination MAC address—**Load distribution is based on the destination-host MAC address of the incoming packet.
- **Source-Destination MAC address—**Load distribution is based on the source-and-destination host-MAC address.

- **Source IP address—**Load distribution is based on the source-host IP address.
- **Destination IP address—**Load distribution is based on the destination-host IP address.
- **Source-Destination IP address—**Load distribution is based on the source-and-destination host-IP address.

Field Reference

Table 73-1 Cisco CP —EtherChannel window

Elements	Description
Group	Displays the number assigned to the port group.
Ports	Displays the ports that belong to the EtherChannel.
Status	Displays the status of the EtherChannel: • Connected • Not connected
Create button	Click this button to creates a port group.
Edit button	Click this button to edits or modify the parameters an existing EtherChannel.
Delete button	Click this button delete the port group.

Related Topic

- Create or Edit EtherChannel Dialog Box, page 73-9

Create or Edit EtherChannel Dialog Box

You can choose the **Create** button to assign ports, set mode, and assign priority to a new group.You can Use the **Edit** button to modify the existing configuration of the selected EtherChannel.

How to Get to This Page

Choose **Configure > Switching > Ports > EtherChannel > Create**.

Choose **Configure > Switching > Ports > EtherChannel > Edit**.

Related Topics

- EtherChannel Summary Page, page 73-7
- EtherChannel Overview, page 73-1
- Configuring EtherChannel, page 73-4

Field Reference

Table 73-2 Create or Edit EtherChannel Dialog box

Elements	Description
EtherChannel number	Enter the Port Group number to assign the EtherChannel into it. **EtherChannel Number—**Enter the number for the port group. The range is from 1 to 48. • **Layer 2—** EtherChannel and all the ports in this layer are configured as Layer 2 EtherChannel. • **Layer 3—**EtherChannel and all the ports in this layer are configured as Layer 3 EtherChannel.
Ports	Enter the following parameters to the EtherChannel. • **Select Port—**Displays the number of ports in the device that are not associated (free ports) with any EtherChannel. Displays the free ports, along with the associated ports, to a particular EtherChannel in case of an **Edit** window. • **Status—**Displays the runtime status of the port. • **Mode—**Choose one of the following options from the drop-down menu: – **On**—The port does not use PAgP or LACP. A usable EtherChannel only exists if the port group is connected to another group in this mode. – **Auto—**The port responds to the PAgP packets it receives but does not initiate PAgP negotiations. This mode minimizes PAgP transmissions. This is the default option. – **Auto (Non-silent)—**The same as Auto but without support for connections to file servers or packet analyzers. – **Desirable—**The port initiates negotiations with other ports by sending PAgP packets.

Table 73-2 Create or Edit EtherChannel Dialog box (continued)

Elements	Description
	– **Desirable (Non-silent)—**The same as Desirable but without support for connections to file servers or packet analyzers. – **LACP**—The port can form a link aggregate and initiate the channel. The aggregate is formed if the other end is running LACP in LACP or LACP (Passive) mode. LACP mode is similar to the PAgP mode of Desirable. – **LAPC (Passive)**—The port can understand LACP packets but does not initiate the channel. It replies to a received LACP packet to form the channel if the other end is in LACP mode. LACP (Passive) mode is similar to the PAgP mode of Auto.
Priority	Click the Priority cells for the selected ports, and enter a PAgP or LACP priority to avoid the default (128 for PAgP, 32768 for LACP). The port with the highest priority sends the packets.
OK button	Click this button to save the changes. The new port group appears in the EtherChannel window
Cancel button	Click this button to avoid saving the changes that you entered.

CHAPTER 74

Smartport

Smartport helps you to configure your network consistently and use its full potential. With smartports, you can reliably configure:

- Essential security
- Availability
- Quality of Service
- And manageability features of switches in Ethernet networks.

Smartport macros provide a convenient way to save and share common configurations. Smartport macros enables features and settings based on the location of a switch in the network and for mass configuration deployments across the network.

To configure individual ports or entire devices, apply a command that generates a predefined set of commands called Roles.

Note You cannot apply smartports to routed ports and ether channel ports. This feature is supported only on Cisco 2520 series switches.

Use the port setup and device setup features to apply roles to a port or device.

Related Topics

- Port Setup, page 74-2
- Device Setup, page 74-7

Port Setup

The smartport feature is applied to any interface on the switch, except the routed ports. Roles are applied to the ports that do not have device connections or edit the existing Role.

For more information on configuring a smart port, see:

http://www.cisco.com/en/US/docs/switches/connectedgrid/cgs2520/software/release/12_2_53_ex/configuration/guide/swsmart.html

Related Topics

- Apply or Edit the Role for an interface, page 74-2
- Port Setup Reference, page 74-3

Apply or Edit the Role for an interface

Procedure

Use this procedure to apply or edit the roles for an interface.

Step 1 Choose **Configure > Switching > Ports > Smartport > Port Setup**. See Port Setup Reference, page 74-3.

Step 2 Select the interface from the Port Setup Summary page.

Step 3 Click **Edit**. The Edit SmartPort window opens. The selected interface name is displayed in the **Interface** field.

Note You can select multiple interfaces to edit the parameters. When you select multiple interfaces, the Edit Smartport dialog box does not display the **Interface** field.

Step 4 Select the type of Role from the drop-down menu to apply for the selected interface.

a. If you select Desktop or Substation HMI as the port Role, select the **Active VLAN** from the drop-down menu.

Note The list of VLANs are the VLANs defined in Cisco CP.

b. If you select Switch, Router, AccessPoint, Substation Switch, Substation Router, Substation AccessPoint,or Substation IED as the port Role, you need to select the **Native VLAN** from the drop-down menu.

c. If you select Diagnostics as the port Role, enter the Attribute like **Source Port** and **Ingress VLAN** from the drop-down menu.

Step 5 After you have applied Roles and Attributes, click **OK**. The Deliver Configure to Device dialog box opens.

Step 6 Click **Deliver** in the Deliver dialog box to deliver the configuration changes to the device.

Related Topic

- Port Setup Reference, page 74-3

Port Setup Reference

This section describes the summary page and dialog boxes that you can use when working with Port Setup and includes following topics:

- Port Setup Summary Page, page 74-3
- Edit Port Setup Dialog Box, page 74-4

Port Setup Summary Page

Use this page to view all the interface and modify the roles for the selected interface using Cisco CP.

How to Get into This Page

Choose **Configure > Switching > Ports > Smartport > Port Setup**.

Related Topics

- Edit Port Setup Dialog Box, page 74-4

- Apply or Edit the Role for an interface, page 74-2

Field Reference

Table 74-1 Cisco CP—Port Setup Summary Page

Elements	Description
Interface	Displays all the interface or port in the switch, except the routed port. When you select multiple interfaces, the Edit Smartport dialog box does not display the **Interface** field.
Role	Displays the Role that is applied to the interfaces.
Edit button	Click this button to edits the Role applied to the interface.

Edit Port Setup Dialog Box

The edit Port Setup window allows you to edit smartport role or to apply smartport role to a interface that do not have any smartport configured.

How to Get to This Page

1. Choose **Configure > Switching > Ports > Smartport > Port Setup**.
2. Click **Edit**.

Related Topics

- Port Setup Summary Page, page 74-3
- Apply or Edit the Role for an interface, page 74-2

Field Reference

Table 74-2 Edit Port Setup Dialog box

Elements	Description
Interface	Displays the name of the selected interface. When you select multiple interfaces, the Edit Smartport dialog box does not display the **Interface** field.
Role	Select one of the following option from the drop-down menu: • **Desktop**—Internal end host, with access to the Internet. It connects to the internal subnets of an organization. – Select the VLAN number from the Access VLAN ID drop-down menu. **Note** There can be only one interface to which a Desktop role can be applied. Also, the source port lists all the ports except for the port that is being configured with desktop role. • **Switch**—Switch-to-switch connection. – Select the native VLAN number from the Native VLAN drop-down menu. • **Router**—Layer-3 switch with routing capability connection. – Select the native VLAN number from the Native VLAN drop-down menu. • **AccessPoint**—Connects to mobile end hosts. Depending on the access-point setup, the mobile end hosts can be either guest or desktop end hosts. – Select the native VLAN number from the Native VLAN drop-down menu. • **Diagnostics**—Connects to a network analyzer, monitoring device, or security device. – Select the interface from the **SourcePort** drop-down menu. – Select the Ingress VLAN number from the Ingress VLAN drop-down menu.

Table 74-2 Edit Port Setup Dialog box (continued)

Elements	Description
	• **Substation Switch**—This interface configuration macro can be used when connecting a ring of switches. This macro is optimized for utility deployments. – Select the native VLAN number from the Native VLAN drop-down menu. • **Substation Router**—This interface configuration macro can be used when connecting the switch and a WAN router. This macro is optimized for utility deployments. – Select the native VLAN number from the Native VLAN drop-down menu. • **Substation Accesspoint**—This interface configuration macro can be used when connecting the switch and a wireless access point. This macro is optimized for utility deployments. – Select the native VLAN number from the Native VLAN drop-down menu. • **Substation HMI**—This interface configuration macro can be used for increased network security and reliability when connecting a desktop device, such as a PC, or a switch port. This macro is optimized for utility deployments – Select the VLAN number from the Access VLAN ID drop-down menu. • **Substation IED**—This interface configuration macro can be used when connecting the switch to an IED. – Select the native VLAN number from the Native VLAN drop-down menu. **Note** The cisco-cg-ied macro works properly only if the cisco-cg-global macro is applied.
OK button	Click this button to save the changes.
Cancel button	Click this button to avoid saving the changes that you entered.

Device Setup

Use Device Setup feature to apply the global role by configuring essential networking features on a device.

Related Topic

- Device Setup Summary Page, page 74-8

How to Apply or Remove the Device role

Procedure

Use this procedure to apply or remove the device role to the selected device.

Step 1 Choose **Configure > Switching > Ports > Smartport > Device Setup**. The Device Setup Summary Page, page 74-8 opens.

Step 2 To apply the device role, do the following:

a. Check the cisco-cg-global check box to apply the global role to the selected device.

b. Click **Apply**. The Deliver Configure to Device dialog box opens.

c. Click **Deliver** in the Deliver dialog box to deliver the configuration changes to the device.

Step 3 To remove the device role, do the following:

a. Uncheck the cisco-cg-global check box to remove the global role of the selected device.

b. Click **Apply**. The Deliver Configure to Device dialog box opens.

c. Click **Deliver** in the Deliver dialog box to deliver the configuration changes to the device.

Related Topic

- Device Setup Reference, page 74-8

Device Setup Reference

This section describes the summary page that you can use when working with device setup and includes the following topic:

- Device Setup Summary Page, page 74-8

Device Setup Summary Page

Use this page to apply the global role on the device.

How to Get into This Page

Choose **Configure > Switching > Ports > Smartport > Device Setup**.

Field Reference

Table 74-3 Cisco CP - Device Setup

Elements	Description
cisco-cg-global	Check this box to apply the global role on the selected device, otherwise uncheck the check box to remove the global role.
Apply button	Applies the changes.

CHAPTER 75

VLAN Settings

A VLAN is a switched network; segmented by a function, project team, or application; irrespective of the physical location of the device. Create, edit, or delete a VLAN, using Cisco CP.

Note The HWIC and NM modules related screens are available at **Configure > Interface Management > Ports > Port**. The SM and NME modules related screens are available at **Configure > Switching Module > Ports > Port**.

Related Topics

- Configure VLANs, page 75-1
- Configure Port, page 75-9

Configure VLANs

A VLAN is an administratively defined broadcast domain, logically segmented by function, team, or application. It enhances performance by limiting traffic to stations in the same VLAN and blocks the traffic from other VLANs.

VLANs have the same attributes as physical LANs, but you can group end stations even if they are not physically located on the same LAN segment. Any switch port can belong to a VLAN, and unicast, broadcast, and multicast packets are forwarded and flooded only to end stations in the VLAN.

Assigning Static-Access Ports to VLANs

By default, all ports are static-access ports assigned to VLAN 1. To change the VLAN ID, you must use ID from 1 to 1001 or from 1006 to 4094.

Note VLAN IDs from 1002 to 1005 are reserved.

Static-access ports cannot be assigned to multiple VLANs. Therefore, you can move a port connection from one switch to another and configure the port as a trunk port to avoid reconfiguring it.

Note Before you assign ports to a VLAN, you must first create the VLAN, and determine whether to use VLAN Trunking Protocol.

Configuring a Trunk Port

A trunk is a point-to-point link between two switches. carry the traffic of multiple VLANs and extend VLANs from one switch to another.

You can configure the port as an IEEE 802.1Q trunk port. On an 802.1Q trunk port, the switch receives both untagged traffic and traffic containing 802.1Q tags.

Follow these guidelines when configuring a trunk port:

- Do not configure a trunk port as a secure port or a monitor port.
- Assign a static-access port to monitor a VLAN on a trunk port. The VLAN monitored is the one associated with the static-access port.
- If you configure a trunk port as a network port, the trunk port becomes the network port for all the VLANs associated with the port.
- Do not configure one end of the trunk as an 802.1Q trunk and the other end as an nontrunk port.

Set the following parameters when creating a VLAN or edit existing a VLAN in the VLAN database:

- VLAN ID
- VLAN name
- VLAN type
- UNI-ENI VLAN configuration.

Related Topics

- Creating, Editing, and Deleting a VLAN, page 75-4
- VLAN Reference, page 75-6

VLAN Configuration Guidelines

Use these guidelines while creating or modifying a VLAN:

- The switch supports 4094 VLANs.
- Normal-range Ethernet VLANs are identified with a number between 1 and 1001.
- VLAN numbers 1002 through 1005 are reserved for Token Ring.
- VLAN configurations for VLANs 1 to 1005 are always saved in the VLAN database.
- Configuration options for VLAN IDs 1006 through 4094 are limited to private VLAN and UNI-ENI VLAN.

Related Topics

- Configure VLANs, page 75-1
- VLAN Reference, page 75-6

Creating, Editing, and Deleting a VLAN

Procedure

Use this procedure to create a new VLAN, modify the parameters of the existing VLAN, and delete the selected VLAN.

Step 1 Choose **Configure > Switching Module > Ports > VLAN Settings > Configure VLAN** or **Configure > Interface Management > Ports > VLAN Settings > Configure VLAN** or **Configure > Switching > Ports > VLAN Settings > Configure VLAN**.

The VLAN settings page opens. See Configure VLAN Summary Page, page 75-6 for more information.

Step 2 To create a VLAN, do the following:

a. Click **Create**. The Create VLAN dialog box opens. See Create or Edit VLAN Dialog Box, page 75-7 for more information.

b. Enter the VLAN ID in the range from 1 to 4094. See Create or Edit VLAN Dialog Box, page 75-7 for more information.

c. Enter the name for the VLAN.

d. Choose **Isolated VLAN** type from the UNI-ENI type drop-down menu, so that the local switching is not allowed among UNIs or ENIs on the switch that belong to the same UNI-ENI isolated VLAN. See Create or Edit VLAN Dialog Box, page 75-7 for more information.

Note By default, the UNI-ENI Type is selected to Isolated VLAN.

e. Choose **Community VLAN** type from the UNI-ENI type drop-down menu to allow local switching among UNIs and ENIs on the switch that belongs to the same community VLAN. See Create or Edit VLAN Dialog Box, page 75-7 for more information.

f. Click **OK**. The Deliver to Configuration dialog box opens.

g. Click **Deliver** in the Deliver dialog box to save the configuration to the device.

Step 3 To edit a VLAN, do the following:

a. Select the VLAN from the VLAN Setting summary page, and click **Edit**. The Edit VLAN dialog box opens with the same fields as the Create VLAN window. However, the VLAN Name field displays either the default name or the name of the VLAN. You can edit the name of the selected VLAN. See Create or Edit VLAN Dialog Box, page 75-7 for more information.

b. Choose **Isolated VLAN** type from the UNI-ENI type drop-down menu so that the local switching is not allowed among UNIs or ENIs on the switch that belong to the same UNI-ENI isolated VLAN. Otherwise choose **Community VLAN**. See Configure VLAN Summary Page, page 75-6 for more information.

c. Click **OK**. The Deliver to Configuration dialog box opens.

d. Click **Deliver** in the Deliver dialog box to save the configuration to the device.

Step 4 To delete a VLAN, do the following:

a. Select the VLAN from the VLAN Setting Page that you want to delete.

b. Click **Delete**. A Confirmation dialog box opens.

c. Click **Yes** in the Confirmation dialog box.

Related Topic

- VLAN Reference, page 75-6

VLAN Reference

This section describes the pages and dialog boxes you can use when working with Configure VLAN, and includes the following topics:

- Configure VLAN Summary Page, page 75-6
- Create or Edit VLAN Dialog Box, page 75-7

Configure VLAN Summary Page

Use this page to view information about the VLANs configured on the device. Create, edit, and delete using Cisco CP.

How to Get to This Page

Configure > Switching Module > Ports > VLAN Settings > Configure VLAN or **Configure > Interface Management > Ports > VLAN Settings > Configure VLAN** or **Configure > Switching > Ports > VLAN Settings > Configure VLAN**.

Related Topic

- Create or Edit VLAN Dialog Box, page 75-7

Field Reference

Table 75-1 Cisco CP —Configure VLAN Summary Page

Elements	Description
VLAN ID	Displays the VLAN IDs.
Name	Displays the VLAN names.
Status	Displays the status of the device. This field is read-only. Following are the VLAN status: • Active • Suspended

Table 75-1 Cisco CP —Configure VLAN Summary Page (continued)

Elements	Description
UNI-ENI Type	Displays the one of the following UNI-ENI types. See Create or Edit VLAN Dialog Box, page 75-7 for more information. • Isolated • Community
Create button	Creates a VLAN.
Edit button	Click this button to edit the configuration of selected VLAN.
Delete button	Click this button to delete the selected VLAN.

Create or Edit VLAN Dialog Box

Use this window to create and edit VLAN settings, using Cisco CP.

How to Get to This Page

Choose **Configure > Switching Module > Ports > VLAN Settings > Create** or **Configure > Interface Management > Ports > VLAN Settings > Configure VLAN > Create** or **Configure > Switching > Ports > VLAN Settings > Create**.

Choose **Configure > Switching Module > Ports > VLAN Settings > Edit** or **Configure > Interface Management > Ports > VLAN Settings > Configure VLAN > Edit** or **Configure > Switching Module > Ports > VLAN Settings > Edit**.

Related Topic

- Configure VLAN Summary Page, page 75-6

Field Reference

Table 75-2 VLAN Create or Edit Dialog box

Element	Description
VLAN ID	Displays the VLAN ID. Enter a value from 1 to 4094. **Note** VLAN IDs 1 and from 1002 to 1005 are reserved and cannot be modified.
Name	Displays the name of the VLAN. Enter a VLAN name from 1 to 32 characters. The name must be unique within the administrative domain. The default name is VLANxxxx where xxxx represents four digits (including leading zeros) equal to the VLAN ID number.
UNI-ENI Type	Allows two types of UNI-ENI VLANs: • **Isolated VLAN**—Local switching is not allowed among UNIs or ENIs on the switch that belongs to the same UNI-ENI isolated VLAN. This is the default VLAN state for all VLANs created on the switch. • **Community VLAN**—Local switching is allowed among UNIs and ENIs on the switch that belongs to the same community VLAN. The switch supports a combination of only eight UNIs and ENIs in a UNI-ENI community VLAN. **Note** Tunnel is not applicable for the HWIC and NM modules.
OK button	Click this button to save the changes.
Cancel button	Click this button to avoid saving the changes that you entered.

Configure Port

The switch ports are used for managing the physical interface, are associated Layer 2 protocols, and do not handle routing or bridging. The switch ports are Layer 2 interfaces associated with a physical port. Switch ports belong to one or more VLAN. A switch port can be an access port, a trunk port, or a tunnel port. You can configure a port as an access port, trunk port, or a private VLAN port as a host.

Access Ports

An access port belongs to, and carries the traffic of, only one VLAN. The traffic is received and sent in native formats with no VLAN tagging. Traffic arriving on an access port is assumed to belong to the VLAN assigned to the port. If an access port receives an IEEE 802.1Q tagged packet, the packet is dropped, and the source address is not learned. IEEE 802.1x can also be used for VLAN assignment.

The access port supports static access port that are manually assigned to a VLAN.

Trunk Ports

An IEEE 802.1Q trunk port carries the traffic of multiple VLANs and by default is a member of all VLANs in the VLAN database. A trunk port supports simultaneous tagged and untagged traffic. An IEEE 802.1Q trunk port is assigned to default Port VLAN ID (PVID), and all untagged traffic travels on the port default PVID.

All possible VLANs (VLAN ID from 1 to 4094) are part of the allowed list, by default. A trunk port can become a member of a VLAN only if the VLAN is in the enabled state.

Tunnel Ports

Tunnel ports are used in IEEE 802.1Q tunneling to segregate the traffic between service-provider networks and unknown networks using the same VLAN number. On configuring an asymmetric link from a tunnel port on a service-provider edge switch to an IEEE 802.1Q trunk port on the users network. Packets entering the tunnel port on the edge switch and user VLANs that is already tagged to IEEE 802.1Q, are encapsulated with another layer of an IEEE 802.1Q tag (called the metro tag), containing a VLAN ID unique in the service-provider network, for each user. The double-tagged packets go through the service-provider network, keeping the original user VLANs separate from those of other user. At the outbound interface, also a tunnel port, the metro tag is removed and the original VLAN numbers from the user network are retrieved.

Routed Ports

A routed port is a physical port that acts like a port on a router but does not have to be connected to a router. A routed port is not associated with a particular VLAN because it is an access port. A routed port behaves like a regular router interface, except that it does not support VLAN sub interfaces. Routed ports can be configured with a Layer 3 routing protocol. A routed port is Layer 3 interface and does not support Layer 2 protocols, such as STP.

Related Topics

- How to Edit a Port Mode, page 75-11
- Port Reference, page 75-12

How to Edit a Port Mode

Procedure

Use this procedure to edit the parameters of the selected port.

Step 1 Choose **Configure > Switching Module > Ports > VLAN Settings > Configure Port** or **Configure > Interface Management > Ports > VLAN Settings > Configure Port** or **Configure > Switching Module > Ports > VLAN Settings > Configure Port**.

The Configure Port Summary Page, page 75-12 opens.

Step 2 Select the interface to edit the parameters, and then click **Edit**. The Edit Port Mode dialog box opens with parameters such as: Port Type, Administrative Mode, operating Mode, Administrative Encapsulation, Operating Encapsulation, Static Access VLAN, Trunk Allowed VLAN, and Native VLAN. See Edit Port Mode Dialog Box, page 75-14 for more information.

Step 3 The **Port** field displays the name of the selected interface.

Note You can select multiple ports to edit the parameters. When you select multiple ports, the Edit Port Mode dialog box does not display the Port, operating Mode, Administrative Encapsulation, and Operating Encapsulation fields to edit.

Step 4 Select the port type from the drop-down menu that best suits the selected interface. See Edit Port Mode Dialog Box, page 75-14 for more information.

Step 5 Select the type of administrative mode from the drop-down menu. See Edit Port Mode Dialog Box, page 75-14 for more information.

Step 6 If Static Access is selected as the administrative mode, do the following:

a. Choose the existing VLAN ID from the **Static Access VLAN** drop-down menu to assign the port. The range is from 1 to 4094.

Note By default, the Native VLAN ID for Static Access and Tunnel is 1.

Step 7 If Trunk 802.1Q is selected as the administrative mode, do the following:

a. In the Trunk Allowed VLANs field, enter the numbers of the allowed VLANs in a range from 1 to 4094 or enter **ALL** to select all the VLANs.

b. Select the existing VLAN ID as the native VLAN from the **Native VLAN** the drop-down menu.

Step 8 If Tunnel is selected as the administrative mode, do the following:

a. Choose the existing VLAN ID from the **Static Access VLAN** drop-down menu to assign the port. The range is from 1 to 4094.

Step 9 Select Routed from the **Administrative Mode** drop-down menu.

Step 10 Click **OK**. The Deliver to Configuration dialog box opens.

Step 11 Click **Deliver** in the Deliver dialog box to save the configuration to the device.

Related Topic

- Port Reference, page 75-12

Port Reference

This section describes the summary pages and dialog boxes you can use when working with configure port and includes the following topics:

- Configure Port Summary Page, page 75-12
- Edit Port Mode Dialog Box, page 75-14

Configure Port Summary Page

Use this page to view, and edit the information about assigning the VLAN to the Port, using Cisco CP.

How to Get to This Page

Choose **Configure > Switching Module > Ports > VLAN Setting > Configure Port** or Choose **Configure > Interface Management > Ports > VLAN Settings > Configure Port** or **Configure > Switching > Ports > VLAN Setting > Configure Port**.

Related Topic

- Edit Port Mode Dialog Box, page 75-14

Field Reference

Table 75-3 Cisco CP —Configure Ports Summary Page

Elements	Description
Interface	Identifies the port: Fast Ethernet, Gigabit Ethernet, the module or slot number (0, 1, or 2), and the port number.
EtherChannel number	Displays the EtherChannel number.
Administrative mode	Displays the mode to which the port is set. Displays one the following: • Static Access • Trunk 802.1 Q • Tunnel • Routed
Operational mode	Displays the mode in which the port is operating. Displays one of the following: • Down • Trunk • Static
VLANs	Displays the VLAN number to which the port is assigned, or if its a trunk port, the VLANs that can use the trunk.
Port-Type	Displays the type VLAN. Displays one of the following: • UNI • ENI • NNI
Edit button	Edits the parameters of the selected interface. When you select multiple ports, the Edit Port Mode dialog box does not display the Port, operating Mode, Administrative Encapsulation, and Operating Encapsulation fields to edit.

Edit Port Mode Dialog Box

Use this dialog box to modify the parameters of the selected interface.

How to Get to This Page

1. Choose **Configure > Switching Module > Ports > VLAN Settings > Configure Port** or **Configure > Interface Management > Ports > VLAN Settings > Configure Port**.
2. Click **Edit**.

Related Topic

- Configure Port Summary Page, page 75-12

Field Reference

Table 75-4 Edit Port Mode Dialog Box

Element	Description
Port	Displays the type of the selected port. When you select multiple ports, the Edit Port Mode dialog box does not display the Port, operating Mode, Administrative Encapsulation, and Operating Encapsulation fields to edit
Port type	Choose one of the following port type from the drop-down menu: • **UNI**—Typically connected to a host, and are configured to support hosts like a PC or a Cisco IP phone. • **NNI**—Typically connected to a router, or to another switch. • **ENI**—Contains the same functionality as UNIs, but can be configured to support protocol control packets for Cisco Discovery Protocol (CDP), Spanning-Tree Protocol (STP), Link Layer Discovery Protocol (LLDP), and Ether Channel Link Aggregation Control Protocol (LACP) or Port Aggregation Protocol (PAgP). **Note** Tunnel is not applicable for the HWIC and NM modules.

Table 75-4 Edit Port Mode Dialog Box (continued)

Element	Description
Administrative mode	Choose one of the following administrative modes from the drop-down menu. See Configure Port, page 75-9 for more information. • Static Access • 802.1Q Trunk • Tunnel **Note** Tunnel is not applicable for the HWIC and NM modules. • Routed
Operating mode	Displays one of the following modes: • **Down**—Displays when the interface is not connected, improper cabling, or administratively not enabled. • **Trunk**—Displays when the port is configured as trunk. • **Static**—Displays the default behavior of the port, which is static access.
Administrative encapsulation	Displays the administrative mode and administrative encapsulation as read-only information.
Operating encapsulation	Displays the operating mode and operating encapsulation as read-only information.
Static access VLAN	If **Static Access** is selected as the administrative mode, you must assign the ports to a VLAN. Choose the existing VLAN ID from the **Static Access VLAN** drop-down menu to assign the port.
Trunk allowed VLANs	If **Trunk 802.1Q** is selected as the administrative mode, you can restrict the VLAN membership for the trunk ports by specifying which VLANs are allowed to use them, and the port forwards traffic only for these VLANs. Enter the numbers of the existing VLANs. The range is from 1 to 4094. You can also choose **All**.

Table 75-4 Edit Port Mode Dialog Box (continued)

Element	Description
Native VLAN	By default, the native VLAN is VLAN 1. To assign another VLAN to be the native VLAN, select a different VLAN ID from the Native VLAN list.
OK button	Click this button to save the changes.
Cancel button	Click this button if you do not want to save the changes that you entered.

CHAPTER 76

PoE

The Cisco Power Over Ethernet (PoE) feature allows you to automatically obtain the power supply to the connected devices.

The following sections provide more information:

- Understanding PoE, page 76-1
- Configuring PoE, page 76-3
- Power Management Modes, page 76-2
- Managing PoE, page 76-4

Understanding PoE

PoE-capable switch ports supply power to the following connected devices when the switch senses that there is no power on the circuit:

- Cisco prestandard powered devices such as Cisco IP Phones and Cisco Aironet access points
- 802.3af-compliant powered devices

A powered device can receive redundant power when it is connected only to a PoE switch port and to an AC power source.

After the switch detects a powered device, it determines the device power requirements and then grants or denies power to the device.

Note This feature is only supported on Cisco GS-2520-16S-8PC series devices. Devices that support PoE will also support the power policing feature.

Supported Protocols and Standards

The switch uses these protocols and standards to support PoE:

- Cisco Discovery Protocol (CDP) with power consumption—The powered device notifies the switch of the amount of power it consumes. The switch does not reply to the power-consumption messages. The switch can only supply power to or remove power from the PoE port.
- Cisco intelligent power management—The powered device and the switch negotiate through the power-negotiation CDP messages for an agreed power-consumption level. The negotiation allows a high-power device, which consumes more than 7 W to operate at its highest power mode. The powered device first boots up in low-power mode, consumes less than 7 W, and negotiates to obtain enough power to operate in high-power mode. The device changes to high-power mode only when it receives confirmation from the switch.
- IEEE 802.3af—The major features of this standard are powered-device discovery, power administration, disconnect detection, and optional powered-device power classification. For more information, see the IEEE standard.

Power Management Modes

The switch supports these PoE modes:

- Auto—The switch automatically detects if the connected device requires power. If the switch discovers a powered device connected to the port and if the switch has enough power, it grants power, updates the power budget, turns on power to the port on a first-come first-served basis, and updates the LEDs. If enough power is available for all the powered devices connected to the switch, power is turned on to all the devices. If there is not enough available PoE, or if a device is disconnected and reconnected while other devices are

waiting for power, it cannot be determined which devices are granted or are denied power. You can specify the maximum wattage that is allowed on the port.

- Static—The switch pre-allocates power to the port (even when no powered device is connected) and guarantees that the power will be available for the port. The switch allocates the port configured maximum wattage, and the amount is never adjusted through the IEEE class or by CDP messages from the powered device. Because power is pre-allocated, any powered device that uses less than or equal to the maximum wattage is guaranteed to be powered when it is connected to the static port. The port no longer participates in the first-come first-served model.
- Never—The switch disables powered-device detection and never powers the PoE port even if an unpowered device is connected. Use this mode only when you want to make sure power is never applied to a PoE-capable port, making the port a data-only port.

Related Topics

- Configuring PoE, page 76-3
- Managing PoE, page 76-4
- PoE Reference, page 76-4

Configuring PoE

For most situations, the default configuration (Auto mode) works well, providing plug-and-play operation. No further configuration is required. However, use the following procedure to give a PoE port higher priority, to make it data only, or to specify a maximum wattage to disallow high-power powered devices on a port.

Note Devices that support PoE will also support the power policing feature.

IRelated Topics

- Managing PoE, page 76-4
- PoE Summary Page, page 76-5

Managing PoE

Procedure

Use this procedure to view and edit the PoE for the selected port.

Step 1 Choose **Configure > Switching > PoE**. The PoE Summary page opens. See PoE Summary Page, page 76-5.

Step 2 To edit the PoE, do the following:

a. Select the interface from the PoE Summary page, and click **Edit**. The Edit PoE dialog box opens.

b. In the Edit PoE window, choose the modes from the Modes drop-down list.

c. Enter the maximum power in watts. The range is 4 to 20 W. The default value is 15.4 W. The extended PoE allows the switch to allocate more power than 15.4 W and limits the power to 20 W.

d. Choose the priority from the Priority drop-down list.

e. Click **OK** to apply the changes to the configuration.

f. Click **Deliver** in the Deliver dialog box to deliver the configuration changes to the device.

Related Topics

- PoE Reference, page 76-4

PoE Reference

This section describes the pages and windows that you can use when working with configuring PoE and includes the following topics:

- PoE Summary Page, page 76-5
- Edit PoE Dialog Box, page 76-5

PoE Summary Page

Use the PoE Summary page to view the PoE for the selected port.

How to Get to This Page

Choose **Configure > Switching > PoE**.

Related Topic

- Managing PoE, page 76-4

Field Reference

Table 76-1 PoE Summary Page

Elements	Description
Interface	Displays the physical port.
Mode	Displays the mode for the port. The modes are: Auto, Static, and Never.
Device power (Watts)	Displays the device power.
Powered device	Displays the powered device.
Max power (Watts)	Displays the power allowed on the port. The range is 4 to 20 W. The default value is 15.4 W.
Priority	Displays the priority.
Extended max power (Watts)	Displays the extended maximum power allowed on the port. The range is 15.4 to 20 W. The default value is 15.4 W. The extended PoE allows the switch to allocate power more than 15.4 W and limits it to 20 W.
Edit button	Edits the PoE.

Edit PoE Dialog Box

Use the Edit PoE dialog box to edit the PoE.

How to Get to This Dial Box

1. Choose **Configure > Switching > PoE.**
2. Click the **Edit** button.

Related Topics

- PoE Summary Page, page 76-5

Field Reference

Table 76-2 Edit PoE Dialog Box

Element	Description
Interface	Displays the selected physical port.
Mode	Allows you to choose the mode for the port from the drop-down list. The modes are: • Auto—Enables powered-device detection. If enough power is available, automatically allocates power to the PoE port after device detection. This is the default setting. • Static—Enables powered-device detection. Pre-allocates (reserve) power for a port before the switch discovers the powered device. The switch reserves power for this port even when no device is connected and guarantees the power. The switch allocates power to a port configured in static mode before it allocates power to a port configured in auto mode. • Never—Disables device detection, and disables power to the port.
Powered device	Displays the powered device.
Device power (Watts)	Displays the device power.
Priority	Allows you to choose the priority from the drop-down list. The priorities are: Low and High. By default, the priority is set to low when you select the mode as Auto.
Extended max power (Watts)	Limits the extended maximum power allowed on the port. The range is 15.4 to 20 W. The default value is 15.4 W. The extended PoE allows the switch to allocate power more than 15.4 W and limits it to 20 W.
Max power (Watts)	(Optional) Limits the power allowed on the port. The range is 4 to 20 W. The default is 15.4 W.

Table 76-2 Edit PoE Dialog Box

Element	Description
OK button	Click the **Ok** button to save the changes.
Cancel button	Click the **Cancel** button to avoid saving the changes that you entered.

CHAPTER 77

Device Alarm

The Device Alarm window is used to configure primary or secondary alarm settings for switch temperature alarms, redundant power supply alarms, and port pinout alarms, using Cisco CP.

See the following topics for more information:

- Configuring System Alarms, page 77-2
- External Alarm Input, page 77-3.
- Power Supply Alarms, page 77-3.
- Device Alarm Reference, page 77-5

Configuring System Alarms

The Cisco CP Alarm feature allows you to configure alarm settings for interfaces or for the entire device. Alarms notify you when the traffic signal has failed or degraded, or when the equipment is not functioning.

On the Device Alarm window, you can configure temperature alarms and redundant power supply alarms. Primary temperature alarms are fixed and the maximum or minimum threshold values are set to default. Secondary temperature alarms are triggered when the switch temperature goes above a set threshold. If a switch has a second power supply, you need to enable the redundant-power-supply alarm, which is triggered when the secondary power supply is missing or not functioning.

For more information on Configuring Alarm, see:

http://www.cisco.com/en/US/docs/switches/connectedgrid/cgs2520/software/release/12_2_53_ex/configuration/guide/swalarms.html

Related Topics

- External Alarm Input, page 77-3
- Power Supply Alarms, page 77-3
- Applying Alarm Settings for the Device, page 77-4

External Alarm Input

You can connect up to four alarm inputs from external devices in your environment (such as a door, a temperature gauge, or a fire alarm) to the alarm input port on the switch front panel.

For each alarm input, you can configure an open or closed circuit to trigger an alarm and configure the severity of the alarm. A triggered alarm generates a system message. If you enter a descriptive name for the alarm, that name is displayed in the system message. A triggered alarm turns on the LED display. Alarms that are generated can be syslog messages or snmp traps based on the configuration on the device.

How to Get to This Page

Choose **Configure > Switching > Alarm > Device Alarm**.

Related Topics

- Power Supply Alarms, page 77-3
- Applying Alarm Settings for the Device, page 77-4

Power Supply Alarms

When the switch is operating with two power supplies, an alarm is triggered when one is missing or not functioning.

The default power supply configuration has one power supply installed in slot 1. This suppresses any alarms triggered by not having two power supplies installed.

Related Topics

- Configuring System Alarms, page 77-2
- External Alarm Input, page 77-3
- Applying Alarm Settings for the Device, page 77-4

Applying Alarm Settings for the Device

Procedure

Use this procedure to set the primary and secondary, redundant and port pinout alarms.

Step 1 Choose **Configure > Switching > Alarm > Device Alarm**. The Device Alarm page opens. See Device Alarm Summary Page, page 77-5.

Step 2 To configure the primary temperature alarm, do the following:

a. Enter or choose the threshold value between –200°C to 250°C from the **Threshold (Low)** field.

b. Enter or choose the threshold value between –150ºC to 300ºC from the **Threshold (High)** field.

Step 3 To configure the secondary temperature alarm, do the following:

a. Check the **Secondary Temperature** check box to enable the secondary temperature alarm.

a. Enter or choose the threshold (Low) value between –200ºC to 250ºC from the **Threshold (Low)** field.

b. Enter or choose the threshold value between –150ºC to 300ºC from the **Threshold (High)** field.

Step 4 To configure the power supply redundant, do one of the following:

a. Choose **Enable**, if you are using two power supplies so that an alarm is generated when the redundant (second) power supply is missing or not functioning.

b. Choose **Disable**, if you have a single power supply.

Step 5 To configure alarm input, do one of the following:

a. Select the **Enable Alarm Input** check boxes to set the alarm.

b. Enter a text in the **Description** field.

c. By default, the trigger is set to **Closed**. Click **Open**, to set the alarm if there is no flow of current.

d. Choose Minor, Major, or Critical from the **Severity** drop-down menu.

Note The previous procedure is applicable for the four alarm input displayed on the Device Alarm page. See Device Alarm Summary Page, page 77-5 for more information.

Step 6 To apply the alarm settings, do the following:

a. Click **Apply**. The Deliver Configuration to Device dialog box opens.

b. Click **Deliver** in the Deliver dialog box to apply the configuration changes to the device.

Device Alarm Reference

This section describes the summary page that you can use when working with device alarm and includes the following topic:

- Device Alarm Summary Page, page 77-5

Device Alarm Summary Page

Use this page to set the threshold value for temperature, redundant, and port pinout alarms.

How to Get to This Page

Choose **Configure > Switching > Alarm > Device Alarm**.

Related Topics

- Applying Alarm Settings for the Device, page 77-4
- External Alarm Input, page 77-3
- Power Supply Alarms, page 77-3

Field Reference

Table 77-1 Cisco CP - Device Alarm Summary Page

Element	Description
Temperature - Primary	Enter the value for the temperature primary fields. • **Threshold (Low)**—Enter or choose the minimum threshold temperature between –200ºC to 250ºC. • **Threshold (High)**—Enter or choose the maximum threshold temperature between –150ºC to 300ºC.
Temperature - Secondary	Select this check box to set the secondary threshold temperature value in the following field: • **Threshold (Low)**—Enter or choose the minimum threshold temperature between –200ºC to 250ºC. • **Threshold (High)**—Enter or choose the maximum threshold temperature between –150ºC to 300ºC.
Power supply redundant	Select one of the following options: • **Enable—**Enable this alarm if you are using two power supplies, this setting generates an alarm when the redundant (second) power supply is missing or not functioning. • **Disable**—Disable this alarm if you have a single power supply.

Table 77-1 Cisco CP - Device Alarm Summary Page (continued)

Element	Description
Alarm 1 Input / Alarm 2 Input / Alarm 3 Input / Alarm 4 Input	Select this check box to generate an alarm when more than one port is connected. • **Description**—Enter a description of the port. • **Trigger**—The alarm trigger setting is open or closed. – **Open**—The normal condition has current flowing through the contact (normally closed contact). The alarm is generated when the current stops flowing. – **Closed**—No current flows through the contact (normally open contact). The alarm is generated when current does flow. **Note** By default, the alarm trigger is set to Closed. • **Severity**—Choose the severity for the desired threshold from the drop-down menu: – Major – Minor – Critical **Note** These configuration settings are applicable for the four alarm input displayed on the Device Alarm page. For information on alarm input, see External Alarm Input, page 77-3.
Apply button	Click this button to apply the changes.

CHAPTER 78

ModBus

The Modicon Communication Bus (ModBus) feature allows you to communicate between a switch and a device in the network by using the ModBus client software.

The following sections provide more information:

- Understanding ModBus, page 78-1
- Configuring MODBUS, page 78-2

Understanding ModBus

ModBus is a serial communications protocol for client-server communication between a switch (server) and a device in the network running ModBus client software (client). You can use ModBus to connect a computer to a Remote Terminal Unit (RTU) in Supervisory Control and Data Acquisition (SCADA) systems.

ModBus Transmission Control Protocol (TCP) is used over an Ethernet network when connecting the switch to devices such as Intelligent Electronic Devices (IEDs), distributed controllers, substation routers, Cisco IP Phones, Cisco Wireless Access Points, and other network devices such as redundant substation switches.

The client can be an IED or a Human Machine Interface (HMI) application that remotely configures and manages devices running ModBus TCP. The switch functions as the server.

The switch encapsulates a request or response message in a ModBus TCP Application Data Unit (ADU). A client sends a message to a TCP port on the switch. The default port number is 502.

MODBUS and Security

If a firewall or other security services are enabled, the switch TCP port can be blocked, and the switch and the client cannot communicate. If a firewall and other security services are disabled, a denial-of-service attack can occur on the switch.

Multiple Request Messages

The switch can receive multiple request messages from clients and respond to them simultaneously.

You can set the number of client connections from one to five. The default is one.

Related Topics

- Configuring MODBUS, page 78-2
- ModBus Reference, page 78-3

Configuring MODBUS

By default, the switch is not configured as a ModBus TCP server and the TCP switch port number is set to 502. The number of simultaneous connection requests is set to one.

Procedure

Use this procedure to configure the switch as a ModBus server.

Step 1 Choose **Configure > Switching > ModBus**. The ModBus configuration dialog box opens. See ModBus Dialog Box, page 78-3.

Step 2 To configure the switch as a ModBus server, do the following:

a. Check the Enable ModBus check box.

b. From the ModBus dialog box, enter the TCP Port number and the number of connections information for the device.

Step 3 Click **Apply** to apply the changes to the configuration.

Related Topics

- ModBus Reference, page 78-3
- ModBus Dialog Box, page 78-3

ModBus Reference

This section describes the page that you can use when working with configuring ModBus and includes following topics:

- ModBus Dialog Box, page 78-3

ModBus Dialog Box

Use this page to configure the switch as a ModBus TCP server.

How to Get to This Page

Choose **Configure > Switching > ModBus**.

Related Topic

- Configuring MODBUS, page 78-2

Field Reference

Table 78-1 ModBus Dialog Box

Elements	Description
Enable ModBus check box	Check the Enable ModBus check box to enable ModBus on the switch.
TCP Port	(Optional) Set the TCP port to which clients send messages. The range for TCP-port-number is 1 to 65535. The default value is 502.

Table 78-1 ModBus Dialog Box

Elements	Description
No. of Connections	(Optional) Set the number of simultaneous connection requests that are sent to the device. The range for connection requests is 1 to 5. The default value is 1.
Apply	Click **Apply** to save the changes.

CHAPTER 79

Quality of Service Classes

A *Quality of Service* (QoS) class identifies packets that contain a certain Differentiated Services Code Point (DSCP), IP precedence value, VLAN, 802.1p (CoS), QoS Group. In addition, these packets could match a filtering criterion in a certain ACL. When a QoS class is specified in a QoS policy, it is paired with a QoS policer.

The networks operate on a best-effort delivery basis, which means that all traffic has equal priority and an equal chance of being delivered in a timely manner. When congestion occurs, all traffic has an equal chance of being dropped.

Configuring the QoS feature, you can select specific network traffic, prioritize it according to its relative importance, and use congestion-management and congestion-avoidance techniques to provide preferential treatment. Implementing QoS in the network makes its performance more predictable and bandwidth utilization more effective.

The classification is carried in the IP packet header, using 6 bits from the deprecated IP type of service (ToS) field to carry the classification (class) information. Classification can also be carried in the Layer 2 frame.

- **Prioritization bits in Layer 2 frames**:
  - Layer 2 Inter-Switch Link (ISL) frame headers have a 1-byte User field that carries an IEEE 802.1p class of service (CoS) value in the three least-significant bits. On ports configured as Layer 2 ISL, all traffic is in ISL frames.

  - Layer 2 IEEE 802.1Q frame headers have a 2-byte Tag Control Information field that carries the CoS value in the three most-significant bits, which are called the User Priority bits. On ports configured as Layer 2 IEEE 802.1Q, all traffic is in IEEE 802.1Q frames except for traffic in the native VLAN.
  - Other frame types cannot carry Layer 2 CoS values.
  - Layer 2 CoS values range from 0 for low priority to 7 for high priority.
- **Prioritization bits in Layer 3 packets**:
  - Layer 3 IP packets can carry either an IP precedence value or a Differentiated Services Code Point (DSCP) value. QoS supports the use of either value because DSCP values are backward-compatible with IP precedence values.
  - IP precedence values range from 0 to 7.
  - DSCP values range from 0 to 63.

Note This feature is supported only on Cisco 2520 series switches.

For more information, see:

http://www.cisco.com/en/US/docs/switches/connectedgrid/cgs2520/software/release/12_2_53_ex/configuration/guide/swqos.html

Related Topics

- QoS Classes, page 79-3
- QoS Class Reference, page 79-5

QoS Classes

You can create new QoS Classes, modify parameters of the existing QoS classes, and delete QoS Classes, using Cisco CP.

How to Get to This Page

Choose **Configure > Switching >Quality of Service > Classes**.

Related Topics

- Creating, Editing and Deleting a QoS Classes, page 79-3
- QoS Class Reference, page 79-5

Creating, Editing and Deleting a QoS Classes

Procedure

Use this procedure to create QoS Classes, edit the parameters of the existing QoS classes and delete QoS classes.

Step 1 Choose **Configure > Switching > Quality of Service > Classes**. See QoS Classes Summary Page, page 79-5.

Step 2 To create a QoS Class, do the following:

a. Click **Create**. The Create QoS Class window opens. See Create and Edit QoS Classes Dialog Box, page 79-6 for more information.

b. Enter a unique class name for the class in the **Class Name** field.

c. Enter a description to describe the class in the **Description** field (Optional).

- Select one of the following type of packet-matching characteristic from the **Match Type** drop-down menu. See Create and Edit QoS Classes Dialog Box, page 79-6 for more information. Options include:
- DSCP
- IP Precedence
- ACLs
- 802.1p

- VLAN
- QoS Group.
  - If you select DSCP from the match type, enter one or more DSCP values in the DSCP field.

Note The DSCP value must range from 0 to 63. Use spaces to separate multiple values.

  - If you select IP Precedence from the Match type, choose one or more match value from the Match Value field.
  - If you select IP Standard ACL, IP Extended ACL, or MAC ACL, select the ACL name or number from the drop-down menu.
  - If you select 802.1p from the Match type, enter the 802.1p (or CoS) value with a range from 0 to 7.
  - If you select VLAN from the Match type, enter the VLAN ID in the VLAN field.
  - If you select QoS Group from the Match type, select the QoS group number from the Outstrip drop-down menu in a range from 0 to 99.
  - Click **OK**. The Deliver Configure to Device dialog box opens. See Create and Edit QoS Classes Dialog Box, page 79-6 for more information.

d. Click **Deliver** in the Deliver Configure to Device dialog box to deliver the configuration changes to the device.

Step 3 To edit a QoS Class, do the following:

a. Select the QoS Class to edit parameters from the QoS Classes Summary Page.

b. Click **Edit**. The Edit QoS Classes window opens. See Create and Edit QoS Classes Dialog Box, page 79-6 for information.

c. The Class Name field displays the selected QoS class.

d. Enter or edit the description name for the selected QoS in the **Description** field. See Create and Edit QoS Classes Dialog Box, page 79-6 for information.

e. Click the Match type drop-down menu to change the Match type for the selected QoS Class and enter the attributes accordingly.

f. Click **OK**. A Deliver Configure to Device dialog box opens. See Create and Edit QoS Classes Dialog Box, page 79-6 for more information.

g. Click **Deliver** in the Deliver Configure to Device dialog box to deliver the configuration changes to the device.

Step 4 To delete a QoS Class, do the following:

a. Choose the QoS Class to delete, and click **Delete**. A confirmation dialog box opens.

b. Click **Yes** in the confirmation dialog box.

Related Topic

- QoS Class Reference, page 79-5

QoS Class Reference

This section describes the pages and dialog boxes you can use when working with QoS Class and includes the following topics:

- QoS Classes Summary Page, page 79-5
- Create and Edit QoS Classes Dialog Box, page 79-6

QoS Classes Summary Page

You can use this summary page to create new QoS classes, or to modify the parameters of the existing QoS classes, and delete a QoS classes using Cisco CP.

How to Get to This Page

Choose **Configure > Switching > Quality of Service > Classes**.

Related Topic

- Create and Edit QoS Classes Dialog Box, page 79-6

Field Reference

Table 79-1 Cisco CP —QoS Classes Summary Page

Element	Description
Class Name	Displays the names of the classes.
Description	Displays the text that describes the class.
Match Type	Displays the packet characteristic (DSCP, IP precedence, IP Standard ACL, IP Extended ACL, MAC ACL, 802.1p, VLAN, or QoS Group that is associated with the class.
Match Value	Displays the specific DSCP values, IP precedence values, IP Standard ACL name or number, IP Extended ACL name or number, MAC ACL name, 802.1p value, VLAN number, or QoS Group value that is associated with the class.
Create	Click this button to create a QoS classes.
Edit	Click this button to edit the selected QoS classes.
Delete	Click this button to delete one or more QoS classes.

Create and Edit QoS Classes Dialog Box

Use this dialog box to create a new QoS class or to edit the existing QoS Classes.

How to Get to This Page

- Choose **Configure > Switching > Quality of Service > Classes > Create**.
- Choose **Configure > Switching > Quality of Service > Classes > Edit**.

Related Topic

- QoS Classes Summary Page, page 79-5

Field Reference

Table 79-2 Create or Edit QoS Classes Dialog box

Element	Description
Class Name	Enter a unique name for the class.
Description	Enter text that describes the purpose of the class.
Match Type	Select one of the following packet-matching characteristic that defines the class form the drop-down menu: • **DSCP**—In a packet, the 6 most significant bits are of the 1-byte Type of Service (ToS) field. It prompts to enter **DSCP** value in the Match Value field. – **DSCP**—Enter to match packets with the DSCP value specified by a number with a range from 0 to 63. • **IP Precedence**—In a packet, the three most significant bits are of the 1-byte type of service (ToS) field. It prompts to enter **IP Precedence** value in the Match Value field. – **Match Value—**Enter to match packets with a precedence level specified as a number in the range from 0 to 7 or by name: routine (0), priority (1), immediate (2), flash (3), flash-override (4), critical (5), internet (6), network (7).

Table 79-2 Create or Edit QoS Classes Dialog box (continued)

Element	Description
	• **IP Standard ACL**—List of one or more access list elements (ACEs) with Standard IP that collectively define the network traffic profile. It prompts to select **Standard ACL** values from the drop-down menu in the Match Value field. – **Standard ACL**—Select the Standard ACL name or number from the drop-down menu to apply to the QoS Classes. • **IP Extended ACL**—List of one or more ACEs with Extended IP that collectively define the network traffic profile. It prompts to select **Extended ACL** values from the drop-down menu in the Match Value field. – **Extended ACL**—Select the Extended ACL name or number from the drop-down menu to apply to the QoS Classes. • **MAC ACL**—List of one or more ACEs with Extended IP that collectively define the network traffic profile. It prompts user to select **MAC ACL** values from the drop-down menu in the Match Value field. – **MAC ACL**—Select the MAC ACL name from the drop-down menu that you want the QoS Classes to be applied. • **802.1p**—Also known as Class of Service (CoS), is a 3-bit field within an Ethernet frame header when using tagged frames on an 802.1 network. It specifies a priority value between 0 and 7 inclusive that can be used by Quality of Service (QoS) to differentiate traffic. It prompts to enter 802.1p number in the Match Value field. – **802.1p**—Enter the CoS number in a range from 0 to 7 to apply the QoS Classes.

Table 79-2 Create or Edit QoS Classes Dialog box (continued)

Element	Description
	• **VLAN**—Virtual LAN enhances performance by limiting traffic to stations in the same VLAN and blocks the traffic from other VLANs. It prompts to enter VLAN ID in the Match Value field. – **VLAN**—Enter the VLAN ID to apply to the QoS Classes to be applied.The range is from 1 to 4094. • **QoS Group**—A QoS group is an internal label used by the switch to identify packets as a members of a specific class. QoS groups provide a way to tag a packet for subsequent QoS action without explicitly changing the packet. – **QoS-Group**—Select the Qos group number from the drop-down menu in a range from 0 to 99.
OK button	Click this button to save the changes.
Cancel button	Click this button to avoid saving the changes that you entered.

CHAPTER 80

QoS Policies

A *Quality of Service* policy is a set of one or more QoS classes and their associated QoS policers. A QoS policer is a specification that contains a maximum permitted rate of transmission, a maximum burst size for transmissions, and an action to take if either maximum is exceeded. You associate a QoS policer with a QoS class. Ultimately, you associate one or more class with a QoS policy and attach policies to interfaces. In this way, policers set transmission and burst limits, per class of packets, on an interface. You use a QoS policy to regulate input, output, or both, on an interface. You can use the same or different policies with different interfaces.

When you create a policy, you can specify classes and policers that already exist, or define classes and policers in the process of creating the policy.

Note This feature is supported only on Cisco 2520 series switches.

Related Topics

- Input and Output Policies, page 80-2
- Ingress Policy, page 80-3
- Egress Policy, page 80-24
- Attach, page 80-38

Input and Output Policies

Policy maps are either Input (Ingress) policy maps or Output (Egress) policy maps, attached to packets as they enter or leave the switch by service policies applied to interfaces. Input policy maps perform policing and marking on received traffic. Policed packets can be dropped or reduced in priority (marked down) if they exceed the maximum permitted rates. Output policy maps performs scheduling and queuing on traffic as it leaves the switch.

Input policies and output policies have the same basic structure; the difference is in the characteristics that they regulate.

For more information on QoS, see:

http://www.cisco.com/en/US/docs/switches/connectedgrid/cgs2520/software/release/12_2_53_ex/configuration/guide/swqos.html

Related Topics

- Ingress Policy, page 80-3
- Egress Policy, page 80-24

Ingress Policy

Ingress Policy map classification criteria include matching a Class of Service (CoS), a DSCP, an IP precedence value, an access control list (ACL), or VLAN ID (for per-port, per-VLAN QoS).

Note This QOS policing feature in Ingress QOS is supported only on Cisco 2520 series switches. GRWIC-D-ES-2S and GRWIC-D-ES-6S switching modules does not support the QOS Policing feautre in Ingress QOS. Hence, the QOS Policing feautre is greyed out for the GRWIC-D-ES-2S and GRWIC-D-ES-6S switching module.

Ingress policy map can have any of the following actions:

- Setting or marking a CoS, a DSCP, an IP precedence, or QoS group value.
- Individual policing.

Only Ingress policies provide matching on access groups or VLAN IDs, and only Egress policies provide matching on QoS groups. You can assign a QoS group number in an Ingress policy and match it in the Egress policy. The class **class-default** is used in a policy map for any traffic that does not explicitly match any other class in the policy map.

An Ingress policy map can have a maximum of 64 classes, including class-default. You can configure a maximum of 64 classes in an Ingress policy.

How to Get to This Page

Choose **Configure > Switching > Quality Of Service > Policies > Ingress Policy**.

Related Topics

- Creating, Editing, and Deleting the Ingress Policy, page 80-4
- Ingress Policy Reference, page 80-7

Creating, Editing, and Deleting the Ingress Policy

Procedure

Use this procedure to create a new Ingress policy, modify parameters of the existing Ingress policy, and delete the selected Ingress policy.

Step 1 Choose **Configure > Switching > Quality Of Service > Policies > Ingress Policy**. The QoS Ingress Policy summary page opens. See Ingress Policy Summary Page, page 80-7 for more information.

Step 2 To create an Ingress policy, do the following:

a. Click **Create**. The Create QoS Ingress Policy dialog box opens. See Create or Edit QoS Ingress Policy Dialog Box, page 80-8 for more information.

b. Enter the policy name in the **Policy Name** field and enter a text for the policy in the **Description** field. See Create or Edit QoS Ingress Policy Dialog Box, page 80-8 for more information.

c. To create flat policy, do the following:

- Click **Create**. The Assign Class To Policy—Flat or the dialog box with the policy name opens. See Assign Class To Policy—Flat, page 80-16 for more information.
- Select the class from the Class drop-down menu and enter the policy parameters, and click **OK**. You return to the Create QoS Ingress Policy dialog box. See Assign Class To Policy—Flat, page 80-16 for more information.
- Click **OK**. The Deliver Configure to Device dialog box opens.
- Click **Deliver** in the Deliver dialog box to deliver the configuration changes to the device.

d. To create hierarchical policy, do the following:

Note The Hierarchical policy associates a VLAN-based QoS Class to the Flat Ingress Policy. To use Hierarchical policy, first create the Flat policy that needs to be assigned to the VLAN-based QoS Class.

- Check the **Hierarchical Policy** check box in the Create QoS Policy dialog box, if the policy is based on the classification of the VLAN.

- Click **Create**. The Assign Class To Policy—Hierarchical or the dialog box with the policy name opens. See Assign Class To Policy—Hierarchical, page 80-23 for more information.
- Choose the QoS class and child policy from the drop-down menus, and click **OK**. You will be returned to the Create or Edit QoS Ingress Policy dialog box.
- Click **OK**. The Deliver Configure to Device dialog box opens.
- Click **Deliver** in the Deliver dialog box to deliver the configuration changes to the device.

Step 3 To edit the Ingress policy, do the following:

a. To edit the flat policy, do the following:

- Select flat policy from the Ingress Policy Summary page, and click **Edit**. The Edit QoS Ingress Policy dialog box open. See Create or Edit QoS Ingress Policy Dialog Box, page 80-8 for more information.

Note You cannot change a Flat policy to a Hierarchical policy, and vice versa.

- Select the QoS Class listed in the table, and click **Edit**. The Assign Class To Policy—Flat or the dialog box with policy name opens. See Assign Class To Policy—Flat, page 80-16 for more information.

The window that has the same fields as the Assign Class To Policy—Flat dialog box opens. However, the field shows the parameters that were entered while assigning a QoS Policy.

- Modify the class and other policy parameters, and click **OK**. You will be returned to the Edit QoS Ingress Policy dialog box. See Create or Edit QoS Ingress Policy Dialog Box, page 80-8 for more information.
- Click **OK**. The Deliver Configure to Device dialog box opens.
- Click **Deliver** in the Deliver dialog box to deliver the configuration changes to the device.

b. To edit the hierarchical policy, do the following:.

- Select hierarchical policy from the Ingress Policy summary page, and click **Edit**. The Edit QoS Ingress Policy dialog box open. See Create or Edit QoS Ingress Policy Dialog Box, page 80-8 for more information.

- Select the QoS Parent Class listed in the table, and click **Edit**. The Assign Class To Policy—Hierarchical or the dialog box with the policy name opens. See Assign Class To Policy—Hierarchical, page 80-23 for more information. The window that has the same fields as the Assign Class To Policy—Hierarchical dialog box opens. However, the field shows the parameters that were previously entered in the selected QoC Policy.
- Modify the QoS Parent Class and the required QoS Child Policy, and click **OK**. You will be returned to the Edit QoS Policy dialog box. See Create or Edit QoS Ingress Policy Dialog Box, page 80-8 for more information.
- Click **OK**. The Deliver Configure to Device dialog box opens.
- Click **Deliver** in the Deliver dialog box to deliver the configuration changes to the device.

Step 4 To delete the Ingress Policy, do the following:

a. Choose the QoS Ingress Policy from the Ingress Policy summary page, and click **Delete**. The Confirmation dialog box opens.

b. Click **Yes** in the confirmation dialog box. The Deliver Configure to Device dialog box opens.

c. Click **Deliver** in the Deliver dialog box to deliver the configuration changes to the device.

Related Topics

- Ingress Policy, page 80-3
- Ingress Policy Reference, page 80-7
- Assign Class To Policy Dialog Box, page 80-11

Ingress Policy Reference

This section describes the pages and dialog boxes you can use when working with QoS Ingress Policy and includes the following topics:

- Ingress Policy Summary Page, page 80-7
- Create or Edit QoS Ingress Policy Dialog Box, page 80-8
- Assign Class To Policy Dialog Box, page 80-11

Ingress Policy Summary Page

Use the Ingress policy summary page to view the Ingress policy that are configured; to create new Ingress policy, modify parameters of the existing Ingress policy, and delete the selected Ingress policy.

How to Get to This Page

Choose **Configure > Switching > Quality Of Service > Policies > Ingress Policy**.

Related Topics

- Create or Edit QoS Ingress Policy Dialog Box, page 80-8
- Assign Class To Policy Dialog Box, page 80-11

Field Reference

Table 80-1 Cisco CP—Ingress Policy Summary Page

Elements	Description
Policy Name	Displays the policy name of the Ingress policy.
Description	Displays the description of the Ingress policy.
Policy Type	Displays the types of Ingress policy. Displays one of the following types: • Flat • Hierarchical

Table 80-1 Cisco CP—Ingress Policy Summary Page

Elements	Description
Create button	Click this button to create new Ingress policy.
Edit button	Click this button to modify parameters of the selected Ingress policy
Delete button	Click this button to delete the Ingress policy.

Create or Edit QoS Ingress Policy Dialog Box

Use the create or edit QoS Ingress policy dialog box to create a new Ingress policy or to modify parameters of the existing Ingress Policy using Cisco CP.

How to Get to This Page

- Choose **Configure > Switching > Quality Of Service > Ingress Policy > Create**.
- Choose **Configure > Switching > Quality Of Service > Ingress Policy > Edit**.

Related Topics

- Ingress Policy Summary Page, page 80-7
- Assign Class To Policy Dialog Box, page 80-11

Field Reference

Table 80-2 Create or Edit QoS Ingress Policy—Dialog box

Element	Description
Policy Name	Enter a unique name for the policy in the **Policy Name** field.
Description	Enter the text that describes the purpose of the policy in the **Description** field. This field is optional.
Hierarchical Policy	Select this **Hierarchical Policy** check box when classification is needed based on VLAN.
QoS CLASS	Displays the selected QoS Class.
ACTION TYPE	Displays the type of action selected. Displays one of the following type: • Unconditional Marking • Policing
CIR	Displays the Committed Information Rate (CIR), in bits per sec for the selected QoS Class.
PIR	Displays the Peak Information Rate (PIR) in bits per sec for the selected QoS Class. **Note** GRWIC-D-ES-2S and GRWIC-D-ES-6S switching modules does not support the PIR.
Bc	Displays the Confirm Burst Size (Bc), in bytes, for the selected QoS Class.
Be	Displays the Exceed Burst Size (Be), in bytes, for the selected QoS Class. **Note** GRWIC-D-ES-2S and GRWIC-D-ES-6S switching modules does not support the Exceed Burst Size.

Table 80-2 Create or Edit QoS Ingress Policy—Dialog box (continued)

Element	Description
ACTION	Displays the type of action applied on the incoming traffic. • If the ACTION TYPE is Unconditional Marking, the value of ACTION is Unconditional Marking. • If the ACTION TYPE is Policing, the value of ACTION displays one of the following: – Conform Action – Exceed Action – Violate Action
Hierarchical Policy	
QoS Parent Class	Displays the VLAN-based Class as the QoS parent Class.
QoS Child Policy	Displays the Child Policy (Flat policy) assigned to corresponding QoS Parent Class.
Create button	Click this button to set new parameters and assign the Class to Policy in the **Flat** and **Hierarchical Policy** type.
Edit button	Click this button to modify the parameters of the QoS Policy in the **Flat** and **Hierarchical Policy** type.
Delete button	Click this button to delete one or more QoS Class and QoS Parent Class in the **Flat** and **Hierarchical** Policy type.
OK button	Click this button to save the changes.
Cancel button	Click this button if you do not want to save the changes that you entered.

Assign Class To Policy Dialog Box

Use this dialog box to assign the QoS Class to Policy. This dialog box contains two tables: Flat Policy and Hierarchical Policy. See the following topics as appropriate:

- Assign Class To Policy—Flat, page 80-16
- Assign Class To Policy—Hierarchical, page 80-23

Create, Edit, and Delete the parameters of QoS Class

Procedure

Use this procedure to assign parameters for the new QoS Class, modify the parameters of the existing policy, and delete the parameters of the QoS policy using Cisco CP.

Step 1 Choose **Configure > Switching > Quality Of Service > Ingress Policy > Create** or **Edit**. The Create or Edit QoS Ingress Policy dialog box opens. See Create or Edit QoS Ingress Policy Dialog Box, page 80-8 more information.

Step 2 To create or apply the parameters to the policy, do the following:

a. For a flat policy, do the following:

- Click **Create**. The Assign Class To Policy—Flat dialog box or the dialog box with the policy name opens. See Assign Class To Policy—Flat, page 80-16 for more information.
- Choose the QoS class from the **Class** drop-down menu.

- **Policing—**Click the **Policing** radio button to apply the parameters for a fine filtering on the incoming traffic, such as, CIR, PIR, Bc, Be, Conform Action, Exceed Action, and Violate Action. See Assign Class To Policy—Flat, page 80-16 for more information.
  - Enter the Committed Information Rate (CIR) and Peak Information rate (PIR). The range is from 8000 to 10000000000 bits per sec. See Assign Class To Policy—Flat, page 80-16 for more information.

Note You can set the Yellow traffic only if the PIR value is entered.

- Enter the Confirm Burst Size (Bc) and the Exceed Burst Size (Be). The range is from 8000 to 1000000 bytes.
- Set the restriction action for the incoming traffic for those that are below CIR (Green Traffic) rate, between CIR and PIR (Yellow Traffic) rate, and above PIR (Red Traffic) rate.

Note At least one action; that is, Green Traffic (also known as Conform Action), Yellow Traffic (also known as Exceed Action), or Red Traffic (also known as Violate Action) must be set for a policy.

- Click the **Set** radio button in **Green Traffic**, **Yellow Traffic**, or **Red Traffic** to set further specific limitations to match the incoming traffic. Check the check boxes of the packet characteristics that define the class, such as **802.1p (CoS)**, **QoS Group**, **IP Precedence**, and **DSCP**. Choose the values of the packet characteristic from the respective drop-down menu. See Assign Class To Policy—Flat, page 80-16 for more information.
- Click the **Transmit** radio button in **Green Traffic**, **Yellow Traffic**, or **Red Traffic** to transfer the packets without setting any restriction or limitation on the incoming traffic. See Assign Class To Policy—Flat, page 80-16 for more information.
- Click the **Drop** radio button in **Green Traffic**, **Yellow Traffic** or **Red Traffic** to drop the packets from the incoming traffic immediately. See Assign Class To Policy—Flat, page 80-16 for more information.
- After setting the parameters or the limitations that defines the class, click **OK**. You will be returned to the Create or Edit QoS Policy dialog box. See Create or Edit QoS Ingress Policy Dialog Box, page 80-8 for more information.

- **Unconditional Marking—**Click the **Unconditional Marking** radio button to modify the attributes for the traffic that belongs to a specific class. See Assign Class To Policy—Flat, page 80-16 for more information.
  - Click the **Set** radio button in **Green Traffic**, **Yellow Traffic,** or **Red Traffic** to set further specific limitations to match the incoming traffic. Check the check boxes of the packet characteristics that define the class, such as **802.1p (CoS)**, **QoS Group**, **IP Precedence**, and **DSCP**. Choose the values of the packet characteristic from the respective drop-down menu. See Assign Class To Policy—Flat, page 80-16 for more information.
  - After setting the parameters or the limitations that define the class, click **OK**. You will be returned to the Create or Edit QoS Policy dialog box. Se Create or Edit QoS Ingress Policy Dialog Box, page 80-8 for more information.
  - Click **OK**. The Deliver Configure to Device dialog box opens.
  - Click **Deliver** in the Deliver dialog box to deliver the configuration changes to the device.

b. For a hierarchical policy, do the following:

- Check the **Hierarchical Policy** check box to assign the child policy (Flat policy) to the QoS parent Class based on the VLAN classification.
- Click **Create** in the Create or Edit QoS Policy dialog box. The Assign Class To Policy—Hierarchical dialog box or the dialog box with the policy name opens. See Assign Class To Policy—Hierarchical, page 80-23 for more information.
- Choose the VLAN-based QoS parent class from the **Class** drop-down menu. See Assign Class To Policy—Hierarchical, page 80-23 for more information.
- Choose the policy (Flat policy) to assign it to the selected QoS Class from the **Child Policy** drop-down menu. See Assign Class To Policy—Hierarchical, page 80-23 for more information.
- Click **OK**. You will be returned to the Create or Edit QoS Policy dialog box. Se Create or Edit QoS Ingress Policy Dialog Box, page 80-8 for more information.
- Click **OK**. The Deliver Configure to Device dialog box opens.

- Click **Deliver** in the Deliver dialog box to deliver the configuration changes to the device.

Step 3 To edit the parameters of the selected policy, do the following:

a. For a flat policy, do the following:

- Select the flat policy from the Ingress policy summary page, and click **Edit**. The Edit QoS Ingress Policy dialog box opens. See Create or Edit QoS Ingress Policy Dialog Box, page 80-8 for more information.
- Select the QoS Class listed in the table, and click **Edit**. The Assign Class To Policy—Flat or the dialog box with policy name opens. See Assign Class To Policy—Flat, page 80-16 for more information.

The window that has the same fields as the Assign Class To Policy—Flat dialog box opens. However, the field shows the parameters that were entered earlier for the selected QoS Policy.

- Edit the parameters or the limitation from the Class drop-down menu, Action filed in the Policing and Unconditional Marking type for the selected QoS Policy, and click **OK**. You will be returned to the Create or Edit QoS Policy dialog box. See Assign Class To Policy—Flat, page 80-16 and Create or Edit QoS Ingress Policy Dialog Box, page 80-8 for more information.
- Click **OK**. The Deliver Configure to Device dialog box opens.
- Click **Deliver** in the Deliver dialog box to deliver the configuration changes to the device.

b. For a hierarchical policy, do the following:

- Select the hierarchical policy from the Ingress policy summary page, and click **Edit**. The Edit QoS Policy dialog box opens. See Create or Edit QoS Ingress Policy Dialog Box, page 80-8 for more information.
- Select the Hierarchical QoS Policy listed in the table, and click **Edit**. The Assign Class To Policy—Hierarchical or the dialog box with policy name opens. See Assign Class To Policy—Hierarchical, page 80-23 for more information.

The window that has the same fields as the Assign Class To Policy—Hierarchical dialog box opens. However, the field shows the policy that was assigned earlier to its parent QoS Class.

- Edit the parent QoS Class and the child Policy of the selected Hierarchical Policy, and click **OK**. You will be returned to the Create or Edit QoS Policy dialog box. See Assign Class To Policy—Hierarchical, page 80-23 and Create or Edit QoS Ingress Policy Dialog Box, page 80-8 for more information.
- Click **OK**. The Deliver Configure to Device dialog box opens.
- Click **Deliver** in the Deliver dialog box to deliver the configuration changes to the device.

Step 4 To delete the parameters, do the following:

a. For a flat policy, do the following:

- Select the flat policy from the summary page, and click **Edit**. Select the QoS Class listed in the table from the Create or Edit QoS Ingress Policy dialog box. See Create or Edit QoS Ingress Policy Dialog Box, page 80-8 for more information.

Note Every Policy must have at least one QoS Class associated with it.

- Click **Delete**. A Confirmation dialog box opens.
- Click **Yes** in the Confirmation dialog box.
- Click **OK** in the Create or Edit QoS Ingress Policy dialog box. The Deliver Configure to Device dialog box opens.
- Click **Deliver** in the Deliver dialog box to deliver the configuration changes to the device.

b. For a hierarchical policy, do the following:

- Select the hierarchical policy from the summary page, and click **Edit**.
- Select the QoS Parent Class, which is listed in the table, from the Create or Edit QoS Ingress Policy dialog box. See Create or Edit QoS Ingress Policy Dialog Box, page 80-8 for more information.

– Click **Delete**. A Confirmation dialog box opens.

Note Every Policy must have at least one QoS Class associated with it.

– Click **Yes** in the Confirmation dialog box.

– Click **OK** in the Create or Edit QoS Ingress Policy dialog box. The Deliver Configure to Device dialog box opens.

– Click **Deliver** in the Deliver dialog box to deliver the configuration changes to the device.

Related Topics

- Assign Class To Policy—Flat, page 80-16
- Assign Class To Policy—Hierarchical, page 80-23

Assign Class To Policy—Flat

Use the Flat policy dialog box to assign the QoS class to the Flat policy and define the parameters, such as Committed Information Rate (CIR); Peak Information Rate (PIR); Conform Burst Size (Bc); Exceed Burst Size (Be); and Conform Action, Exceed Action, and Violate Action.

How to Get to This Page

- Choose **Configure > Switching > Quality Of Service > Ingress Policy > Create** or **Edit**.
- Click **Create** to set parameters and assign the class to the Flat policy.
- Click **Edit** to modify the parameters and assign the class to the Flat policy.

Related Topics

- Assign Class To Policy—Hierarchical, page 80-23
- Create or Edit QoS Ingress Policy Dialog Box, page 80-8
- Ingress Policy Summary Page, page 80-7

Field Reference

Table 80-3 Assign Class To Policy—Flat

Element	Description
Class	Choose the QoS Class from the **Class** drop-down menu.
Action	Click one of the following actions to assign the QoS Class: • Policing, page 80-17—Policers examine the classification of each packet and determine if the packet is "in profile" or "out of profile" for that classification. Policing involves using a token bucket to determine if the packet is in or out of profile. • Unconditional Marking, page 80-21—Unconditional Marking sets or modifies the attributes for traffic belonging to a specific class. The marking action can cause the CoS, DSCP, or IP Precedence bits to be rewritten or left unchanged, depending on the software configuration. This can increase or decrease the priority of a packet in accordance with the policy used in the QoS domain so that other QoS functions can use the marking information to judge the relative and absolute importance of the packet.
Policing	
Committed Information Rate (CIR)	CIR in a Frame relay network is the average bandwidth for a virtual circuit guaranteed by an ISP to work under normal conditions. Enter the average bandwidth. The range is from 8000 to 10000000000 bits per sec in the **Committed Information Rate (CIR)** field.
Peak Information Rate (PIR)	Packets that exceed the CIR but are below the PIR are marked with medium-high packet-loss priority (Yellow). Packets that exceed the PIR are marked with high packet-loss priority (Red). Enter the maximum achievable bandwidth in a range from 8000 to 10000000000 bits/sec in **Peak Information Rate (PIR)** field. **Note** GRWIC-D-ES-2S and GRWIC-D-ES-6S switching modules does not support the PIR.

Table 80-3 Assign Class To Policy—Flat (continued)

Element	Description
Confirm Burst Size (Bc)	Enter the burst size. The range is from 8000 to 1000000 bytes in the **Confirm Burst Size** field.
Exceed Burst Size (Be)	Enter the burst size. The range is from 8000 to 1000000 bytes in the **Exceed Burst Size** field. This field is enable only if PIR is entered. **Note** GRWIC-D-ES-2S and GRWIC-D-ES-6S switching modules does not support the Exeed Burst Size.

Table 80-3 Assign Class To Policy—Flat (continued)

Element	Description
Green Traffic: (Conform Action)	Set the restriction for the incoming traffic that is below CIR rate by choosing one of the following actions: • **Set**—Click the **Set** radio button and apply the following characteristic to the incoming packets: – **802.1p (CoS)**—Check the **802.1p (CoS)** check box and choose a value to apply the class of service value to the incoming packets in the range from 0 to 7 from the **802.1p (CoS)** drop-down menu – **QoS Group—**Provides a way to tag the packet for subsequent QoS action without explicitly marking (changing) the packet. Check the **QoS Group** check box and choose a value to apply QoS group value to the incoming packets in the range from 0 to 99 from the **QoS Group** drop-down menu. – **IP Precedence—**Check the **IP Precedence** check box and choose a value to apply the **IP Precedence** value to the incoming packets in the range from 0 to 7 from the **IP Precedence** drop-down menu t – **DSCP—**Check the **DSCP** check box and choose a DSCP value to apply the DSCP value to the incoming packets in the range from 0 to 63 from the **DSCP** drop-down menu. **Note** The IP Precedence and DSCP are mutually exclusive, therefore, you can select only one at any time. This is true for all the configurations in which IP Precedence and DSCP options are available. • **Transmit—**Click the **Transmit** radio button to transmit the incoming traffic, without any restriction or limitations. • **Drop—**Click the **Drop** radio button to drop the incoming traffic that is below CIR rate. **Note** By default, the conform action is set to **Transmit**.

Table 80-3 Assign Class To Policy—Flat (continued)

Element	Description
Yellow Traffic: (Exceed Action)	Set the restriction for the incoming traffic that holds the rate between CIP and PIR on choosing one of the following action: • **Set**—Click the **Set** radio button and apply the following characteristic to the incoming packets: – **802.1p (CoS)**—Check the **802.1p (CoS)** check box and choose a value to apply the class of service value to the incoming packets in the range from 0 to 7 from the **802.1p (CoS)** drop-down menu – **QoS Group—**Provides a way to tag the packet for subsequent QoS action without explicitly marking (changing) the packet. Check the **QoS Group** check box and choose a value to apply QoS group value to the incoming packets in the range from 0 to 99 from the **QoS Group** drop-down menu. – **IP Precedence—**Check the **IP Precedence** check box and choose a value to apply the **IP Precedence** value to the incoming packets in the range from 0 to 7 from the **IP Precedence** drop-down menu t – **DSCP—**Check the **DSCP** check box and choose a DSCP value to apply the DSCP value to the incoming packets in the range from 0 to 63 from the **DSCP** drop-down menu. • **Transmit—**Click the **Transmit** radio button to transmit the incoming traffic, without any restriction or limitation. • **Drop—**Click the **Drop** radio button to drop the incoming traffic that has the rate between CIR and PIR. **Note** By default, the exceed action is set to **Drop**.

Table 80-3 Assign Class To Policy—Flat (continued)

Element	Description
Red Traffic: (Violate Action)	Set the restriction for the incoming traffic that exceeds PIR rate on choosing one of the following action: • **Set**—Click the **Set** radio button and apply the following characteristic to the incoming packets: – **802.1p (CoS)**—Check the **802.1p (CoS)** check box and choose a value to apply the class of service value to the incoming packets in the range from 0 to 7 from the **802.1p (CoS)** drop-down menu – **QoS Group—**Provides a way to tag the packet for subsequent QoS action without explicitly marking (changing) the packet. Check the **QoS Group** check box and choose a value to apply QoS group value to the incoming packets in the range from 0 to 99 from the **QoS Group** drop-down menu. – **IP Precedence—**Check the **IP Precedence** check box and choose a value to apply the **IP Precedence** value to the incoming packets in the range from 0 to 7 from the **IP Precedence** drop-down menu t – **DSCP—**Check the **DSCP** check box and choose a DSCP value to apply the DSCP value to the incoming packets in the range from 0 to 63 from the **DSCP** drop-down menu. • **Transmit—**Click the **Transmit** radio button to transmit the incoming traffic, without any restriction or limitation. • **Drop—**Click the **Drop** radio button to drop the incoming traffic that exceeds the PIR rate. **Note** By default, the violate action is set to **Drop**.
Unconditional Marking	

Table 80-3 Assign Class To Policy—Flat (continued)

Element	Description
Set	Click the **Set** radio button and apply the following characteristic to the incoming packets: • **802.1p (CoS)**—Check the **802.1p (CoS)** check box and choose a value to apply the class of service value to the incoming packets in the range from 0 to 7 from the **802.1p (CoS)** drop-down menu • **QoS Group**—Provides a way to tag the packet for subsequent QoS action without explicitly marking (changing) the packet. Check the QoS Group check box and choose a value to apply QoS group value to the incoming packets in the range from 0 to 99 from the QoS Group drop-down menu. • **IP Precedence**—Check the IP Precedence check box and choose a value to apply the IP Precedence value to the incoming packets in the range from 0 to 7 from the IP Precedence drop-down menu t • **DSCP**—Check the DSCP check box and choose a DSCP value to apply the DSCP value to the incoming packets in the range from 0 to 63 from the DSCP drop-down menu.
OK button	Click this button to save the changes.
Cancel button	Click this button to avoid saving the configuration changes that you entered.

Assign Class To Policy—Hierarchical

Use the hierarchical policy dialog box to assign the QoS Class to the Hierarchical policy when classification is based on VLAN, using Cisco CP.

How to Get to This Page

- Choose > **Configure > Switching > Quality Of Service > Ingress Policy > Create** or **Edit**.
- Check the **Hierarchical Policy** check box.
- Click **Create** to assign the parent class to child (hierarchical) policy.
- Click **Edit** to modify parent class and the child policy.

Related Topics

- Assign Class To Policy—Flat, page 80-16
- Create or Edit QoS Ingress Policy Dialog Box
- Ingress Policy Summary Page

Field Reference

Table 80-4 Assign Class To Policy—Hierarchical

Element	Description
Class	Choose the VLAN-based parent class from the **Class** drop-down menu.
Child Policy	Choose the child (Flat) policy to be assigned to the parent class from the **Child Policy** drop-down menu.
OK button	Click this button to save the changes.
Cancel button	Click this button to avoid saving the configuration changes that you entered.

Egress Policy

Egress policy map classification criteria include matching a CoS, a DSCP, an IP precedence, or a QoS group value.

Egress policy maps can have any of following actions:

- Queuing (queue-limit)
- Scheduling (bandwidth, priority, and shape average)

Egress policies do not support marking or policing (except in the case of priority with policing). There is no egress packet marking on the switch.

The class **class-default** is used in a policy map for any traffic that does not explicitly match any other class in the policy map. There can be a maximum of four classes in the Egress policy map (including class-default) because egress ports have a maximum of four queues.

Egress policy maps do not support matching of access groups. You can use QoS groups as an alternative by matching the appropriate access group in the Ingress policy map and set a QoS group. In the Egress policy map, you can then match the QoS group.

An Egress policy map attached to an egress port can match only the packets that have already been matched by an Ingress policy map attached to the ingress port for the packets. You can attach an Egress policy map to any or all ports on the switch. The switch supports configuration and attachment of a unique Egress policy map for each port. However, these Egress policy maps can contain only three unique configurations of queue limits. These three unique queue-limit configurations can be included in as many Egress policy maps as there are ports on the switch. There are no limitations on the configurations of bandwidth, priority, or shaping.

How to Get to This Page

Choose **Configure > Switching > Quality of Service > Policies > Egress Policy**.

Related Topics

- Creating, Editing, and Deleting the Egress Policy, page 80-25
- Egress Policy Reference, page 80-28

Creating, Editing, and Deleting the Egress Policy

Procedure

Use this procedure to create a new Egress policy, modify the parameters or values of the existing Egress policy, and delete the selected Egress policy.

Step 1 Choose **Configure > Switching > Quality of Service > Policies > Egress Policy**. The Egress Policy summary page opens. See Egress Policy Summary Page, page 80-28.

Step 2 To create an Egress policy, do the following:

a. Click **Create**. The Create or Edit QoS Egress Policy opens. See Create or Edit QoS Egress Policy, page 80-29 for more information.

b. Enter the policy name and a brief description in the **Policy Name** and **Description** field. See Create or Edit QoS Egress Policy, page 80-29 for more information.

c. To create a flat policy, do the following:

- Click **Create**. The Assign Class to Policy—Flat dialog box or the dialog box with the policy name opens. See Assign Class To Policy Dialog Box, page 80-31 for more information.
- Choose the type of class from the Class drop-down menu and enter the parameters for Congestion Management and Congestion Avoidance fields. See Assign Class To Policy Dialog Box, page 80-31 for more information.
- Click **OK**. You will be returned to Create or Edit QoS Egress Policy dialog box. See Assign Class To Policy Dialog Box, page 80-31 for more information

Note

- The QoS Egress Policy can have a maximum of four QoS Classes. To modify any of the above parameters that are not editable, you must delete the policy and create a new one.
- If the first Egress policy is created with *n* number of classes, all other policy created in the later stage should also have the same number of classes, where *n* is =< 4 classes.

- Click **OK**. The Deliver Configure to Device dialog box opens.
- Click **Deliver** in the Deliver dialog box to deliver the configuration changes to the device.

d. To create a hierarchical (Port Based Shaping) policy, do the following:

- Check the **Port Based Shaping** check box in the Create QoS Egress Policy dialog box. See Create or Edit QoS Egress Policy, page 80-29 for more information.
- By default, the **class-default** is attached as the parent class in the **Name** field. Enter the value in the **Rate** field. The range is from 64000 to 1000000000 bps. See Create or Edit QoS Egress Policy, page 80-29 for more information.
- Choose the type of policy from the **Child Policy** drop-down menu. See Create or Edit QoS Egress Policy, page 80-29 for more information.
- Click **OK**. The Deliver Configure to Device dialog box opens.
- Click **Deliver** in the Deliver dialog box to deliver the configuration changes to the device.

Step 3 To edit an Egress Policy, do the following:

a. To edit a flat policy, do the following:

- Select a flat egress policy from the Egress Policy summary page and click **Edit**. The Edit QoS Egress Policy dialog box opens. See Create or Edit QoS Egress Policy, page 80-29 for more information.

Note

- You can only modify the values of Congestion Management and Congestion Avoidance of the selected QoS Class in the selected QoS policy. You cannot change or modify the policy name, add a QoS class, or change the congestion management of the selected QoS class in a QoS policy.
- You cannot change a flat policy to a hierarchical (Port Based Shaping) policy or vice versa.

- Select the QoS class, and click **Edit**. The Assign Class to Policy dialog box or the dialog box with the policy name opens.

- Modify the values of the Congestion Management and Congestion Avoidance, and click **OK**. You will be returned to the Edit QoS Egress Policy dialog box. See Assign Class To Policy Dialog Box, page 80-31 and Create or Edit QoS Egress Policy, page 80-29 for more information.
- Click **OK**. The Deliver Configure to Device dialog box opens.
- Click **Deliver** in the Deliver dialog box to deliver the configuration changes to the device.

b. To edit a hierarchical (Port Based Shaping) policy, do the following:

- Select hierarchical policy from the Egress Policy summary page, and click **Edit**. The Edit QoS Egress Policy dialog box open. See Create or Edit QoS Egress Policy, page 80-29 for more information.
- Enter or modify the value in the **Rate** field for the selected hierarchical policy. The range is from 64000 to 1000000000 bps.
- Choose the type of policy to be attached to the selected hierarchical policy from the **Child Policy** drop-down menu.
- Click **OK**. The Deliver Configure to Device dialog box opens.
- Click **Deliver** in the Deliver dialog box to deliver the configuration changes to the device.

Step 4 To delete the Egress Policy, do the following:

a. Choose the QoS Egress Policy from the Egress Policy summary page, and click **Delete**. The Confirmation dialog box opens.

Note

- A child policy cannot be deleted if it is assigned to a hierarchical policy; therefore, delete the hierarchical policy before deleting the flat policy.
- Also, you will receive a warning message if you try to delete a policy that is attached to an interface.

b. Click **Yes** in the confirmation dialog box. The Deliver Configure to Device dialog box opens.

c. Click **Deliver** in the Deliver dialog box to deliver the configuration changes to the device.

Related Topics

- Egress Policy, page 80-24
- Egress Policy Reference, page 80-28
- Assign Class To Policy Dialog Box, page 80-31

Egress Policy Reference

This section describes the pages and dialog boxes you can use when working with QoS Egress Policy and includes the following topics:

- Egress Policy Summary Page, page 80-28
- Create or Edit QoS Egress Policy, page 80-29
- Assign Class To Policy Dialog Box, page 80-31

Egress Policy Summary Page

Use the Egress Policy summary page to view the Egress policies that are configured and to create new Egress policies, modify parameters of the existing Egress policy, and delete the selected Egress policy.

How to Get to This Page

Choose **Configure > Switching > Quality of Service > Policies > Egress Policy**.

Related Topics

- Create or Edit QoS Egress Policy, page 80-29
- Assign Class To Policy Dialog Box, page 80-31

Field Reference

Table 80-5 Cisco CP—QoS Egress Policy Summary Page

Elements	Description
Policy Name	Displays the policy names of the Egress Policy.
Description	Displays the description of the Egress Policy.

Table 80-5 Cisco CP—QoS Egress Policy Summary Page (continued)

Elements	Description
Policy Type	Displays the types of Egress Policy. Displays one of the following type: • Flat • Hierarchical
Create button	Click this button to create new Egress policy.
Edit button	Click this button to modify parameters of the selected Egress policy
Delete button	Click this button to delete the Egress policy.

Create or Edit QoS Egress Policy

Use the create or edit QoS Egress policy dialog box to create a new Egress policy, or to modify the parameters of the existing Egress Policy using Cisco CP.

How to Get to This Page

Choose **Configure > Switching > Quality of Service > Policies > Egress Policy > Create**.

Choose **Configure > Switching > Quality of Service > Policies > Egress Policy > Edit**.

Related Topics

- Assign Class To Policy Dialog Box, page 80-31
- Egress Policy Summary Page, page 80-28

Field Reference

Table 80-6 Create or Edit Egress QoS Policy Dialog box

Elements	Description
Policy Name	Enter a unique name for the policy in the **Policy Name** field.
Description	Enter the text that describes the purpose of the policy in the **Description** field. This field optional.

Table 80-6 Create or Edit Egress QoS Policy Dialog box (continued)

Elements	Description
Port Based Shaping	Select this **Port Based Shaping** check box to apply the rate limit to the aggregate traffic egressing an interface.
QoS Class	Displays the QoS Classes added to the particular policy.
Congestion Management Type	Displays the types of the congestion management. Displays one of the following type: • Priority Queuing • Class Based Weighted Queuing • Class Based Shaping
Add button	Click this button to add the class to the selected policy.
Edit button	Click this button to modify the parameters of the QoS Class and the Port Based Shaping of the selected QoS Policy.
Delete button	Click this button to delete one or more QoS Class and Congestion Management Type on the Port Based Shaping.
Port Based Shaping	
Name	By default, the class **class-default** is used as the Parent Class.
Rate	Enter the value in a range from 64000 to 1000000000 bps in the **Rate** field.
Child Policy	Choose the option from the **Child Policy** drop-down menu.
OK button	Click this button to save the changes.
Cancel button	Click this button to avoid saving the configuration changes that you entered.

Assign Class To Policy Dialog Box

Use this dialog box to assign a class to the Egress policy and set the parameters for congestion management and congestion avoidance. This dialog box contains following topics:

- Create, Edit, and Delete the parameters of QoS Class for the QoS Policy, page 80-31
- Assign Class to Policy—Flat, page 80-35

Create, Edit, and Delete the parameters of QoS Class for the QoS Policy

Procedure

Use this procedure to associate a QoS class within the QoS policy, modify the parameters related to the QoS class, and remove association of the selected QoS class in the QoS policy using Cisco CP.

Step 1 Choose **Configure >Switching > Quality of Service > Egress Policy > Create** or **Edit**. The Create or Edit QoS Egress Policy dialog box opens. See Create or Edit QoS Egress Policy, page 80-29 for more information.

Step 2 Enter the policy name and description that best describes the policy in the **Policy Name** and **Description** field.

Step 3 To associate a QoS class to the QoS policy and set the parameters, do the following:

a. For a flat policy, do the following:

- Click **Create**. The Assign Class to Policy dialog box or the dialog box with the policy name opens. See Assign Class to Policy—Flat, page 80-35 for more information.
- Choose the QoS class from the **Class** drop-down menu.

Note

- An Egress policy can have maximum of four QoS classes, including the "**class-default**" class.
- The new Egress policy must have the same number of QoS classes defined as the first Egress policy. For example, if you defined three QoS classes in the first Egress policy, the subsequent Egress policies created must also have three QoS classes defined.

Congestion Management

- **Priority Queuing—**Click this radio button to priorities the incoming traffic.
  - You can check the **Policer** check box and enter the policer rate.The range is from 8000 to 10000000000 bits per sec.

Note

- Priority Queuing will not be created with the **class-default** class.
- Only one class can have a Priority Queuing in each policy.
- You cannot add Priority Queuing to a policy that already uses a QoS Class with Class Based Weighted Queuing or Class Based Shaping. If the Priority Queuing needs to be used in a Policy, you must first add the Priority Queueing, followed by others.

- **Class Based Weighted Queuing**—Click this radio button and enter the following parameters:
  - **Rate in Percentage Remaining**—Enter the rate of percentage for the remaining traffic. The range is from 0 to 99 percent.

On defining the policer rate in the policy, enter the following parameters:

  - **Rate in Percentage—**Click this radio button and enter the rate of percentage for the traffic to obtain the CBWQ. The range is from 0 to 99 percent.
  - **Absolute Rate**—Click this radio button and enter bandwidth for the absolute rate. The range is from 64000 to 1000000000 bps.
- **Class Based Shaping—**Click this radio button and enter the parameters if the policer rate is defined in the policy.

Note A Class Based Shaping is not allowed if Priority Queuing is created without policer.

- **Absolute Rate**—Enter the absolute rate. The range is from 64000 to 1000000000 bps.

Congestion Avoidance

- **Queue 1 Limit**—Enter the first buffer Queue limit. The range is from 16 to 544 buffer for all the traffic.
- Choose the class from the **Class Type** drop-down menu. Queue2 and Queue3 class values need to be specified for this class type.
  - **Queue 2 Limit**—Enter the buffer limit for Queue 2. The range is from 16 to 544 buffer.
  - **Queue2 Class Value—**Enter the class value in the Queue 2 buffer limit of the selected class type within its respective range.
  - **Queue 3 Limit**—Enter the buffer limit for Queue 3. The range is from 16 to 544 buffer.
  - **Queue3 Class Value**—Enter the class value in the Queue3 buffer limit of the selected class type within its respective range.
- After all the above parameters are set, click **OK**. You will be returned to the Create QoS Egress Policy dialog box.
  - Click **OK**. The Deliver Configure to Device dialog box opens.
  - Click **Deliver** in the Deliver dialog box to deliver the configuration changes to the device.

b. For a hierarchical (Port Based Shaping) policy, do the following:

- Check the **Port Based Shaping** check box to assign the child policy (Flat policy) and to apply the rate limit the aggregate traffic egressing an interface.

Note By default, the port based shaping (hierarchical) uses the QoS Class **class-default** as the parent class.

- Enter the limit value in the **Rate** field. The range is from 64000 to 1000000000 bps.
- Choose the type of policy to be attached to the QoS Class (Parent) to specify class-based actions for the queues on the shaped port.
- Click **OK**. The Deliver Configure to Device dialog box opens.
- Click **Deliver** in the Deliver dialog box to deliver the configuration changes to the device.

Step 4 To edit the parameters related to QoS class for the QoS policy, do the following:

a. For a flat policy, do the following:

- Select the flat policy from the QoS Egress summary page, and click **Edit**. The Edit QoS Egress Policy dialog box opens. See Create or Edit QoS Egress Policy, page 80-29 for more information.
- Select the QoS Class listed in the table, and click **Edit**. The Assign Class To Policy dialog box or the dialog box with policy name opens. See Assign Class to Policy—Flat, page 80-35 for more information.

The window that has the same fields as the Assign Class To Policy—Flat dialog box opens. However, the field shows the parameters that are already entered for the selected QoS Class.

- Modify the required parameters in the Congestion Management and Congestion Avoidance fields, and click **OK**. You will be returned to the Edit QoS Egress Policy dialog box. See Create or Edit QoS Egress Policy, page 80-29 for more information.
- Click **OK**. The Deliver Configure to Device dialog box opens.
- Click **Deliver** in the Deliver dialog box to deliver the configuration changes to the device.

b. For a hierarchical (Port Based Shaping) policy, do the following:

- Select the Hierarchical policy from the QoS Egress Policy summary page, and click **Edit**. The Edit QoS Egress Policy dialog box opens. See Create or Edit QoS Egress Policy, page 80-29 for more information.
- Modify the limit value in the **Rate** field and the policy from the Child Policy drop-down menu for the selected hierarchical policy.
- Click **OK**. The Deliver Configure to Device dialog box opens.
- Click **Deliver** in the Deliver dialog box to deliver the configuration changes to the device.

Step 5 To remove the association of a QoS Class from the QoS Policy, do the following:

- A QoS class can be deleted only while creating a QoS Policy.

Note You cannot delete a QoS Class after the Policy is created.

- When creating a QoS Policy, select the QoS class from the Create QoS Egress Policy dialog box, and click **Delete**. A Confirmation dialog box opens.
- Click **Yes** in the Confirmation dialog box.

Related Topics

- Assign Class to Policy—Flat, page 80-35
- Create or Edit QoS Egress Policy, page 80-29
- Egress Policy Summary Page, page 80-28

Assign Class to Policy—Flat

Use the Add Class to Policy dialog box or the dialog box with the policy name to add the classes and apply the Congestion Management and Congestion Avoidance parameters to the selected policy, using Cisco CP.

How to Get to This Page

- Choose **Configure > Switching > Quality of Service > Egress Policy > Create** or **Edit**.
- Click **Add** to add the QoS Classes to the selected policy.
- Select the QoS Class, and click **Edit** to modify the Congestion Management and Congestion Avoidance parameters.

Related Topics

- Create or Edit QoS Egress Policy, page 80-29
- Egress Policy Summary Page, page 80-28

Field Reference

Table 80-7 Assign Class to Policy Dialog box

Elements	Description
Class	Choose the type of QoS Class to add or assign it to the selected policy from the **Class** drop-down menu.
Congestion Management	
Priority Queuing	Priority Queuing ensures that a particular class of traffic is given preferential treatment. With strict priority queuing, the priority queue is constantly serviced; all packets in the queue are scheduled and sent until the queue is empty. The congestion management for the first class should always have Priority Queuing. Define the rate of traffic in the **Policer** and **Policer Rate** field. • **Policer**—Check the **Policer** check box to define a specific rate of traffic. • **Policer Rate**—Enter the policer rate. The range is from 8000 to 10000000000 in bits per sec.
Class Based Weighted Queuing	Class Based Weighted Queuing sets the relative precedence of a queue by allocating a portion of the total bandwidth that is available for the port. • When defining the Policer rate in the priority queuing, you must enter one of the following parameters: – **Rate in Percentag**e—Click the radio button and enter the number of percentage for the traffic to obtain the CBWQ. The range is from 0 to 99 percent. – **Absolute Rate**—Click the radio button and enter the bandwidth for the absolute rate. The range is from 64000 to 1000000000 bps. • If the Policer rate is not defined in the priority queuing, you must enter the following parameter: – **Rate in Percentage Remaining—**Enter the bandwidth for the remaining traffic. The range is from 0 to 99percent.

Table 80-7 Assign Class to Policy Dialog box (continued)

Elements	Description
Class Based Shaping	Class Based Shaping is a control mechanism that is applied to limit the rate on classes of traffic leaving an interface. You can use the Class Based Shaping only if the Policer rate is defined in the Policy. – **Absolute Rate**—Enter the absolute rate. The range is from 64000 to 1000000000 bps.
Congestion Avoidance	
Queue 1 Limit	Enter the first buffer Queue limit. The range is from 16 to 544 for all the traffic. The Queue 1 limit is also called the Global Queue Limit.
Class Type	Choose the type of class for the Queue 2 and Queue 3 limit. Choose one of the following: • cos • dscp • precedence • qos-group
Queue 2 Limit	Enter the second buffer limit (capacity to hold the selected class type traffic). The range is from 16 to 544.
Queue2 Class Value	Enter the value of the class type. For example, when selecting DSCP traffic as the class type, enter the value within the range from 0 to 63.
Queue 3 Limit	Enter the third buffer limit (capacity to hold the selected class type traffic). The range is from 16 to 544.
Queue3 Class Value	Enter the value of the class type.
OK button	Click this button to save the changes.
Cancel button	Click this button to avoid saving the configuration changes that you entered.

Attach

Initially, the interfaces or the ports associated with the selected device do not have any policy attached to them. Therefore, you can use this page to attach Ingress and Egress policy to the incoming and outgoing packets, using Cisco CP.

How to Get to This Page

Choose **Configure > Switching > Quality of Service > Policies > Attach**.

Related Topics

- Attach Policy to an Interface, page 80-38
- Attach Policy Reference, page 80-39

Attach Policy to an Interface

Procedure

Use this procedure to attach or detach a QoS Ingress Policy or Egress Policy on the selected interface.

Step 1 Choose **Configure > Switching > Quality of Service > Policies > Attach**. The Attach Policy Summary Page opens. See Attach Policy Summary Page, page 80-39 for more information.

Step 2 Select the interface to which QoS Ingress Policy and QoS Egress Policy will be attached, and click **Edit**. The Edit QoS Policy Attach dialog box opens. See Attach Policy Summary Page, page 80-39 and Edit QoS Policy Attach Dialog Box, page 80-40 for more information.

Step 3 The selected interface is displayed in the **Interface** field. See Edit QoS Policy Attach Dialog Box, page 80-40 for more information.

Step 4 Choose the type of Ingress policy that has to be attached to the selected interface from the **Ingress Policy** drop-down menu.

Step 5 Choose the type of Egress policy that has to be attached to the selected interface from the **Egress Policy** drop-down menu.

Step 6 Click **OK**. The Deliver Configure to Device dialog box opens.

Step 7 Click **Deliver** in the Deliver dialog box to deliver the configuration changes to the device.

Related Topics

- Attach Policy Summary Page, page 80-39
- Edit QoS Policy Attach Dialog Box, page 80-40

Attach Policy Reference

This section describes the summary page and dialog box you can use when attaching an Ingress and Egress Policy to an interface and includes the following topics:

- Attach Policy Summary Page, page 80-39
- Edit QoS Policy Attach Dialog Box, page 80-40

Attach Policy Summary Page

Use this summary page to view the Ingress and Egress policy attached to the interface or edit the same for the selected interface.

How to Get to This Page

Choose **Configure > Switching > Quality of Service > Policies > Attach**.

Related Topics

- Edit QoS Policy Attach Dialog Box, page 80-40
- Ingress Policy, page 80-3
- Egress Policy, page 80-24

Field Reference

Table 80-8 Attach Policy Summary Page

Elements	Description
Interface	Displays all the interface or ports in the device.
Ingress Policy	Displays the name of the Ingress policy attached to the interface.
Egress Policy	Displays the name of the Egress policy attached to the interface.
Edit button	Click this button to modify the attached policy of the selected interface.

Edit QoS Policy Attach Dialog Box

Use the Edit QoS Policy Attach dialog box to edit the policy attached to the selected interface using Cisco CP.

How to Get to This Page

Choose Configure > Switching > Quality of Service > Policies > Attach.

- Click **Edit**.

Related Topics

- Attach Policy Summary Page, page 80-39
- Ingress Policy, page 80-3
- Egress Policy, page 80-24

Field Reference

Table 80-9 Edit QoS Policy Attach Dialog Box

Element	Description
Interface	Displays the name of the selected interface.
Ingress Policy	Choose the Ingress Policy to attach to the selected interface from the **Ingress Policy** drop-down menu.

Table 80-9 Edit QoS Policy Attach Dialog Box (continued)

Element	Description
Egress Policy	Choose the Egress Policy to attach it to the selected interface from the **Egress Policy** drop-down menu.
OK button	Click this button to save the changes.
Cancel button	Click this button to avoid saving the changes that you entered.

CHAPTER 81

Quality of Service Report

Quality of Services (QoS) is defined as the ability of a network or device to provide preferential service to selected traffic. QoS report displays or reports the incoming and outgoing traffic on connected switch interfaces. When QoS is not configured on a device, the device offers best-effort service to each packet, regardless of the packet contents or size.

A QoS report displays the following counts:

- Incoming and outgoing packets that match each possible DSCP and CoS value.
- In-profile and out-of-profile packets, as determined by the policer.

Note This feature is supported only on Cisco 2520 series switches.

Related Topics

- DSCP Statistics, page 81-2
- Class of Service Statistics, page 81-3
- Policer Statistics, page 81-4

DSCP Statistics

Differentiated Services Code Point (DSCP) statistics display the total incoming and outgoing packets that match every possible DSCP value.

Related Topics

- Refreshing the DSCP Statistic Page, page 81-2
- DSCP Statistics Summary Page, page 81-2

Refreshing the DSCP Statistic Page

Procedure

Use this procedure to refresh the page.

Step 1 Choose **Monitor > Switching > QoS Report > DSCP Statistics**.

Step 2 Click **Refresh**. The page refreshes and updates the incoming and outgoing packets.

Related Topic

- DSCP Statistics Summary Page, page 81-2

DSCP Statistics Summary Page

Use this window to view the incoming and outgoing packets.

How to Get to This Page

Choose **Monitor > Switching > QoS Report > DSCP Statistics**.

Field Reference

Table 81-1 Cisco CP - DSCP Statistics

Elements	Description
Interface	Select the interface from the drop-down menu.
DSCP	Displays the DSCP value.
Incoming Packets	Displays the total incoming packets that matches the DSCP value.
Outgoing Packets	Displays the total outgoing packets that matches the DSCP value.
Refresh button	Refreshes the page.

Class of Service Statistics

Class of Service (CoS) statistics displays the total incoming and outgoing packets that match every possible CoS value.

Related Topics

- Refreshing the CoS Statistics Page, page 81-3
- CoS Statistics Summary Page, page 81-4

Refreshing the CoS Statistics Page

Procedure

Use this procedure to refresh the page.

Step 1 Choose **Monitor > Switching > QoS Report > CoS Statistics**.

Step 2 Click **Refresh**. The page refreshes and updates the incoming and outgoing packets.

Related Topic

- CoS Statistics Summary Page, page 81-4

CoS Statistics Summary Page

Use this window to view the incoming and outgoing packets.

How to Get to This Page

Choose **Monitor > Switching > QoS Report > CoS Statistics**.

Field Reference

Table 81-2 Cisco CP - CoS Statistics

Elements	Description
Interface	Select the Interface from the drop-down menu.
CoS	Displays the CoS value.
Incoming Packets	Displays the total incoming packets that matches the CoS value.
Outgoing Packets	Displays the total outgoing packets that matches the CoS value.
Refresh button	Refreshes the page.

Policer Statistics

The Policer displays the total in-profile and out-of-profile packets, as determined by the QoS policy configured.

Related Topics

- Refreshing the Policer Statistics Page, page 81-5
- Policer Statistic Summary Page, page 81-5

Refreshing the Policer Statistics Page

Procedure

Use this procedure to refresh the page.

Step 1 Choose **Monitor > Switching > QoS Report > Policer Statistics**.

Step 2 Click **Refresh**. The page refreshes and updates the in-profile and out-profile packets.

Related Topic

- Policer Statistic Summary Page, page 81-5

Policer Statistic Summary Page

Use this page to view the in-profile and out-profile packets.

How to Get to This Page

Choose **Monitor > Switching > QoS Report > Policer Statistics**.

Field Reference

Table 81-3 Cisco CP - Policer Statistics

Element	Description
Interface	Select the Interface from the drop-down menu.
In Profile Packets	Displays the total In-profile packets determined by the policer.
Out Profile Packets	Displays the total Out-profile packets determined by the policer.
Refresh button	Refreshes the page.

CHAPTER 82

STP Configuration

Spanning Tree Protocol (STP) is a standardized technique for maintaining a network of multiple bridges or switches. When the network topology changes, STP prevents the creation of loops by placing ports in a forwarding or blocking state, and transparently reconfigures bridges and switches. Each VLAN is treated as a separate network, and a separate instance of STP is applied to each VLAN.

The following two protocols are supported on the switch:

- Per-VLAN spanning-tree (PVST+), based on the IEEE 802.1D standard and Cisco proprietary extensions.
- Rapid per-VLAN spanning-tree (rapid-PVST+), based on the IEEE 802.1W standard.

Note By default, the switch runs in the PVST+ mode. This feature is supported only on Cisco 2520 series switches.

The Per-VlAN and Rapid per-VLAN are described as follows:

- **Per-VLAN**—PVST+ protocol runs on each VLAN on the switch up to the maximum supported, ensuring that each has a loop-free path through the network.
- **Rapid per-VLAN**—Rapid PVST+ protocol is the same as the PVST+, except that it uses a rapid convergence based on IEEE 802.1W. To provide rapid convergence, rapid PVST+ immediately deletes dynamically learned MAC address entries on a per-port basis after receiving a topology change. By contrast, PVST+ uses a short aging time for dynamically learned MAC address entries.

For more information on STP configuration, see:

http://www.cisco.com/en/US/docs/switches/connectedgrid/cgs2520/software/release/12_2_53_ex/configuration/guide/swstp.html

Switches send and receive spanning-tree frames at regular intervals called Bridge Protocol Data Units (BPDUs). The switches do not forward these frames but use them to construct a loop-free path. BPDUs contain information about the sending switch and its ports, including switch and MAC addresses, switch priority, port priority, and path cost. Spanning tree uses this information to elect the root switch and root port for the switched network and the root port and designated port for each switched segment. See Port Parameters, page 82-9 for more information.

Related Topics

- STP Status, page 82-2
- Bridge Parameters, page 82-5
- Port Parameters, page 82-9

STP Status

This section describes the summary page of the STP status and includes the following topic:

- To Apply Global Spanning-Tree Protocol, page 82-2
- STP Status Summary Page, page 82-3

To Apply Global Spanning-Tree Protocol

Procedure

Use this procedure to select the spanning-tree protocol applied to the selected VLAN.

Step 1 Choose **Configure > Switching > STP > STP Configuration > STP Status**. The STP Status Summary Page opens.

Step 2 Choose the type of spanning-tree protocol from the **Spanning Tree Mode** drop-down menu. See STP Status Summary Page, page 82-3.

Step 3 Click **OK**. The Deliver Configure to Device dialog box opens.

Step 4 Click **Deliver** in the Deliver dialog box to deliver the configuration changes to the device.

Related Topic

- STP Status Reference, page 82-3

STP Status Reference

This section describes the summary page that you can use when working with STP Status and includes following topic:

- STP Status Summary Page, page 82-3

STP Status Summary Page

Use this page to select the spanning-tree protocol that is globally applied to all the VLANs, using Cisco CP.

How to Get to This Page

1. Choose **Configure > Switching > STP > STP Configuration**.
2. Choose **STP Status**.

Related Topics

- Bridge Parameters, page 82-5
- Port Parameters, page 82-9

Field Reference

Table 82-1 STP Status Summary Page

Field	Description
Spanning Tree Mode	Choose one of the following type of spanning-tree protocol from the drop-down menu: • rapid-pvst • pvst
Apply button	Click this button to apply the changes to the device.

Bridge Parameters

This section describes the spanning-tree bridge parameters for the selected switch and includes the following topics:

- Bridge Parameters Reference, page 82-6
- Edit STP Bridge Parameters Dialog Box, page 82-7

To Edit the STP Bridge Parameters

Procedure

Use this procedure to edit the STP Bridge Parameters.

Step 1 Choose **Configure > Switching > STP > STP Configuration > Bridge Parameters**. The Bridge Parameter Summary Page opens. See Bridge Parameters Summary Page, page 82-6.

Step 2 Select the VLAN ID from the Bridge Parameter summary page to edit the parameters, and click **Edit**. The Edit STP Bridge Parameters dialog box opens. See Edit STP Bridge Parameters Dialog Box, page 82-7 for more information.

Step 3 The **VLAN ID** field displays the selected VLAN ID.

Step 4 Choose the priority from 0 to 61440 from the **Priority** drop-down menu. The default priority number is 32768. See Edit STP Bridge Parameters Dialog Box, page 82-7 for more information.

Step 5 Enter the time in seconds from 6 to 40 in the **Max Age** field. See Edit STP Bridge Parameters Dialog Box, page 82-7 for more information.

Step 6 Enter the hello time in seconds from 1 to 10 in the **Hello Time** field. See Edit STP Bridge Parameters Dialog Box, page 82-7 for more information.

Step 7 Enter the time in seconds from 4 to 30 in the **Forward Delay** field that a port waits for the specified time before changing from its STP learning and listening states to the forwarding state. See Edit STP Bridge Parameters Dialog Box, page 82-7 for more information.

Step 8 Click **OK**. The Deliver Configure to Device dialog box opens.

Step 9 Click **Deliver** in the Deliver dialog box to deliver the configuration changes to the device.

Related Topic

- Bridge Parameters Reference, page 82-6

Bridge Parameters Reference

This section describes the summary page and dialog box you can use when working with Bridge Parameters and includes the following topics:

- Bridge Parameters Summary Page, page 82-6
- Edit STP Bridge Parameters Dialog Box, page 82-7

Bridge Parameters Summary Page

Use this page to view the VLAN parameters, or to edit the existing parameters for the selected switch.

How to Get to This Page

1. Choose **Configure > Switching > STP > STP Configuration**.
2. Choose **Bridge Parameters**.

Related Topic

- Edit STP Bridge Parameters Dialog Box, page 82-7

Field Reference

Table 82-2 Bridge Parameters Summary page

Field	Description
VLAN ID	Displays the VLAN to which these root settings apply.
Protocol	Displays the protocol used on the VLAN: IEEE (pvst), or RSTP.

Table 82-2 Bridge Parameters Summary page (continued)

Field	Description
Priority	Displays the priority value of the switch. The switch with the lowest value has the highest priority and is selected as the root. See Edit STP Bridge Parameters Dialog Box, page 82-7 for more information.
Max Age	Displays the number of seconds that a switch waits without receiving STP configuration messages before it attempts a reconfiguration. See Edit STP Bridge Parameters Dialog Box, page 82-7 for more information.
Hello Time	Displays the number of seconds between STP configuration messages. See Edit STP Bridge Parameters Dialog Box, page 82-7 for more information.
Forward Delay	Displays the number of seconds that a port waits before changing from its STP learning and listening states to the forwarding state. This delay in time ensures that no loop is formed before the switch forwards a packet. See Edit STP Bridge Parameters Dialog Box, page 82-7 for more information.
Edit button	Edits the parameters for the selected VLAN.

Edit STP Bridge Parameters Dialog Box

Use this dialog box to edit the STP Bridge parameters on the selected VLAN using Cisco CP.

How to Get to This Page

1. Choose **Configure > Switching > STP > STP Configuration**.
2. Choose **Bridge Parameters**.
3. Click **Edit**.

Related Topic

- Bridge Parameters Summary Page, page 82-6

Field Reference

Table 82-3 Edit STP Bridge Parameters—Dialog Box

Fields	Description
VLAN ID	Displays the selected VLAN ID.
Priority	The lowest value has the highest priority and is selected as the root switch. Choose the priority from the Priority drop-down menu in the range from 0 to 61440. **Note** The default priority is 32768.
Max Age (6-40)	Enter the number of seconds in the range from 6 to 40 that a switch waits without receiving STP configuration messages, before it attempts a reconfiguration. **Note** The default Max Age is 20 seconds.
Hello Time (1-10 Seconds)	Enter the number of seconds between STP configuration messages in the range from 1 to 10. **Note** The default Hello Time is 2seconds.
Forward Delay (4-30)	Enter the number of seconds from 4 to 30, that a port waits before changing from its STP learning and listening states to the forwarding state. This delay time ensures that no loop is formed before the switch forwards a packet. The default Forward Delay is 15 seconds.
OK button	Click this button to save the changes.
Cancel button	Click this button to avoid saving the changes that you entered.

Port Parameters

The section describes the spanning-tree port parameters and the usage of Bridge Protocol Data Unit guard (BPDU).

The port parameters serves the following purpose:

- Controls Bridge Protocol Data Unit guard (BPDU). BPDU guard prevents ports with Port Fast enabled from influencing STP topology in undesirable ways.
- Displays the list of parameters for VLAN ports on the switch. These parameters affect how the port responds if a loop is formed.

Related Topics

- Port Parameters Reference, page 82-11
- Edit STP Port Parameters Dialog Box, page 82-12

To Enable BPDU Guard

Procedure

Use this procedure to enable or disable the BPDU Guard globally on the ports.

Step 1 Choose **Configure > Switching > STP > STP Configuration > Port Parameters**. The Port Parameter Summary Page opens. See Port Parameters Summary Page, page 82-11.

Step 2 Check the BPDU Guard check box to enable or disable the Bridge Protocol Data Unit guard on the port globally.

Step 3 Click **Apply**. The Deliver Configure to Device dialog box opens.

Step 4 Click **Deliver** in the Deliver dialog box to deliver the configuration changes to the device.

Related Topics

- To Edit the STP Port Parameters, page 82-10
- Port Parameters Reference, page 82-11

To Edit the STP Port Parameters

Procedure

Use this procedure to edit the parameters of the STP Port Parameters.

Step 1 Choose **Configure > Switching > STP > STP Configuration > Port Parameters**. The Port Parameter Summary Page opens. See Port Parameters Summary Page, page 82-11.

Step 2 Select the port from the Port Parameter summary page, and click **Edit**. The Edit STP Port Parameters dialog box opens. See Edit STP Port Parameters Dialog Box, page 82-12 for more information.

Step 3 The **Port** field displays the selected port name. See Edit STP Port Parameters Dialog Box, page 82-12 for more information.

Step 4 Choose **Enable** from the **Port Fast** drop-down menu to enable the port fast on the selected port. Otherwise, choose **Disable**. See Edit STP Port Parameters Dialog Box, page 82-12 for more information.

Step 5 Enter the path cost in the range from 1 to 200000000 in the **Path Cost** field. See Edit STP Port Parameters Dialog Box, page 82-12 for more information.

Step 6 Choose the priority from 0 to 240 from the Priority drop-down menu. See Edit STP Port Parameters Dialog Box, page 82-12 for more information.

Step 7 Click **OK**. The Deliver Configure to Device dialog box opens.

Step 8 Click **Deliver** in the Deliver dialog box to deliver the configuration changes to the device.

Related Topic

- Port Parameters Reference, page 82-11

Port Parameters Reference

This section describes the summary page and dialog box you can use when working with Port Parameters and includes the following topics:

- Port Parameters Summary Page, page 82-11
- Edit STP Port Parameters Dialog Box, page 82-12

Port Parameters Summary Page

Use this Port Parameters summary page to view the list of parameters for VLAN port, to enable the BPDU guard, and to edit the port parameters for the selected VLAN.

How to Get to This Page

1. Choose **Configure > Switching > STP > STP Configuration**.
2. Choose **Port Parameters**.

Related Topic

- Edit STP Port Parameters Dialog Box, page 82-12

Field Reference

Table 82-4 Port Parameters Summary Page

Filed	Description
Enable BPDU Guard	Check this check box to enable the BPDU guard, and click **Apply**.
VLAN ID	Choose the VLAN ID from the VLAN ID drop-down menu.
Port	Identifies the ports in the selected VLAN ID: Fast Ethernet, Gigabit Ethernet, the module or slot number (0, 1, or 2), and the port number.

Table 82-4 Port Parameters Summary Page (continued)

Filed	Description
State	Displays several states in which ports exist. The port role and port state appears when the switch is in PVST+ or rapid PVST+ mode. See Port State Tables, page 82-14 for information on Port State and Port Role.
Port Fast	Port Fast immediately brings a port from the blocking state into the forwarding state by eliminating the forward delay (the amount of time a port waits before changing from its STP learning and listening states to the forwarding state). Displays one of the following status of Port Fast: • Enable • Disable
Path Cost	Displays the weight assigned to a port based on its speed. A lower path cost represents higher-speed transmission.
Priority	Displays the weight assigned to a port to affect its selection to carry traffic.
Apply button	Applies the changes to the configuration.
Edit button	Edits the parameters for the selected port.

Edit STP Port Parameters Dialog Box

Use this dialog box to edit the STP Port Parameters on the selected port using Cisco CP.

How to Get to This Page

1. Choose **Configure > Switching > STP > STP Configuration**.
2. Choose **Port Parameters**.
3. Click **Edit**.

Related Topics

- Port Parameters Summary Page, page 82-11
- Port Role, page 82-15

Field Reference

Table 82-5 Edit Port Parameters Dialog Box

Field	Description
Port	Displays the name of the selected interface.
Port Fast	Enable or disable the Port Fast on the selected port. Choose one of the following form the Port Fast drop-down menu: • Disable • Enable **Note** Choose to **enable** it, only for static-access ports or for both static-access and trunk ports.
Path Cost (1-200000000)	Enter the Path Cost in the range from 1 to 200000000. **Note** A lower path cost represents higher-speed transmission.
Priority	Choose the priority number from 0 to 240 from the Priority drop-down menu. **Note** The lowest number has the highest priority and the default for all the protocols is 128.
OK button	Click this button to save the changes.
Cancel button	Click this button to avoid saving the changes that you entered.

Port State Tables

Table 82-6 lists one of the port state if the switch is in the PVST+ mode.

Table 82-6 Port State Table—PVST+ mode

State	Description
Blocking	The port does not participate in the frame-forwarding process and will not learn new addresses.
Listening	The port does not participate in the frame-forwarding process and will not learn new addresses, but will progress toward a forwarding state.
Learning	The port does not forwards frames but will learn the addresses.
Forwarding	The port forwards frames and learn addresses.
Disabled	The port is disabled and has been removed from STP operation.
Down	The port has no physical link.
Broken	One end of the link is configured as an access port and the other end is configured as an 802.1Q trunk port, or both ends of the link are configured as 802.1Q trunk ports but have different native VLAN IDs.

Table 82-7 list the one of the port state if the switch is in the rapid-PVST+ mode.

Table 82-7 Port State Table—Rapid-PVST+ mode

State	Description
Discarding	The port does not participate in the frame-forwarding process and will not learn new addresses.
Learning	The port does not forwards frames but will learn addresses.
Forwarding	The port forwards frames and learns addresses.

Port Role

Table 82-8 lists one of the port role with the port state, if the switch is in the rapid-PVST+ mode.

Table 82-8 Port Parameters—Port Role

Role	Description
Root Port	A root port provides a path to the root bridge.
Designated Port	A forwarding port elected for every switched LAN segment.
Alternate Port	A blocked port providing an alternate path to the root port in the spanning tree.
Backup Port	A backup port providing a backup path for the designated port.

CHAPTER 83

STP Monitor

Spanning-Tree Protocol (STP) is a Layer2 link management protocol that provides path redundancy and prevents loops in the network. In a Layer-2 Ethernet network, only one active path can exist between any two stations. Multiple active paths among end stations cause loops in the network. If a loop exists in the network, the end stations might receive duplicate messages that results in an unstable network.

Note This feature is supported only on Cisco 2520 series switches.

The STP Monitor feature performs the following functions:

- Displays the spanning-tree protocols: per-VLAN spanning-tree plus (PVST+) or rapid-PVST+
- Enables or disables STP for each VLAN on the switch.

Note Disable STP only if you are sure that there are no loops in the network topology. If STP is disabled and loops are present in the topology, network performance is degraded by excessive traffic and indefinite packet duplication occurs.

Related Topics

- STP Status, page 83-2
- Current Roots, page 83-6

STP Status

The STP Status is a monitoring feature that allows you to enable or disable the STP on the VLAN and includes the following topics:

- Enable or Disable STP on a VLAN, page 83-2
- STP Status Reference, page 83-3

Enable or Disable STP on a VLAN

Procedure

Use this procedure to enable, or disable the STP on the selected VLAN.

Step 1 Choose **Configure > Switching > STP > STP Monitor > STP Status**. See STP Status Summary Page, page 83-3 for more information.

Step 2 To enable STP on a VLAN, do the following:

a. Choose the VLAN ID from the STP Status Summary Page. See STP Status Summary Page, page 83-3, page 83-3 for more information.

b. Click **Edit**. The Edit STP Status window opens. See Edit STP Status Dialog Box, page 83-4 for more information. In the Edit STP Status window, the selected VLAN ID is displayed in the **VLAN ID** filed.

c. Select **enable** from the Spanning-Tree Status drop-down menu to enable the STP on the selected VLAN ID. See Edit STP Status Dialog Box, page 83-4 for more information.

d. Click **OK**. The Deliver Configure to Device dialog box opens.

e. Click **Deliver** in the Deliver dialog box to deliver the configuration changes to the device.

Step 3 To disable STP on a VLAN, do the following:

a. Choose the VLAN ID from the STP Status Summary Page. See STP Status Summary Page, page 83-3, page 83-3 for more information.

b. Click **Edit**. The Edit STP Status window opens. See Edit STP Status Dialog Box, page 83-4 for more information. In the Edit STP Status window, the selected VLAN ID is displayed in the **VLAN ID** filed.

c. Select **disable** from the Spanning-Tree Status drop-down menu to disable the STP on the selected VLAN ID. See Edit STP Status Dialog Box, page 83-4 for more information.

d. Click **OK**. The Deliver Configure to Device dialog box opens.

e. Click **Deliver** in the Deliver dialog box to deliver the configuration changes to the device.

Related Topic

- STP Status Reference, page 83-3

STP Status Reference

This section describes the summary page and the dialog box you can use when working with STP Status and includes the following topics:

- STP Status Summary Page, page 83-3
- Edit STP Status Dialog Box, page 83-4

STP Status Summary Page

Use this page to view the STP operational mode, or VLAN status on the selected VLAN.

How to Get to This Page

Choose **Configure > Switching > STP > STP Monitor > STP Status**.

Related Topics

- Enable or Disable STP on a VLAN, page 83-2
- Edit STP Status Dialog Box, page 83-4

Field Reference

Table 83-1 Cisco CP —STP Status Summary Page

Elements	Description
VLAN ID	Displays the VLAN ID configured in the switch.
Spanning-Tree Status	Displays the status of STP on the VLANs. Displays one of the following status: • Enable • Disable
Edit	Edits the status for the selected VLAN.

Edit STP Status Dialog Box

Use this dialog box to modify the STP status to enable, or disable on the selected VLAN.

How to Get to This Page

1. Choose **Configure > Switching > STP > STP Monitor > STP Status**.
2. Click **Edit**.

Related Topics

- Enable or Disable STP on a VLAN, page 83-2
- STP Status Summary Page, page 83-3, page 83-3

Field Reference

Table 83-2 Edit STP Status Dialog Box

Element	Description
VLAN ID	Displays the selected VLAN ID.
Spanning-Tree Status	Choose one of the following from the **Spanning-tree Status** drop-down menu: • **Enable**—Enable the STP configuration on the selected VLAN ID. • **Disable**—Disables the STP configuration on the selected VLAN ID.
OK button	Click this button to save the configuration.
Cancel button	Click this button to avoid saving the changes that you entered.

Current Roots

The Current Root page displays the STP settings on the current root switch for each VLAN. These settings, define the parameters that take effect when the switch acts as the VLAN root. This page is not editable.

How to get to This Page

Choose **Configure > Switching > STP > STP Monitor > Current Roots**.

Related Topics

- Refreshing the Current Roots Page, page 83-6
- Current Roots Reference, page 83-7

Refreshing the Current Roots Page

Procedure

Use this procedure to refresh the page.

Step 1 Choose **Configure > Switching > STP > STP Monitor > Current Roots**.

Step 2 Click **Refresh**. The page refreshes and updates the STP settings on each VLAN.

Related Topic

- Current Roots Reference, page 83-7

Current Roots Reference

This section describes the summary page that you can use when working with Current Roots and includes the following topic:

- Current Roots Summary Page, page 83-7

Current Roots Summary Page

Use this page to view the STP settings on each VLAN. Table 83-3 defines the parameters that takes the effect when a switch is acting as the root.

How to Get to This Page

Choose **Configure > Switching > STP > STP Monitor > Current Roots**.

Field Reference

Table 83-3 Cisco CP—Current Roots Summary Page

Element	Description
VLAN ID	Displays the VLAN to which STP settings are applied.
MAC Address	Displays the MAC address of the root switch.
Priority	Identifies the root bridge. **Note** The switch with the lowest value, has the highest priority and is selected as the root. The default is 32768.
Max Age	Displays the number of seconds that a switch waits without receiving STP configuration messages, before it attempts a re-configuration.
Hello Time	Displays the number of seconds between STP configuration messages. The default is 2 seconds.
Forwarded Delay	Displays the number of seconds that a port waits before changing from STP learning and listening states to the forwarding state. This delay time ensures that, no loop is formed before the switch forwards a packet.
Root Path Cost	Displays a relative measure that determines the most favorable path to the destination.

Table 83-3 Cisco CP—Current Roots Summary Page (continued)

Element	Description
Root Port	Displays the port to which the settings are applied.
Root Bridge	Displays the status of the root of STP for the VLAN. Displays one of the following: • **Yes**—If the switch is actually the root of STP for the VLAN. • **No**—If the switch is not the root of STP for the VLAN. **Note** The device root port is listed in the Root Port column.
Refresh button	Refreshes the page.

CHAPTER 84

REP

A *Resilient Ethernet Protocol* (REP) segment is a set of inter-connected ports and configured with a segment ID. Each segment consists of standard (non-edge) segment ports and two user-configured edge ports. A switch cannot have more than two ports that belong to the same segment, and each segment port can have only one external neighbor. A segment can go through a shared medium on any link, but only two ports can belong to the same segment. REP is supported only on Layer 2 trunk interface.

Note This feature is supported only on Cisco 2520 series switches.

This section contains following topic:

- Configuring REP, page 84-2

Configuring REP

A segment is a collection of inter-connected ports and configured with a segment ID. To configure REP segments, you should configure the REP administrative VLAN (or use the default VLAN 1) and then add the ports to the segment using interface configuration mode. Every segment should be configured with edge ports, wherein one of them is the primary edge port and the other, by default is the secondary edge port. A segment has a single primary edge port only. If two ports in a segment are configured as the primary edge port, that is., ports on different switches, the REP selects one of them to serve as the segment primary edge port. Optionally you can also configure where to send Segment Topology Change Notices (STCNs).

For more information on Configuring REP, see:

http://www.cisco.com/en/US/docs/switches/connectedgrid/cgs2520/software/release/12_2_53_ex/configuration/guide/swrep.html

Characteristics of REP segment

The characteristics of the REP segment are as follows:

- If all ports in the segment are operational, one port (referred to as the alternate port) is in the blocked state for each VLAN.
- If one or more ports in a segment is not operational, or causing a link failure, all ports forward traffic on all VLANs to ensure connectivity.
- In case of a link failure, the alternate ports are unblocked as quickly as possible. When the failed link comes back up, a logically blocked port per VLAN is selected with minimal disruption to the network.

Limitations of REP segments

The limitation of the REP segment are as follows:

- Each segment port must be configured. An incorrect configuration can cause forwarding loops in the networks.
- REP can manage only a single failed port within the segment; multiple port failures within the REP segment cause loss of network connectivity.

- REP must be configured only in networks with redundancy. Configuring REP in a network without redundancy causes loss of connectivity.

Related Topics

- Create, Edit, or Delete REP Segment, page 84-4
- REP Reference, page 84-6

Create, Edit, or Delete REP Segment

Procedure

Use this procedure to create, edit, and delete a REP Segment using Cisco CP.

Step 1 Choose **Configure > Switching > STP > REP**. The REP Summary page opens. See REP Summary Page, page 84-6 for more information.

Step 2 Choose the administrative VLAN from the REP Admin VLAN drop-down menu.

Step 3 To create a new REP Segment, do the following:

a. Click **Create**. The Create REP Segment page opens. See Create or Edit REP Segment Dialog Box, page 84-7 for more information.

b. Enter the segment ID with a range from 1 to 1024, in the **Segment ID** field.

c. Choose the interface from the REP Port drop-down menu for the First Port of the REP Segment. See Create or Edit REP Segment Dialog Box, page 84-7 for more information.

d. Click **Yes** if the selected interface is one of the edge port for the REP Segment in the Is this Edge port for REP Segment field. Otherwise, click **No**.

e. Click **Yes** if the selected interface has to be alternate port in the **I**s this preferred alternate port for REP Segment field. Otherwise, click **No**.

On selecting **Yes** in the Is this Edge port for REP Segment field, following information must be entered. See Create or Edit REP Segment Dialog Box, page 84-7 for more information.

- Click **Yes**, if the selected interface has to be the primary edge port in the **Is this primary edge port for REP Segment** field. Otherwise, click **No**.
- Click **Yes**, if the selected interface has no neighbor edge port in the **Is this no neighbor edge port for REP Segment** field. Otherwise, click **No** if the selected interface has a neighbor edge port.

f. Choose the interface from the **STCN Interface** drop-down menu to receive the STCN of the REP segment. Otherwise, choose **None**.

g. Enter a segment ID or group of segment IDs in the **STCN Segments** field to receive the STCN of the REP segment.

h. Click **Yes**, to send the STCN messages to STP in the **Send STCN to STP** field. Otherwise, click **No**.

i. Likewise, choose the interface from the **REP Port** drop-down menu for the Second Port of the REP Segment (Optional). See Create or Edit REP Segment Dialog Box, page 84-7 for more information.

Note The second REP port cannot have the same interface as the first REP port.

j. Repeat the procedure from steps d.to h., and click **OK**. The Deliver Configure to Device dialog box opens.

k. Click **Deliver** in the Deliver dialog box to deliver the configuration changes to the device.

Step 4 To edit the existing REP Segment, do the following:

a. Select a REP Segment from the REP Summary page, and click **Edit**. See REP Summary Page, page 84-6 for more information. The dialog box having the same fields as the Create REP Segment opens. However, the fields show the parameters that were entered for the create REP Segment. See Create or Edit REP Segment Dialog Box, page 84-7 for more information.

b. Edit the REP Segment parameters such as Segment ID, First Port parameters, and Second Port parameters.

c. Click **OK**. The Deliver Configure to Device dialog box opens.

d. Click **Deliver** in the Deliver dialog box to deliver the configuration changes to the device.

Step 5 To delete a REP Segment, do the following:

a. Choose the REP Segment ID from the REP Summary page, and click **Delete**. See REP Summary Page, page 84-6 for more information. A confirmation dialog box opens.

b. Click **Yes** in the confirmation dialog box. The Deliver Configure to Device dialog box opens.

c. Click **Deliver** in the Deliver dialog box to deliver the configuration changes to the device.

Related Topic

- REP Reference, page 84-6

REP Reference

This section describes the pages and dialog boxes you can use when working with REP, and includes the following topics:

- REP Summary Page, page 84-6
- Create or Edit REP Segment Dialog Box, page 84-7

REP Summary Page

Use this summary page to view the configured REP, create new REP segment, modify parameters of the selected REP segment, and delete REP using Cisco CP.

How to Get to This Page

Choose **Configure > Switching > STP > REP**.

Related Topic

- Create or Edit REP Segment Dialog Box, page 84-7

Field Reference

Table 84-1 REP Segment Summary Page

Element	Description
REP Admin VLAN	Choose the administrative VLAN from the **REP Admin VLAN** drop-down menu.
REP Segment ID	Displays the REP Segments ID.
First Port	Displays the primary edge port of the segment.
First Port REP Type	Displays the type of First REP port. Displays one of the following status: • **Transit**—Displays if the REP ports are not edge ports. These ports are intermediate point of the REP ring and not at the edge ports of the REP segment. • **Edge**—Displays if the REP ports is edge port either with primary, or alternative, or no neighbor port.

Table 84-1 REP Segment Summary Page (continued)

Element	Description
Second Port	Displays the secondary (or alternative) edge port of the segment.
Second Port REP Type	Displays the type of Second REP port. Displays one of the following: • **Transit**—Displays if the REP ports are not edge ports. These ports are intermediate point of the REP ring and not at the edge ports of the REP segment. • **Edge**—Displays if the REP ports is edge port either with primary, or alternative, or no neighbor port.
Create button	Create this button to create a new REP segment.
Edit button	Click this button to modify the existing REP segment.
Delete button	Click this button to delete the selected REP segment.

Create or Edit REP Segment Dialog Box

Use the Create or Edit REP segment dialog box to create a new REP Segment or modify the parameters of the existing REP Segment.

How to Get to This Page

- Choose **Configure > Switching > STP > REP**.
- Click **Create** to create a new REP Segment.
- Click **Edit** to modify the existing REP Segment.

Field Reference

Table 84-2 Create or Edit REP Segment—Dialog Box

Element	Description
Segment ID	Enter the segment ID, with a range from 1 to 1024, for the REP topology.
First Port	
REP Port	Enables REP on the port and identifies a segment number. Choose the first port from the REP port drop-down menu. The segment ID range is from 1 to 1024.
Is this Edge port for REP Segment	Each segment must have two edge ports, including one primary edge port. Select one of the following option: • **Yes**—To choose this REP Port as the Edge Port for the REP Segment. • **No**—To not choose this REP Port as the Edge Port for the Segment.
Is this preferred alternate port for REP Segment	Select one of the following option: • **Yes**—To choose this REP Port as the preferred alternative port for the REP Segment. • **No**—To not choose this REP Port as the preferred alternative port for the REP Segment.
Is this primary edge port for REP Segment	Select one of the following option: • **Yes**—Explicitly assign the selected REP port as the primary edge port for the REP Segment • **No**—Do not assign the selected REP Port as the primary edge port for the REP Segment.
Is this no neighbor edge port for REP Segment	Select one of the following option: • **Yes**—The selected REP port has no neighbor in the REP segment. • **No**—There is a neighbor in the REP segment.

Table 84-2 Create or Edit REP Segment—Dialog Box (continued)

Element	Description
Send Segment Topology Change Notification (STCN) to: Any change in the topology, for example a link failure, notification can be sent to the selected interface or to the segment.	
STCN Interface	Choose the interface from the STCN drop-down menu to receive notifications of any changes on the selected interface topology.
STCN Segments	Enter the STCN segment ID for first port.
Send STCN to STP	Select one of the following options: • **Yes**—To send the segment topology change notification to STP network. • **No**—Restrict to send the segment topology change notification to STP network.
Second Port	
REP Port	Enables REP on the interface, and identify a segment number. Choose the second port from the REP port drop-down menu. The segment ID range is from 1 to 1024. **Note** The first port and second port cannot have the same REP port or interface.
Is this Edge port for REP Segment	Each segment must have two edge ports, including one primary edge port. Select one of the following option: • **Yes**—To choose this REP Port as the Edge Port for the REP Segment. • **No**—To not choose this REP Port as the Edge Port for the Segment.
Is this preferred alternate port for REP Segment	Select one of the following option: • **Yes**—To choose this REP Port as the preferred alternative port for the REP Segment. • **No**—To not choose this REP Port as the preferred alternative port for the REP Segment.

Table 84-2 Create or Edit REP Segment—Dialog Box (continued)

Element	Description
Is this primary edge port for REP Segment	Select one of the following option: • **Yes**—Explicitly assign the selected REP port as the primary edge port for the REP Segment • **No**—To not assign the selected REP Port as the primary edge port for the REP Segment.
Is this no neighbor edge port for REP Segment	Select one of the following option: • **Yes**—Selected REP port has no neighbor in the REP segment. • **No**—Neighbor in the REP segment.
Send Segment Topology Change Notification (STCN) to: Any change in the topology, example, a link failure notification can be sent to the selected interface or to the segment.	
STCN Interface	Choose the interface from the STCN drop-down menu to receive notifications of any changes on the selected interface topology.
STCN Segments	Enter the STCN segment ID for the second port.
Send STCN to STP	Select one of the following options: • **Yes**—To send the segment topology change notification to STP network. • **No**—Restrict to send the segment topology change notification to STP network.
OK button	Click this button to save the changes.
Cancel button	Click this button to avoid saving the changes that you entered.

Default REP Configuration

The default configuration for REP are as follows:

- REP is disabled on all interfaces. When enabled, the interface is a regular segment port unless it is configured as an edge port.
- When REP is enabled, the STCN is disabled, all VLANs are blocked, and the administrative VLAN is VLAN 1.

CHAPTER 85

Media Access Control Address

The Media Access Control (MAC) address table contains address information used by the switch to forward traffic between ports. All MAC addresses in the address table are associated with one or more ports.

MAC Addresses and VLANs

All MAC addresses are 48 bit and represented in a hexadecimal format, and are used basically in Layer 2.

All addresses are associated with a VLAN. An address can exist in more than one VLAN and have different destinations in each VLAN. It maintains its own logical address table.

A known address in a VLAN is unknown in another until it is learned or statically associated with a port in the other VLAN.

This section contains the following sections:

- Dynamic Address, page 85-2
- Aging, page 85-3
- Static Address Page, page 85-6
- Secure Address Page, page 85-9

Managing MAC Address

You can manage MAC addresses by managing the address tables in which a device stores dynamic addresses and static addresses. Cisco CP supports dynamic address learning and manual entering of static addresses.

Dynamic Address

Each device maintains a Dynamic Address table, which identifies ports and their associated addresses that belong to a VLAN.

The device learns the MAC address of attached devices, VLAN IDs, and interface numbers by reading the source address of arriving packets. It dynamically adds these addresses to the table and keeps table entries for the time specified in the Aging Time field. This is a read-only window.

Related Topics

- Refreshing and Removing All the MAC Address, page 85-2
- MAC Address Reference, page 85-2

Refreshing and Removing All the MAC Address

Procedure

Use this procedure to refresh and remove all the MAC addresses from the table.

Step 1 Choose **Monitor > Switching > MAC Address > Dynamic Address**.

Step 2 Click **Refresh**. The window refreshes and updates the MAC addresses.

Step 3 Click **Remove All** to clear the MAC addresses in the table.

Related Topic

- MAC Address Reference, page 85-2

MAC Address Reference

This section describes the MAC address summary page and includes the following topic:

- MAC address Summary Page, page 85-3

MAC address Summary Page

Use this page to view and delete all the MAC addresses from the table.

How to Get to This Page

Choose **Monitor > Switching > MAC Address > Dynamic Address**.

Field Reference

Table 85-1 Cisco CP - Dynamic Address window

Elements	Description
MAC Address	Displays the MAC address of a devices.
VLAN ID	Displays the VLAN ID configured on the output interface.
Output Interface	Displays the interface to where the received packets must be forwarded; that is, when the MAC address of the sender matches with the address in the MAC address column.
Refresh button	Refreshes the window.
Remove All button	Clears the table.

Aging

The Aging window is used to set or modify the aging time for VLANs, using Cisco CP.

How to Get to This Page

Choose **Monitor > Switching > MAC Address > Aging**.

Related Topic

- Guidelines on Changing the Address Aging Time, page 85-4
- Aging Reference, page 85-5

Guidelines on Changing the Address Aging Time

Dynamic addresses are source MAC addresses that the switch learns and then ages when they are not in use. You can change the aging time setting for all VLANs or for a specified VLAN.

The following are guidelines for setting the Aging time:

- Setting a short aging time can cause addresses to be prematurely removed from the table, and when the switch receives a packet for an unknown destination, it floods the packet to all ports in the same VLAN as the receiving port. This unnecessary flooding can affect performance.
- Setting a long aging time can cause the address table to be filled with unused addresses, which prevents new addresses from being learned.
- Flooding affects switch performance.

To Set Aging Parameters

Procedure

Use this procedure to set the Aging parameters for the VLAN.

Step 1 Choose **Monitor > Switching > MAC Address > Aging**. The Aging Summary page opens. See Aging Summary Page, page 85-5 for more information.

Step 2 Select the type of the VLAN to set the Aging time.

Step 3 Enter the VLAN ID from the VLAN drop-down menu.

Step 4 Select the **Enable Aging** check box to enable the Aging time for the specified VLAN.

Step 5 Enter or choose the aging time from 10 to 1000000 seconds (about 11.5 days) from the Aging Time drop-down menu. The default aging time is 300 seconds.

Step 6 To apply the aging time, do the following:

a. Click **Apply**. The Deliver Configuration to Device dialog box opens.

b. Click **Deliver** in the Deliver dialog box to apply the configuration changes to the device.

Related Topic

- Aging Reference, page 85-5

Aging Reference

This section describes the Aging summary page and includes the following topic:

- Aging Summary Page, page 85-5

Aging Summary Page

Use this page to set the Aging parameters on the selected VLAN.

How to Get to This Page

Choose **Monitor > Switching > MAC Address > Aging**.

Related Topic

- To Set Aging Parameters, page 85-4

Field Reference

Table 85-2 Cisco CP - Aging Window

Element	Description
Applicable VLAN	Click the required button to apply the aging on the VLAN: • **Single VLAN**—Enables aging on a single VLAN. **Note** Specify the VLAN ID in the VLAN column if Single VLAN aging is selected. • **All VLAN**—Enables aging on all the VLANs.
VLAN	Choose the VLAN ID from the drop-down menu for which aging time needs to be enabled.

Table 85-2 Cisco CP - Aging Window (continued)

Element	Description
Enable Aging (Default 300 seconds)	Click this button to enable aging on the selected VLAN(s).
Aging time (1 to1000000 seconds)	To set an aging time other than the 300-second default, select the aging time, in seconds from 10 to 1000000 (about 11.5 days).

Static Address Page

Use the Static Address page to add, modify, or remove static addresses.

A static address is entered manually in the address table and must be removed manually. Static addresses can be unicast or multicast. It does not age and is retained when the switch restarts.

Note Static Address feature is not support on the GRWIC-D-ES-2S and GRWIC-D-ES-6S switching modules.

How to Get to This Page:

Click **Configure > Switching > MAC Address > Static Address**.

Note Add a static address to the address table by specifying the destination MAC address (unicast or multicast) and the VLAN from which it is received. Packets received with this destination address are forwarded to the interface specified with the interface-id option.

Related Topics

- Create Static Address Dialog Box, page 85-8
- Edit Static Address Dialog Box, page 85-8
- Secure Address Page, page 85-9

Field Reference

Table 85-3 Static Address Page

Element	Description
MAC Address list	Displays the destination MAC address (unicast or multicast). Packets with a particular destination address received from the specified VLAN are forwarded to the specified interface.
VLAN ID list	Displays the VLAN from which the packet with the specified MAC address is received. Valid VLAN IDs are 1 to 4094.
Output Interface list	Displays the interface to which received packets are to be forwarded, this is when the MAC address of the sender matches with the address in the MAC address column.
Create button	Click **Create**. The Create Static Address dialog box is displayed. See the section Create Static Address Dialog Box, page 85-8
Edit button	Select a static address and click **Edit.** The Edit Static Address dialog box is displayed. See the section Edit Static Address Dialog Box, page 85-8
Delete button	Select a static address from the Static Address list and click **Delete** to delete it. You can remove multiple static addresses by selecting them and clicking **Delete**.

Create Static Address Dialog Box

Use the Create Static Address dialog box to add new static addresses.

Note Static Address feature is not support on the GRWIC-D-ES-2S and GRWIC-D-ES-6S switching modules.

How to Get to This Page

Choose **Configure > Switching > MAC Address > Static Address > Create**.

Related Topics

- Static Address Page, page 85-6
- Edit Static Address Dialog Box, page 85-8

Field Reference

Table 85-4 Create Static Address Dialog Box

Element	Description
MAC Address field	Enter the MAC address.
VLAN ID field	Enter the VLAN ID.
Output Interface drop-down list	Choose the output interface.
OK button	Click **OK** to add the MAC address. The new MAC address is displayed in the address table.
Cancel button	Click **Cancel** to undo your changes.

Edit Static Address Dialog Box

Use the Edit Static Address dialog box to edit static addresses.

Note Static Address feature is not support on the GRWIC-D-ES-2S and GRWIC-D-ES-6S switches.

How to Get to This Page

Choose **Configure > Switching > MAC Address > Static Address > Edit**.

Related Topics

- Static Address Page, page 85-6
- Create Static Address Dialog Box, page 85-8

Field Reference

Table 85-5 Edit Static Address Dialog Box

Element	Description
MAC Address field	Edit the values present.
VLAN ID field	Edit the VLAN ID given.
Output Interface drop-down list	Change the output interface chosen.
OK button	Click **OK** to add your changes. The modified entry is displayed in the address table.
Cancel button	Click **Cancel** to undo your changes.

Secure Address Page

Use the Secure Address page to view information about the secure MAC addresses configured on the device.

Secure MAC Address is used to ensure that safe addresses are included in the MAC address table.

Note Secure Address feature is not support on the GRWIC-D-ES-2S and GRWIC-D-ES-6S switches.

How to Get to This Page:

Click **Configure > Switching > MAC Address > Secure Address**.

Field Reference

Table 85-6 Secure MAC Address Page

Element	Description
MAC Address list	MAC address of a device that sends packets.
VLAN ID list	VLAN ID that is configured on the output interface.
Output Interface list	Interface to which received packets are to be forwarded if the MAC address of the sender matches the one in the MAC Address column.
Type list	Type of secure address; for example, Static.
Refresh button	Click the **Refresh** button to refresh the page.

CHAPTER 86

ACL

Access Control Lists (ACLs) consist of *Access List Elements* (ACEs), which are matched against a packet in sequence. An action in the ACE (*permit* or *deny)* determines whether the packets is forwarded or dropped. That is, a permitted packet is forwarded, and a denied packet is dropped. If no match is found, the packet is denied by default.

Layer 2 Filtering

Layer 2 filtering is done by an ACE of the MAC extended type. It can identify the following packets fields:

- Source MAC address of 48 bits.
- Destination MAC address of 48 bits.
- Ethertype—Two-octet field in an Ethernet frame. It is used to indicate which protocol is encapsulated in the payload of an Ethernet Frame.

Layer 3 Filtering

Layer 3 filtering is done by an ACE of the IP standard or IP extended type. Its mask identifies the following packet fields:

- IP source address. The Mask can be matched against the 32 bits of the address, or it can contain a wildcard that specifies the bits that it needs to be matched against.
- IP destination source address. Here too the mask can be matched against all or part of the address.
- DSCP, CoS, and IP Precedence values.

Layer 4 Filtering

IP extended ACEs can also filter based on Transmission Control Protocol (TCP), User Datagram Protocol (UDP), Internet Control Message Protocol (ICMP), and IP.

For TCP and UDP filtering, the mask can contain:

- A TCP source port number, destination port number.
- A UDP source port number, destination port number.
- Well-known application names in place of port numbers.

Related Topics

- Configuring ACL, page 86-2
- Attach ACL, page 86-29
- Time Range, page 86-33

For more information on Configuring ACL with Standard IP, Extended IP and MAC-Extended, see:

http://www.cisco.com/en/US/docs/switches/connectedgrid/cgs2520/software/release/12_2_53_ex/configuration/guide/swacl.html

Configuring ACL

Packet filtering limits network traffic and restricts network use by users or devices. ACL filters traffic as it passes through the switch and permits or denies packets crossing through specified interfaces.

Perform the following functions using Cisco CP.

- Create and delete ACLs.
- View and edit the ACL details.

Note In Cisco CP, the ACL is removed and recreated with an ACE (Access Control Elements) whenever an ACL is edited.

Related Topics

- Creating, Editing, and Deleting an ACL, page 86-3
- Access Control List Reference, page 86-5
- ACL with Standard IP, page 86-8
- ACL with Extended IP, page 86-13
- ACL with MAC Extended, page 86-25

Creating, Editing, and Deleting an ACL

Procedure

Use this procedure to create, edit, and delete an ACL. Multiple ACEs can be created or edited on a ACL.

Step 1 Choose **Configure > Switch > ACL**. The ACL Summary Page opens. See Access Control List Summary Page, page 86-5.

Step 2 To create an ACL, do the following:

a. Click **Create**. The Create ACL dialog box opens. See Create or Edit Access Control List Window, page 86-6 for more information.

b. Select Standard IP, Extended IP, or MAC Extended type from the ACL Type drop-down menu.

c. Enter the ACL name or number. See Create or Edit Access Control List Window, page 86-6 for more information.

d. Click **Create**. The Create ACE window opens. See Create or Edit Access Control List Window, page 86-6 for more information.

e. Enter the ACE parameters for an ACL, and click **OK**. The Deliver Configure to Device dialog box opens.

f. Click **Deliver** in the Deliver dialog box to deliver the configuration changes to the device.

Step 3 To edit an ACL, do the following:

a. Select the ACL from the ACL Summary Page, and click **Edit**. The Edit Access Control List window opens.

b. Click **Create** in the Edit ACL window to add more ACEs to the selected ACL. The Create ACE window opens. Enter the ACE parameters, and click **OK.** See Create or Edit ACE with Standard IP, page 86-11 for more information on the parameters.

c. In the Edit Access Control List window, select the required ACE from the Access Control Elements list to edit, and click **Edit**.

   The window that has the same fields as the Create ACE windows opens. However, the field shows the setting that were entered for the ACE.

d. Edit the parameters, and click **OK**. The Edit ACL window returns. See Create or Edit Access Control List Window, page 86-6.

e. Click **OK** to apply the changes to the configuration. The Deliver Configure to Device dialog box opens.

f. Click **Deliver** in the Deliver dialog box to deliver the configuration changes to the device.

Step 4 To delete an ACL, do the following:

a. Choose an ACL or multiple ACL rows to delete, and click **Delete**. A confirmation dialog box opens.

b. Click **Yes** in the confirmation dialog box.

Related Topics

- Access Control List Reference, page 86-5
- ACL with Standard IP, page 86-8
- ACL with Extended IP, page 86-13
- ACL with MAC Extended, page 86-25

Access Control List Reference

This section describes the pages and windows that you can use when working with configuring ACL and includes following topics:

- Access Control List Summary Page, page 86-5
- Create or Edit Access Control List Window, page 86-6

Access Control List Summary Page

Use this summary page to view, create, edit, and delete an ACL.

How to Get to This Page

Choose **Configure > Switch > ACL > Configure**.

Related Topic

- Create or Edit Access Control List Window, page 86-6

Field Reference

Table 86-1 Cisco CP—Access Control List Summary Page

Elements	Description
Access Control List Type	Displays the types of ACLs.
Access Control List Name	Displays the names associated to the particular ACL.
Create button	Creates an ACL. This is the first set of window that leads you through the creation process.
Edit button	Edits the ACL. You can create, edit, and delete the ACEs that make up the ACL.
Delete button	Deletes one or more ACL.

Create or Edit Access Control List Window

Use this window to create, or edit, an ACL using Cisco CP.

How to Get to This Page

- Choose **Configure > Switch > ACL > Configure > Create**.
- Choose **Configure > Switch > ACL > Configure > Edit**.

Related Topics

- Access Control Element, page 86-8
- ACL with Standard IP, page 86-8
- ACL with Extended IP, page 86-13
- ACL with MAC Extended, page 86-25
- Access Control List Summary Page, page 86-5

Field Reference

Table 86-2 Create or Edit an ACL window

Element	Description
ACL Type	Choose the ACL type from the drop-down menu. • **Standard IP**—Choose Standard IP type to block or allow packets based on their respective source IP address. • **Extended IP**—Choose Extended IP type to give finer control, over which IP packets are filtered and which are not. • **MAC Extended**—Choose MAC Extended type to block or allow packets based on their respective-source and destination MAC addresses.
ACL Name/Number	Enter a name or number to the ACL.
Access Control Entries	Display the lists of ACEs set for an ACL.
Create button	Creates ACE's for an ACL.
Edit button	Edits the selected ACE from the Access Control Elements.
Delete button	Deletes one or more ACEs from the Access Control Elements.

Table 86-2 Create or Edit an ACL window

Element	Description
Move Up button	Arranges the ACEs based on the required priority in the ACL. See Access Control Element, page 86-8 for more information.
Move Down button	Arranges the ACEs based on the required priority, in the ACL. See Access Control Element, page 86-8 for more information.
OK button	Click this button to save the changes.
Cancel button	Click this button to avoid saving the changes that you entered.

Access Control Element

ACE is a element in an ACL that matches the criteria and action (permit or deny). The action determines what happens to matching packets. Create an ACL by creating one or more ACEs for the ACL.

The order of an ACE is important because ACEs are evaluated sequentially in an ACL.

For example, consider an ACL with five ACEs. If the first ACE matches the criteria (permit or deny), it executes that ACE and exits. Otherwise, the control moves to the next ACE. If no ACE matches the criteria, the evaluation of an ACL exits.

ACL with Standard IP

Use this window to create, edit, and delete an ACE with standard IP, using Cisco CP.

How to Get to This Page

1. Choose **Configure > Switch > ACL > Configure > Create** or **Edit**.
2. Choose **Standard IP** from the ACL Type drop-down menu.
3. Click **Create** or **Edit**.

Related Topics

- Creating, Editing, and Deleting an ACE with Standard IP, page 86-9
- Create or Edit ACE with Standard IP, page 86-11

Creating, Editing, and Deleting an ACE with Standard IP

Procedure

Use this procedure to create, edit, and delete an ACE with standard IP.

Step 1 Choose **Configure > Switch > ACL > Configure > Create** or **Edit**. The Create or Edit Access Control List window opens. See Access Control List Summary Page, page 86-5 for more information.

Step 2 Select Standard IP type from the ACL Type drop-down menu from the Create or Edit Access Control List window.

Step 3 Enter the ACL name or number. See Create or Edit Access Control List Window, page 86-6 for more information.

Note The number must range from 1 to 99 or 1300 to 1999.

Step 4 To create an ACE with Standard IP, do the following:

a. Click **Create**. The Create Access Control Element with Standard IP window opens. See Create or Edit ACE with Standard IP, page 86-11 for more information.

b. Enter the ACE parameters such as, Keyword, Source Address, Source Wildcard, and Log.

c. Click **OK**. See Create or Edit ACE with Standard IP, page 86-11 for more information on parameters.

   The Create Access Control List window returns with the ACE parameters in the Access Control Elements list.

d. Click **OK**. The Deliver Configure to Device dialog box opens.

e. Click **Deliver** in the Deliver dialog box to deliver the configuration changes to the device.

Step 5 To edit an ACE with Standard IP, do the following:

a. Select an ACL from the Access Control List Summary page and click **Edit**.

b. Choose the required ACE from the **Access Control Elements** list, and click **Edit**.

The window that has the same fields as the Create ACE with Standard IP windows opens. However, the fields show the settings that were entered for the ACE. See Create or Edit ACE with Standard IP, page 86-11

c. Edit the ACE parameter for the selected ACL in the Edit ACE with Standard window, and click **OK**.You will be returned to the Edit Access Control List window.

d. Click **OK.** The Deliver Configuration to Device dialog box opens.

e. Click **Deliver** in the Deliver Configure to Device dialog box to deliver the configuration changes to the device.

Step 6 To delete an ACE, do the following:

a. Choose an ACE or multiple ACE rows, and click **Delete**. The Deliver Configure to Device dialog box opens.

Note Every ACL must have at least one ACE associated with it.

b. Click **Deliver** in the Deliver Configure to Device dialog box to deliver the configuration changes to the device.

Related Topics

- Create or Edit ACE with Standard IP, page 86-11
- Access Control List Summary Page, page 86-5
- Create or Edit Access Control List Window, page 86-6

Create or Edit ACE with Standard IP

Use this window to create, edit, or delete a ACEs for an ACL.

How to Get to This Page

1. Choose > **Configure > Switch > ACL > Configure > Create** or **Edit.**
2. Click **Create** to apply the criteria or action to new ACE for an ACL.
3. Click **Edit** to apply the criteria or action to existing ACE for an ACL.

Related Topics

- ACL with Standard IP, page 86-8
- Access Control List Summary Page, page 86-5
- Create or Edit Access Control List Window, page 86-6

Field Reference

Table 86-3 Create or Edit Access Control Element—Standard IP

Element	Description
KeyWord	Choose one of the following criteria by clicking on the respective radio button: • **Permit**—Permits traffic from specified sources. • **Deny**—Denies traffic from those sources.
Source Address	Enter the source IP address.

Table 86-3 Create or Edit Access Control Element—Standard IP (continued)

Element	Description
Source Wildcard	Choose one of the following options from the drop-down menu: • A mask. **Note** **A mask** is a wildcard mask—The high-order bits of the mask that are binary zeros determine how many corresponding high-order bits in the IP address are significant. The selected action applies to any source address with these high-order bits • **Host**—Applies the selected action only to the source address. **Note** **Host** is equivalent to specifying a mask of 0.0.0.0. • **Any**—Applies the selected action to any source address. **Note** **Any** is equivalent to specifying a source address and mask of 255.255.255.255.
Log	Check the Log check box to send messages to the device for incoming and outgoing packets that match the ACL filtering criteria. Uncheck the Log check box to disable sending packet messages to the device.
OK button	Click this button to save the changes.
Cancel button	Click this button to avoid saving the changes that you entered.

ACL with Extended IP

Use this window to create, edit, and delete an ACE with extended IP, using Cisco CP.

How to Get to This Page

1. Choose **Configure > Switch > ACL > Configure > Create** or **Edit**.
2. Choose Extended IP from the ACL Type drop-down menu.
3. Click **Create** or **Edit**.

Related Topics

- Creating, Editing, and Deleting an ACE with Extended IP, page 86-13
- Create or Edit ACE with Extended IP, page 86-16

Creating, Editing, and Deleting an ACE with Extended IP

Procedure

Use this procedure to create, edit, and delete an ACE with extended IP.

Step 1 Choose **Configure > Switch > ACL > Configure > Create** or **Edit**. The Create or Edit Access Control List window opens. See Access Control List Summary Page, page 86-5 for more information.

Step 2 Select Extended IP type from the ACL Type drop-down menu from the Create or Edit Access Control List window.

Step 3 Enter the ACL name or number. See Create or Edit Access Control List Window, page 86-6 for more information.

Note The number must range from 100 to 199 or 2000 to 2699.

Step 4 To create an ACE with extended IP, do the following:

a. Click **Create**. The Create Access Control Element with Extended IP window opens. See Create or Edit ACE with Extended IP, page 86-16 for more information.

b. Select the ACE parameters such as, Action, Log, Source Host/Network, Destination Host/Network. See Create or Edit ACE with Extended IP, page 86-16 for more information on parameters.

c. Select the type of Protocol and Service: TCP, UDP, ICMP, and IP. See Create or Edit ACE with Extended IP, page 86-16 for more information on parameters.

d. If TCP or UDP is selected, select the appropriate operation from the Source port, and Destination port **Service** drop-down menu and the type of protocol from the Protocol List, and click **OK**. See Create or Edit ACE with Extended IP, page 86-16 and TCP Application and Port Number Table, page 86-21 for more information.

e. If ICMP or IP Protocol is selected, select the type of protocol from the Protocol List, and click **OK**. See Create or Edit ACE with Extended IP, page 86-16 for more information.You will be returned to the Create Extended Access Control Element window.

Note All the ACE parameters are listed in the Access Control Elements list.

f. Choose the type of precedence and type of service that describes the priority that you can assign to packets that meets the filtering criteria from the **Precedence** and **Type of Service** drop-down menu.

g. Choose the DSCP value from the **DSCP** drop-down menu if no selection is done from the **Precedence** and **Type of Service** list.

h. Choose the available time range from the **Time Range** drop-down menu.

i. Click **OK**. The Deliver Configure to Device dialog box opens.

j. Click **Deliver** in the Deliver dialog box to deliver the configuration changes to the device.

Step 5 To edit an ACE with extended IP, do the following:

a. Select an ACL from the Access Control List Summary page, and click **Edit**.

b. Choose the required ACE from the **Access Control Elements** list to edit, and click **Edit**.

   The window having the same fields as the Create Access Control Element with Extended IP windows opens. However, the fields show the settings that were entered for the ACE.

c. Edit the ACE parameters for the selected ACL in the Edit Extended Access Control Element window, and click **OK**. See Create or Edit ACE with Extended IP, page 86-16 and for more information. You will be returned to the Edit Access Control List window.

d. Choose the type of precedence and type of service that describes the priority that you can assign to packets that meets the filtering criteria from the **Precedence** and **Type of Service** drop-down menu.

e. Choose the DSCP value from the **DSCP** drop-down menu if no selection is done from the **Precedence** and **Type of Service** list.

f. Choose the available time range from the **Time Range** drop-down menu.

g. Click **OK**. The Deliver Configure to Device dialog box opens.

h. Click **Deliver** in the Deliver dialog box to deliver the configuration changes to the device.

Step 6 To delete an ACE with extended IP, do the following:

a. Choose an ACE or multiple ACE rows, and click **Delete**. The Deliver Configure to Device dialog box opens.

Note Every ACL must have at least one ACE associated with it.

b. Click **Deliver** in the Deliver Configure to Device dialog box to deliver the configuration changes to the device.

Related Topics

- Create or Edit ACE with Extended IP, page 86-16
- Access Control List Summary Page, page 86-5
- Create or Edit Access Control List Window, page 86-6

Create or Edit ACE with Extended IP

Use this window to create, edit, or delete ACE's for an ACL.

How to Get to This Page

1. Choose > **Configure > Switch > ACL > Configure > Create** or **Edit**.
2. Select Extended IP from the ACL Type.
3. Click **Create** or **Edit** to apply the criteria or action to new ACE or to edit the existing ACE for an ACL.

Related Topics

- ACL with Extended IP, page 86-13
- Access Control List Summary Page, page 86-5
- Create or Edit Access Control List Window, page 86-6

Field Reference

Table 86-4 Create or Edit Access Control Element—Extended IP

Elements	Description
Action	Choose one of the following option from the drop-down menu: • **Permit**—Permits traffic from specified sources. • **Deny**—Denies traffic from those sources.
Log	Choose one of the following option from the drop-down menu: • **Log—**Sends messages to the device for incoming and outgoing packets that match the ACL filtering criteria. • **No Logging**—Sends no packet messages to the device. • **log-input**— Sends messages to the console only for incoming packets that match the ACL filtering criteria.

Table 86-4 Create or Edit Access Control Element—Extended IP (continued)

Elements	Description
Source Host/Network	Enter the following source host/network information. • **Source Address**—Enter the source IP address. • **Source Wildcard**—Choose one of the following option from the drop-down menu: – A mask. **Note** **A mask** is a wildcard mask—The high-order bits of the mask that are binary zeros determine how many corresponding high-order bits in the IP address are significant. The selected action applies to any source address with these high-order bits. – **Host**—Applies the selected action only to the source address. **Note** **Host** is equivalent to specifying a mask of 0.0.0.0. – **Any**—Applies the selected action to any source address. **Note** **Any** is equivalent to specifying a source address and mask of 255.255.255.255.

Table 86-4 Create or Edit Access Control Element—Extended IP (continued)

Elements	Description
Destination Host/Network	Enter the following destination host/network information. • **Destination Address**—Enter the destination IP address. • **Destination Wildcard**—Choose one of the following option from the drop-down menu: – A mask. **Note** **A mask** is a wildcard mask—The high-order bits of the mask that are binary zeros determine how may corresponding high-order bits in the IP address are significant. The selected action applies to any source address with these high-order bits. – **Host**—Applies the selected action only to the source address. **Note** **Host** is equivalent to specifying a mask of 0.0.0.0. – **Any**—Applies the selected action to any source address. **Note** **Any** is equivalent to specifying a source address and mask of 255.255.255.255.
Protocol and Service	

Table 86-4 Create or Edit Access Control Element—Extended IP (continued)

Elements	Description
Select one of the following protocol that you are associating with the ACE.	1. **TCP**—Connection-oriented transport layer protocol that provides reliable full duplex data-transmission. • **Source Port (Rarely Changed)**: – **Service**—Select the type of operator from the drop-down menu. Select the type of protocol from the Protocol List. See Table 86-5 for information on protocols. • **Destination Port**: – **Service**—Select the type of operator from the drop-down menu. Enter the type of protocol or select it from the Protocol List. See Table 86-5 for information on protocols. 2. **UDP**—A User Datagram Protocol (UDP) is a simple protocol that exchanges datagram without acknowledgments or guaranteed delivery, requiring that error processing and retransmission be handled by other protocols. • **Source Port (Rarely Changed)**: – **Service**—Select the type of operator from the drop-down menu. Enter the type of protocol or select it from the protocol list. See Table 86-6 for more information. • **Destination Port**: – **Service**—Select the type of operator from the drop-down menu. Enter the type of protocol or select it from the Protocol List. See Table 86-6 for more information.

Table 86-4 Create or Edit Access Control Element—Extended IP (continued)

Elements	Description
	3. **ICMP**—Internet Control Message Protocol (ICMP) is network layer Internet protocol that reports errors and provides other information relevant to IP packet processing. • **ICMP Type**—Select the type of protocol from the Protocol List. 4. **IP**—Internet Protocol (IP) is a routed protocol that selects the best route to send the packets over the internet using routing protocol. • **IP Protocol**—Select the type of protocol from the Protocol List.
Precedence	Select an option from the **Precedence** drop-down menu that describes the priority you can assign to the packets that meets the filtering criteria.
Type of Service	Select the type of service from the **Type of Service** drop-down menu that you can assign to packets that meets the filtering criteria.
DSCP	Select the DSCP from the drop-down if no selection is made in the **Precedence** or **Type of Service** drop-down menus.
Time Range	Select a time range from the drop-down menu that defines the time when the ACE is active.
OK button	Click this button to save the changes.
Cancel button	Click this button to avoid saving the changes that you entered.

TCP Application and Port Number Table

Table 86-5 lists the TCP protocols and their corresponding port numbers.

Field Reference

Table 86-5 TCP Application and Port Number Table

Short Name	Long Name	Port Name
bgp	Border Gateway Protocol	179
chargen	Character generator	19
cmd	Remote commands	514
daytime	Daytime	13
discard	Discard	9
domain	Domain Name Service	53
echo	Echo	7
exec	Exec	512
finger	Finger	79
ftp	File Transfer Protocol	21
ftp-data	FTP data connections	20
gopher	Gopher	70
hostname	NIC hostname server	101
ident	Ident Protocol	113
irc	Internet Relay Chat	194
klogin	Kerberos login	543
kshell	Kerberos shell	544
login	Login	513
lpd	Printer service	515
nntp	Network News Transport Protocol	119
pim-auto-rp	PIM Auto-RP	496
pop2	Post Office Protocol v2	109

Table 86-5 TCP Application and Port Number Table (continued)

Short Name	Long Name	Port Name
pop3	Post Office Protocol v3	110
smtp	Simple Mail Transport Protocol	25
sunrpc	Sun Remote Procedure Call	111
tacacs	TAC Access Control System	49
talk	Talk	517
telnet	Telnet	23
time	Time	37
uucp	Unix-to-Unix Copy Program	540
whois	Nicname	43
www	World Wide Web	80

UDP Application and Port Number Table

Table 86-6 lists the UDP protocols, and their corresponding port numbers.

Field Reference

Table 86-6 UDP Application and Port Number Table

Short Name	Long Name	Port Number
biff	Biff	512
bootpc	Bootstrap Protocol (BOOTP) client	68
bootps	Bootstrap Protocol (BOOTP) server	67
discard	Discard	9
dnsix	DNSIX security protocol auditing	195
domain	Domain Name Service	53
echo	Echo	7
isakmp	Internet Security Association and Key Management Protocol	500
mobile-ip	Mobile IP registration	434
nameserver	IEN116 name service	42
netbios-dgm	NetBios datagram service	138
netbios-ns	NetBios name service	137
netbios-ss	NetBios session service	139
ntp	Network Time Protocol	123
pim-auto-rp	PIM Auto-RP	496
rip	Routing Information Protocol	520
snmp	Simple Network Management Protocol	161
snmptrap	SNMP Traps	162
sunrpc	Sun Remote Procedure Call	111
syslog	Syslog	514
tacacs	TAC Access Control System	49

Table 86-6 UDP Application and Port Number Table (continued)

Short Name	Long Name	Port Number
talk	Talk	517
tftp	Trivial File Transfer Protocol	69
time	Time	37
who	Who service	513
xdmcp	X Display Manager Control Protocol	177

ACL with MAC Extended

Use this window to create, edit, and delete an ACE with MAC Extended, using Cisco CP.

How to Get To This Page

1. Choose **Configure > Switch > ACL > Configure > Create** or **Edit**.
2. Choose **MAC Extended** from the ACL Type drop-down menu.
3. Click **Create** or **Edit**.

Related Topics

- Creating, Editing, and Deleting an ACE with MAC Extended, page 86-25
- Create or Edit ACE with MAC Extended, page 86-27

Creating, Editing, and Deleting an ACE with MAC Extended

Procedure

Use this procedure to create, edit, and delete an ACE with MAC Extended.

Step 1 Choose **Configure > Switch > ACL > Configure > Create** or **Edit**. The Create or Edit Access Control List window opens. See Access Control List Summary Page, page 86-5 for more information.

Step 2 Select MAC Extended from the ACL Type drop-down menu from the Create or Edit Access Control List window.

Step 3 Enter the ACL name. See Create or Edit ACE with MAC Extended, page 86-27 for more information.

Step 4 To create an ACE with MAC Extended, do the following:

a. Click **Create**. The Create Access control List with MAC Extended window opens. See Create or Edit ACE with MAC Extended, page 86-27 for more information.

b. Select the ACE parameters such as, KeyWords, Source MAC Address, Source Wildcard, Destination MAC Address, Destination Wildcard, CoS, Lsap, Ethertype, Others, and click **OK**. See Create or Edit ACE with MAC Extended, page 86-27 for more information.

Note Choose **other** from the Ethertype drop-down menu to enable **Other[0-65535]** field.

c. You will be returned to the Create Access Control List window. To save the ACE parameters in the Access Control Elements lists, and click **OK**. The Deliver Configure to Device dialog box opens.

d. Click **Deliver** in the Deliver dialog box to deliver the configuration changes to the device.

Step 5 To edit an ACE with MAC Extended, do the following:

a. Select an ACL with MAC Extended from the Access Control List Summary page, and click **Edit**.

b. Choose the required ACE from the Access Control Elements list to edit, and click **Edit**. The window having the same fields as the Create ACE with MAC Extended windows opens. However, the fields show the settings that were entered for the ACE. See Create or Edit ACE with MAC Extended, page 86-27 for more information.

c. Edit the ACE parameter for the selected ACL in the Edit ACE with MAC Extended window, and click **OK**. See Create or Edit ACE with MAC Extended, page 86-27 for more information.

d. You will be returned to the Edit Access Control List window. To save the ACE parameters in the Access Control Elements list, click **OK**. The Deliver Configure to Device dialog box opens.

e. Click **Deliver** in the Deliver dialog box to deliver the configuration changes to the device.

Step 6 To delete an ACE with MAC Extended, do the following:

a. Choose an ACE or multiple ACE rows from the Access Control Elements list, and click **Delete**. The Deliver Configure to Device dialog box opens.

Note Every ACL must have at least one ACE associated with it.

b. Click **Deliver** in the Deliver Configure to Device dialog box to deliver the configuration changes to the device.

Related Topics

- Create or Edit ACE with MAC Extended, page 86-27
- Access Control List Summary Page, page 86-5
- Create or Edit Access Control List Window, page 86-6

Create or Edit ACE with MAC Extended

Use this window to create, edit, or delete ACE's for an ACL.

How to Get to This Page

1. Choose > **Configure > Switch > ACL > Configure > Create** or **Edit**.
2. Select MAC Extended from the ACL Type.
3. Click **Create** or **Edit** to set the criteria or action to new ACE or to edit the existing ACE for an ACL.

Related Topics

- ACL with MAC Extended, page 86-25
- Access Control List Summary Page, page 86-5
- Create or Edit Access Control List Window, page 86-6

Field Reference

Table 86-7 Create or Edit Access Control Element—MAC Extended

Element	Description
KeyWord	Choose one of the following action from the drop-down menu: • **Permit**—Permits traffic from specified MAC address sources and to specified MAC address destinations. • **Deny**—Denies traffic from those sources and to those destinations
Source MAC Address	Enter a source MAC address.

Table 86-7 Create or Edit Access Control Element—MAC Extended (continued)

Element	Description
Source Wildcard	Specify a MAC address filter. Choose one of the following filter from the drop-down menu: • **Host**—Designates to a particular source MAC address. • **0000.00ff.ffff**—Designates a type mask. • **Any**—Designates any source MAC address.
Dest MAC Address	Enter a destination MAC address.
Dest Wildcard	Choose one of the following filter from the drop-down menu: • **Host**—Designates to a particular source MAC address. • **0000.00ff.ffff**—Designates a type mask. • **Any**—Designates any source MAC address.
Cos	Select a value from the CoS drop-down menu that the ACE should be match against. **Note** The CoS ranges from 0 to 7.
Lsap[0-65535]	Enter a value for LSAP that the ACE should be matched against.
Ethertype	Choose an EtherType from the drop-down menu.
Other[0-65535]	Enter a specific value from 0 to 65535.
OK button	Click this button to save the changes.
Cancel button	Click this button to avoid saving the changes that you entered.

Attach ACL

Initially, the interfaces associated with the selected device will not have ACLs attached to them. Therefore, Use this page to attach or detach an ACL, using Cisco CP.

How to Get to This Page

1. Choose **Configure > Switch > ACL**.
2. Choose **Attach**.

Related Topics

- Attach or Detach ACL to an Interface, page 86-29
- Attach ACL Reference, page 86-30

Attach or Detach ACL to an Interface

Procedure

Use this procedure to attach or detach an ACL to the selected interface.

Step 1 Choose **Configure > Switch > ACL > Attach**. See Attach ACL Summary Page, page 86-30 for more information.

Step 2 To attach or detach an ACL for a switch port, do the following:

a. Select an interface from the Attach ACL summary page.

b. Click **Edit**. Attach or Detach ACL window opens. See Attach or Detach ACL Dialog Box, page 86-31

c. Select the ACL to attach the interface from the On inbound packets IP ACL drop-down menu, and click **OK**.

d. Select **none** to detach the ACL for the selected interface from the On inbound packets IP ACL drop-down menu, and click **OK**. The Deliver Configure to Device dialog box opens.

e. Click **Deliver** in the Deliver dialog box to deliver the configuration changes to the device.

Step 3 To attach or detach an ACL for a routed port, do the following:

a. Select an interface with routed port from the Attach ACL summary page.

b. Click **Edit**. Attach or Detach ACL window opens. See Attach or Detach ACL Dialog Box, page 86-31 for more information.

c. Select the ACLs to attach the interface from the On inbound packets IP ACL and On outbound packets IP ACL drop-down menu, and click **OK**.

d. Select **none** to detach the ACL for the selected interface from the On inbound packets IP ACL and On outbound packets IP ACL drop-down menu, and click **OK**. The Deliver Configure to Device dialog box opens.

e. Click **Deliver** in the Deliver dialog box to deliver the configuration changes to the device.

Related Topics

- Attach ACL Summary Page, page 86-30
- Attach or Detach ACL Dialog Box, page 86-31

Attach ACL Reference

This section describes the pages and windows that you can use when working with attach ACL and includes following topics:

- Attach ACL Summary Page, page 86-30
- Attach or Detach ACL Dialog Box, page 86-31

Attach ACL Summary Page

Use this page to view the inbound and outbound packets that are applied to an interface or edit the same for the selected interface.

How to Get to This Page

Choose **Configure > Switch > ACL > Attach**.

Related Topic

- Attach or Detach ACL Dialog Box, page 86-31

Field Reference

Table 86-8 Cisco CP—Attach or Detach ACL

Element	Description
Interface	Displays interfaces: Fast Ethernet, Gigabit Ethernet, module or slot number (0, 1, 2), and port number.
Inbound	Displays the incoming packets that are received by the interface.
Outbound	Displays the outgoing packets that are sent form the interface.
Port type	Displays the device Port Type. Displays one of the following option: • Routed • SwitchPort
Edit button	Attaches or detaches the ACL to the selected interface.

Attach or Detach ACL Dialog Box

Use this dialog box to attach or detach an ACL to a routed port or to switch port.

How to Get to This Page

1. Choose **Configure > Switch > ACL > Attach**.
2. Click **Edit**.

Related Topics

- Attach ACL Summary Page, page 86-30
- Attach or Detach ACL to an Interface, page 86-29

Field Reference

Table 86-9 Attach or Detach ACL window

Element	Description
On inbound packets IP ACL	Select one of the ACLs form the drop-down menu.
On outbound packets IP ACL	Select one of the ACLs form the drop-down menu. **Note** The outbound packets drop-down appears when you select a routed port.
OK button	Click this button to save the changes.
Cancel button	Click this button to avoid saving the changes that you entered.

Time Range

You can selectively apply ACLs based on the time of day or week by defining a name for the time-range, and set the time and date, or the days of the week in the time range, when applying an ACL to set restrictions to the access list. For example, during a specified time period or on specified days of the week.Use the time range to define when the permit or deny statements in the ACL should be in effect.

Use this page to view the time on the selected device and the time ranges that is created. Because time ranges are checked against the time on the device, so that you can verify that the displayed time is accurate.

Related Topic

- To Set Time Range for an ACL, page 86-33
- Time Range Reference, page 86-35

To Set Time Range for an ACL

Use this page to create, edit, or delete a time range that is set for an ACL, using a Cisco CP.

How to Get to This Page

1. Choose **Configure > Switch > ACL**.
2. Choose **Time Range**.

Related Topics

- Creating, Editing, and Deleting a Time Range for an ACL, page 86-34
- Creating, Editing, and Deleting the Time Range Entries, page 86-38

Creating, Editing, and Deleting a Time Range for an ACL

Procedure

Use this procedure to create, edit, and delete a Time Range for an ACL.

Step 1 Choose **Configure > Switch > ACL > Time Range**. See Time Range Reference, page 86-35 for more information.

Step 2 To create a time range, do the following:

a. Click **Create**. The Create Time Range window opens. See Create or Edit Time Range window, page 86-37 for more information.

b. Enter a name for the new time range in the **Time Range Name** field.

c. Click **Create**. The Create Time Range Entry window opens. See Creating, Editing, and Deleting the Time Range Entries, page 86-38 and Time Range Entry, page 86-38 for more information.

d. Set the Time Range Entries for the time range, and click **OK**. See Creating, Editing, and Deleting the Time Range Entries, page 86-38 for more information.

The Create Time Range window returns.

Note The Time Range Entries are displayed in the Access Control Elements list. Repeat Step 2 to add more entries to the time range.

e. Click **OK**. The Deliver Configure to Device dialog box opens.

f. Click **Deliver** in the Deliver dialog box to deliver the configuration changes to the device.

Step 3 To edit a time range, do the following:

a. Select a time range from the Time Range Summary Page.

b. Click **Edit**. The Edit Time Range window opens. See Create or Edit Time Range window, page 86-37 for more information.

c. Choose the required time range entry from the **Access Control Elements** list to edit and click **Edit**. The window having the same fields as the Create Time Range Entry windows opens. However, the fields show the settings that were entered for the time range entries.

Note You can create more than one time range entries for the selected time range.

d. Edit the time range entries for the selected Time Range and click **OK**. See Creating, Editing, and Deleting the Time Range Entries, page 86-38 for more information. You will be returned to Edit Time Range window. Click **OK**. The Deliver Configure to Device dialog box opens.

e. Click **Deliver** in the Deliver dialog box to deliver the configuration changes to the device.

Step 4 To delete a time range, do the following:

a. Select one or multiple time range from the Time Range Summary Page and click **Delete**. A confirmation dialog box opens.

b. Click **Yes** in the confirmation dialog box.

Related Topics

- Time Range Reference, page 86-35
- Time Range Entry, page 86-38

Time Range Reference

This section describes the pages and windows that you can use when working with ACL time range and includes the following topics:

- Time Range Summary Page, page 86-36
- Create or Edit Time Range window, page 86-37

Time Range Summary Page

Use this page to view the time range that is set on the devices, or create, edit, and delete a time range for the selected device, using a Cisco CP.

How to Get to This Page

1. Choose **Configure > Switch > ACL**.
2. Choose **Time Range**.

Related Topic

- Create or Edit Time Range window, page 86-37

Field Reference

Table 86-10 Cisco CP—Time Range Summary Page

Element	Description
Time range	Displays all the time ranges.
Status	Displays the status of the time range. Displays one of the following status: • Active • Inactive
Create	Creates a time range. This is the first set of window that leads you through the creation process.
Edit	Edits the time range for the selected device.
Delete	Deletes one or more time range.

Create or Edit Time Range window

Use this window to create a time range by naming it and creating entries or edit the time range entries that already exists, using Cisco CP. The entries specifies when an associated ACE is active.

How to Get to This Page

- Choose **Configure > Switch > ACL > Time Range > Create**.
- Choose **Configure > Switch > ACL > Time Range > Edit**.

Related Topics

- Time Range Entry, page 86-38
- Time Range Summary Page, page 86-36

Field Reference

Table 86-11 Create or Edit Time Range window

Element	Description
Time Range Name	Enter a name for the new time range.
Access Control Elements	Display the lists of entries that are set for the time range.
Create button	Click this button to create new entries for the time range.
Edit button	Click this button to edit the selected entries from the Access Control Elements.
Delete button	Click this button to delete one or more entries of the time range.
OK button	Click this button to save the changes.
Cancel button	Click this button to avoid saving the changes that you entered.

Time Range Entry

Use this page to select a time range entry and click **Create** or **Edit** when creating a new time range entries in the Create Time Range window or in the Edit Time Range window.

How to Get to This Page

1. Choose **Configure > Switch > ACL > Time Range > Create** or **Edit**.
2. Click **Create** to create a new time range entry.
3. Click **Edit** to edit the existing time range entry.

Related Topics

- Creating, Editing, and Deleting the Time Range Entries, page 86-38
- Create or Edit Time Range Entry Window, page 86-40
- Time Range Reference, page 86-35

Creating, Editing, and Deleting the Time Range Entries

Procedure

Use this procedure to create, edit, or delete a time range entry, using Cisco CP.

Step 1 Choose **Configure > Switch > ACL > Time Range > Create** or **Edit**. The Create or Edit Time Range window opens. See Create or Edit Time Range window, page 86-37 for more information.

Step 2 Enter the text in the Time Range name field.

Step 3 To create a time range entry, do the following

a. Click **Create**. The Create Time Range Entry window opens. See Create or Edit Time Range Entry Window, page 86-40 for more information.

b. Select the frequency—weekly (select days), weekly (specify interval), or once—from the Frequency list drop-down menu. See Create or Edit Time Range Entry Window, page 86-40 for more information.

- **Weekly (Select Days)**—Check the check box on the days when the ACE has to be active every week. Similarly, select the start time and end time in Hour and Minute from the respective drop-down menu.
- **Weekly (Specify Interval)**—Select the start time and the end time from the drop-down menu in the interval of Day, Hour, and Minute.
- **Once**—Set the start time and end time from the drop-down menu by specifying Hour, Minute, and Date. Otherwise, check the **Now** check box, so that the start time is the current time on the device.

Note On selecting Once, the ACE will be active only once.

c. After setting the entry, click **OK**. The Deliver Configure to Device dialog box opens.

d. Click **Deliver** in the Deliver dialog box to deliver the configuration changes to the device.

Step 4 To edit a time range entry, do the following:

a. Choose the Time Range from the Time Range Summary Page, and click **Edit**.

b. Choose the required time range entry from the **Access Control Elements** field to edit, and click **Edit**. The window that has the same fields as the Create Time Range Entry windows opens. However, the fields show the settings that were entered for the time range entries. See Create or Edit Time Range Entry Window, page 86-40 for more information.

c. Edit the time range entries for the selected Time Range, and click **OK**. You will be returned to Edit Time Range window.

d. Click **OK**. The Deliver Configure to Device dialog box opens.

e. Click **Deliver** in the Deliver dialog box to deliver the configuration changes to the device.

Step 5 To delete a time range entry, do the following:

a. Choose a time range entry or multiple entries from the **Access Control Elements** field to delete from the selected Time Range.

b. Click **Delete**. The Deliver Configure to Device dialog box opens.

Note Every Time Range must have at least one Time Range Entry associated with it.

c. Click **Deliver** in the Deliver Configure to Device dialog box to deliver the configuration changes to the device.

Related Topics

- Create or Edit Time Range Entry Window, page 86-40
- Time Range Summary Page, page 86-36
- Create or Edit Time Range window, page 86-37

Create or Edit Time Range Entry Window

Use this page to set the time range entry for the ACE to be active in the interval of Hour, Minute, Date, or Day, using Cisco CP.

How to Get to This page

1. Choose **Configure > Switch > ACL > Time Range > Create or Edit**.
2. Click **Create** to set a new entry for the Time range.
3. Click **Edit** to modify the existing entry for the selected Time Range.

Related Topics

- Time Range, page 86-33
- Time Range Summary Page, page 86-36
- Create or Edit Time Range window, page 86-37

Field Reference

Table 86-12 Create or Edit Time Range Entry Window

Elements	Description
Frequency	Select one of the following options from the drop-down menu: • Weekly (Select Days) • Weekly (Specify Interval) • Once
Frequency	**Explanation**
Weekly (Select Days)	Makes an ACE active every week on the days on which check boxes are checked. The start and end times apply to the same checked days. Select a start time as early as Hour 00 Minute 00 (midnight) and an end time as late as Hour 23 Minute 59. **Note** Start and end time that span days cannot be defined.
Weekly (Specify Interval)	Makes an ACE active every week for the specified interval. The interval can begin on one day and end on another.
Once	Makes an ACE active only once. If you check **Now**, the start time is the time on the device. Otherwise, set a start time and the end time by selecting a specific Hour, Minute, and Date.

CHAPTER 87

Port Security

Configuring port security prevents unknown devices from connecting to ports without your knowledge. When a port is secure, a user-specified action occurs whenever an address-security violation occurs.

Note This feature is supported only on Cisco 2520 series switches.

Use the Port Security window to:

- Configure secure ports and define secure MAC addresses.
- Set aging time and type, and enable aging for statically configured secure addresses.

This section contains following topics:

- Secure MAC Addresses, page 87-2
- Security Violations, page 87-2

Secure MAC Addresses

Following are the types of secure MAC addresses:

- **Static secure MAC addresses**—Manually configured, stored in the address table, and added to the switch running configuration.
- **Dynamic secure MAC addresses**—Dynamically configured, stored only in the address table, and removed when the switch restarts.You can convert a dynamic MAC addresses to sticky secure MAC addresses.
- **Sticky secure MAC addresses**—Dynamically learned or manually configured, stored in the address table, and added to the running configuration.

If the sticky behavior is disabled, the sticky secure MAC addresses are converted to dynamic secure MAC addresses and removed from the running configuration.

Note The Cisco CP supports configuration of dynamic secure MAC addresses only.

Related Topics

- Security Violations, page 87-2
- Configuring Port Security, page 87-3
- Enabling and Configuring Port Security Aging, page 87-6
- Port Security Reference, page 87-7

Security Violations

The security violation occurs for one of the following reasons:

- When the unknown station MAC address, that is not stored in the MAC address table tries to access the port.
- An address learned or configured on one secure port is seen on another secure port in the same VLAN.

Configure the port for one of the following violation modes. The configuration is based on the action to be taken if a violation occurs. See Edit Port Security Dialog Box, page 87-8.

- Protect
- Restrict
- Shutdown

For more information on Port Security, see:

http://www.cisco.com/en/US/docs/switches/connectedgrid/cgs2520/software/release/12_2_53_ex/configuration/guide/swtrafc.html

Table 87-1 shows the list of the violation modes:

Table 87-1 Port Security - List of Violation mode

Violation Mode	Traffic is forwarded	Sends SNMP trap	Sends syslog message	Displays error message	Violation counter increment	Shuts down port
Protect	No	No	No	No	No	No
Restrict	No	Yes	Yes	No	Yes	No
Shutdown	No	Yes	Yes	No	Yes	Yes
Shutdown vlan	No	Yes	Yes	No	Yes	No

Related Topics

- Configuring Port Security, page 87-3
- Enabling and Configuring Port Security Aging, page 87-6
- Port Security Reference, page 87-7

Configuring Port Security

This section contains the following topics:

- Enable or Disable Port Security, page 87-4
- Enabling and Configuring Port Security Aging, page 87-6

Enable or Disable Port Security

Procedure

Use this procedure to enable or disable the port security feature on a port.

Step 1 Choose **Configure > Security > Port Security.** The Port Security pages opens. See Edit Port Security Dialog Box, page 87-8.

Step 2 To enable port security, do the following:

a. Select the port to apply the Port Security feature, and click **Edit**. The Edit Port Security window opens.

Note You can select multiple ports to edit the parameters. When you select multiple ports, the Edit Port Security dialog box does not display the port name in the **Port** field.

b. Click the **Enable** radio button to enable Security Status.

c. Setting Sticky Behavior is optional. Click the **Enable** radio button to activate Sticky Behavior. Activating Sticky Behavior ensures that you can restore the dynamically learned addresses, even if the switch restarts or powers off accidentally.

d. Enter the Maximum Address Count. This is the maximum number of address counts to assign. See Edit Port Security Dialog Box, page 87-8 for more information.

Note The range for Maximum Address Count is from 1 to 5120.

e. Select **Violation Action** from the drop-down menu. See Security Violations, page 87-2 and Edit Port Security Dialog Box, page 87-8 for more information.

Step 3 To disable port security, do the following:

a. Select the port to disable the security feature, and click **Edit**.

b. Click the **Disable** radio button to disable Security Status.

c. Click the **Enable** radio button to activate Sticky Behavior. Activating Sticky Behavior ensures that you can restore the dynamically learned addresses, even if the switch restarts or powers off accidentally.

d. Enter the Maximum Address Count. This is the maximum number of address counts to assign. See Edit Port Security Dialog Box, page 87-8 for more information.

e. Select from the drop-down menu. See Security Violations, page 87-2 and Edit Port Security Dialog Box, page 87-8 for more information.

Step 4 To set aging parameters, see How to set the Aging Parameters, page 87-6.

Related Topics

- Enabling and Configuring Port Security Aging, page 87-6
- Port Security Reference, page 87-7

Enabling and Configuring Port Security Aging

Enable port security and set its parameters for all the secure addresses on a port. Following are the types of aging that are supported:

- **Absolute:** The secure addresses on the port are deleted after the specified aging time.
- **Inactivity:** The secure addresses on the port are deleted only if the secure addresses are inactive for the specified aging time.

Use this feature to remove and add devices on a secure port without manually deleting the existing secure MAC addresses and to limit the number of secure addresses on a port.

Related Topics

- How to set the Aging Parameters, page 87-6
- Port Security Reference, page 87-7

How to set the Aging Parameters

Procedure

Use this procedure to set the Aging parameters for a port.

Step 1 Choose **Configure > Security > Port Security > Edit**. The Edit Port Security window opens. See Edit Port Security Dialog Box, page 87-8 for more information.

Step 2 To enable or disable Port Security, see Enable or Disable Port Security, page 87-4 for more information.

Step 3 To set aging parameters, do the following:

a. Click the **Enable** radio button or **Disable** radio button to set the Aging parameters for the selected port.

b. Enter the time interval to set the aging time for the port.

Note The Aging time ranges from 1 to 1440 minutes.

c. Click the **Absolute** radio button or the **Inactive** radio button to set the Aging Type. See Edit Port Security Dialog Box, page 87-8 for more information.

Related Topic

- Port Security Reference, page 87-7

Port Security Reference

This section describes the pages and dialog boxes that you can use when working with port security and includes the following topic:

- Port Security Summary Page, page 87-7
- Edit Port Security Dialog Box, page 87-8

Port Security Summary Page

Use this summary page to view, edit, and set default configuration to port security.

How to Get to This Page

Choose **Configure > Security > Port Security**.

Related Topic

- Edit Port Security Dialog Box, page 87-8

Field Reference

Table 87-2 Cisco CP—Port Security window

Elements	Description
Eligible port	Identifies static-access ports: Fast Ethernet, Gigabit Ethernet, the module or slot number (0, 1, 2), and port number.
Security status	Displays the status of the Port Security. Displays one of the following status options: • Enabled • Disabled
EtherChannel number	Displays the EtherChannel number.
Max address count	Displays the maximum number of secure addresses that are associated with the port.
Violation action	The security violation mode for the port. Displays one of the following options: • Shutdown • Restrict • Protect
Edit button	Click to Edit the configuration of the selected port. See Edit Port Security Dialog Box, page 87-8 for more information. When you select multiple ports, the Edit Port Security dialog box does not display the port name in the **Port** field.
Set defaults button	Applies the default port security configuration for a port. **Note** See Set Default Configuration, page 87-11 for default configuration of port security.

Edit Port Security Dialog Box

The Edit Port Security window allows to change the security parameters for a port.

How to Get to This Page

Choose **Configure > Security > Port Security > Edit**.

Related Topic

- Port Security Summary Page, page 87-7

Field Reference

Table 87-3 Edit Port Security configuration

Elements	Description
Port	Displays the name of the selected port for editing the parameters. When you select multiple ports, the Edit Port Security dialog box does not display the port name in the **Port** field.
Security status	Choose one of the following status by clicking the respective radio button: • **Enable**—Enables Security Status for the selected port. • **Disable**—Disables Security Status for the selected port.
Sticky behavior	Choose one of the following status by clicking the respective radio button: • **Enable**—Enables Sticky Behavior for the selected port. • **Disable**—Disables Sticky Behavior for the selected port.
Maximum address count	Enter the number of MAC addresses that can be configured on the port. **Note** The range is from 1 to 8192.

Table 87-3 Edit Port Security configuration (continued)

Elements	Description
Violation action	Choose the type of violation mode for the port from the drop-down menu. See Security Violations, page 87-2 for additional information. • **Shutdown**—After a security violation, the port immediately shuts down. • **Restrict**—After a security violation, a trap is sent to the network management station. • **Protect—**When the number of secure addresses reaches the maximum number allowed for that port, all packets with unknown addresses are dropped.
Aging parameters	• **Status**: Click the respective radio button to enable or disable the secure address aging. – **Enable**—Enables Aging Parameters for the selected port. – **Disable**—Disables Aging Parameters for the selected port. • **Time**—Sets the time in minutes for the required Aging. The range is from 1 to 1440 minutes. This field is mandatory. • **Type**: Choose the required Aging Type by clicking the respective radio button: – **Absolute**—All the secure addresses on the port age out after the specified time and are removed from the secure address list. – **Inactive**—All the secure addresses on the port age out if there is no traffic from the secure source address for the specified time period.
OK button	Click this button to save the changes.
Cancel button	Click this button to avoid saving the changes that you entered.

Related Topics

- Set Default Configuration, page 87-11

- Port Security Summary Page, page 87-7

Set Default Configuration

Procedure

Use this procedure to return the port to its defaults settings.

Step 1 Select the port on which you want to apply the default configuration.

Step 2 Click **Set Defaults**.

Related Topics

- Port Security Summary Page, page 87-7
- Edit Port Security Dialog Box, page 87-8

Field Reference

Table 87-4 Default Port Security Configuration

Feature	Default Setting
Security status	Disabled on a port.
Sticky behavior	Disabled.
Maximum address count	Set to 1.
Violation mode	**Shutdown**: The port shuts down when the maximum number of secure MAC addresses exceeds.
Aging	• **Disabled**: Aging time is zero. • **Static**: Aging is disabled. • **Type**: The value is absolute.

CHAPTER 88

802.1x

802.1x defines a user-server-based access control, and authentication protocol that prevents unauthorized clients from connecting to a LAN through publicly accessible ports. The authentication server authenticates each user connected to a switch port before making any services offered by the switch or the LAN.

802.1x access control allows only Extensible Authentication Protocol over LAN (EAPOL), Cisco Discovery Protocol (CDP), and Spanning Tree Protocol (STP) traffic through the port to which the user is connected, until the user is authenticated.

Note This feature is supported only on Cisco 2520 series switches.

Related Topics

- 802.1x, page 88-2
- 802.1x Configuration Guidelines, page 88-2
- 802.1x References, page 88-6

802.1x

802.1x can be configured in single-host, multiple-hosts, or multiple-auth modes. When 802.1x is enabled, it authenticates the port and manages the network access for all MAC addresses, including the client. The number or group of users can be limited to access the network through an 802.1x port.

For more information on 802.1x, see:

http://www.cisco.com/en/US/docs/switches/connectedgrid/cgs2520/software/release/12_2_53_ex/configuration/guide/sw8021x.html

Related Topics

- 802.1x Configuration Guidelines, page 88-2
- 802.1x References, page 88-6

802.1x Configuration Guidelines

The section provides guidelines while configuring 802.1x feature on the interface.

- Configurational Guidelines, page 88-2

Configurational Guidelines

Use the following guidelines when configuring 802.1x feature on a interface.

- To configure 802.1x port-based authentication, you must first enable Authentication, Authorization, and Accounting (AAA) server on a switch and specify the authentication method list that describes the sequence and authentication method to be queried to authenticate.
- The RADIUS server should be configured to authenticate the user to access the network. Therefore, you must create a authentication profile for the users in RADIUS server. If the users credentials are available in the RADIUS server database, 802.1x authentication takes place. On failure of 802.1x authentication, MAC Auth takes place based on the mac address of the Host. On failure of 802.1x and MAC Auth the Web Auth takes place and user gains access to the network.

For more information on RADIUS server, see:

http://www.cisco.com/en/US/docs/switches/connectedgrid/cgs2520/software/release/12_2_53_ex/configuration/guide/802.1x.html

- When 802.1x is enabled, ports are authenticated before any other Layer 2 or Layer 3 features are enabled.
- The 802.1x protocol is supported on Layer 2 static-access ports, but it is not supported on Trunk port, Dynamic-access ports, and EtherChannel port.
- If you try to change the mode of an 802.1x-enabled port (for example, from access to trunk), an error message appears, and the port mode is not changed.
- Before enabling 802.1x on a switch, delete the EtherChannel configuration from the interfaces on which 802.1x and EtherChannel are configured.

Related Topics

- Assign 802.1x to an Interface, page 88-3
- 802.1x References, page 88-6

Assign 802.1x to an Interface

Before you Begin

The RADIUS server must be configured to enable or launch the 802.1x feature on the interface. Follow the procedure before working with 802.1x feature.

Note You can skip this procedure for the GRWIC-D-ES-2S and GRWIC-D-ES-6S switching modules. In the GRWIC-D-ES-2S and GRWIC-D-ES-6S switching modules, you cannot change the value for the authorization port. By default, the commands will be delivered.

Step 1 Choose **Configure > Security > AAA > AAA Servers and Groups > Servers**. The AAA Server pages opens. Click **Add**. The Add AAA Server dialog box opens. Choose **RADIUS** from the **Server Type** drop-down menu and enter the informations for Server IP, Authorization Port, Accounting Port, and Timeout. Check the **Configure Key** check box, and enter the values in the New Key and Confirm Key tabs. Click **OK**.

Note The default value for authorization port is 1645 and accounting port is 1646.

Step 2 You must create a method list for the login access to prevent being logged out from the console and VTY access. To do that, choose **Configure > Security > AAA > Authentication Policies > Login**. Click **Add**. The Add a Method List for Authentication Login dialog box opens. Define a name in the **Specify** field, and click **ADD**. The dialog box with list of methods opens. Choose local (local authentication) and click **OK**. You can add upto four methods. Click **OK**. The Deliver to Device dialog box opens. Click **Deliver**.

Step 3 To prevent being logged out from the console and VTY, choose **Switch > Switch Access > VTY**. Select the **Authentication Policy**, and click **Edit**. The Edit VTY Lines dialog box opens. In the Authentication / Authorization field, select the policy from the **Authentication Policy** drop-down menu that was created in login method list, and click **OK**. The Deliver to Device dialog box opens. Click **Deliver**.

Procedure

Use this procedure to apply the 802.1x feature on the interface.

Step 1 Choose **Configure > Security > 802.1x**. The 802.1x summary page opens. See 802.1x Summary Page, page 88-7.

Step 2 Select the interface from the summary screen, and click **Launch Wizard** button. The 802.1x Configuration For Interfaces page opens with Welcome introduction on using 802.1x. See 802.1x Configuration For Interface Page, page 88-8 and Welcome, page 88-8

Step 3 Click **Next**. The screen guides you through next screen and the **802.1x Wizard Configuration** screen opens. See 802.1x Wizard Configuration Screen, page 88-12 for more information.

Step 4 In the 802.1x Wizard Configuration screen, choose the required **Deployment Mode** such as: Monitor, LowImpact, or HighSecurity. See 802.1x Wizard Configuration Screen, page 88-12 for more information.

Step 5 Set the parameters in the **AAA Authentication** field such as: Radius Server IP Address, Key, and Confirm Key. See 802.1x Wizard Configuration Screen, page 88-12 for more information.

Note You can skip the step 5 if you have not selected the GRWIC-D-ES-2S and GRWIC-D-ES-6S switching modules.

Step 6 Set the parameters in the **Authentication Profile** field such as: Authentication Profile, Host Mode For Access Port, or Security Violation Behavior. See 802.1x Wizard Configuration Screen, page 88-12 for more information.

Step 7 Choose the VLAN parameters from the **VLAN Configuration** drop-down menu such as: Auth - Fail VLAN, Critical VLAN, Guest VLAN, and Auth with WoL-In. See 802.1x Wizard Configuration Screen, page 88-12 for more information.

Step 8 After the Deployment mode is set and required parameters are entered for Authentication Profile and VLAN configuration, click **Next**. The screen guides you through step 3 and the **Select Interface** screen opens.

Step 9 In the Enable Column, check the check boxes of the interfaces to which the 802.1x feature must be applied, and click **Finish**. A Confirmation dialog box opens.

Step 10 Click **Yes** in the confirmation dialog box. The Deliver Configure to Device dialog box opens.

Step 11 Click **Deliver** in the Deliver dialog box to deliver the configuration changes to the device.

Related Topics

- To Delete 802.1x Configuration from an Interface, page 88-6
- 802.1x References, page 88-6

To Delete 802.1x Configuration from an Interface

Procedure

Use this procedure to delete one or more interface with 802.1x feature using Cisco CP.

Step 1 Choose **Configure > Security > 802.1x**. The 802.1x summary page opens. See 802.1x Summary Page, page 88-7

Step 2 Select one or more 802.1x interface from the summary page, and click **Remove Dot1x**. A Confirmation dialog box opens,

Step 3 Click **Yes** in the confirmation dialog box. The Deliver Configure to Device dialog box opens.

Step 4 Click **Deliver** in the Deliver dialog box to deliver the configuration changes to the device.

Related Topic

- 802.1x References, page 88-6

802.1x References

This section describes the summary pages and screens you can use when working with 802.1x. It includes the following topics:

- 802.1x Summary Page, page 88-7
- 802.1x Configuration For Interface Page, page 88-8

802.1x Summary Page

Use this page to view the Deployment Mode, Authentication Profile, Host Mode, and Violation Behavior of the interfaces. You can also configure 802.1x to an interface using **Launch Wizard**.

How to Get to This Page

Choose **Configure > Security > 802.1x**.

Related Topics

- 802.1x Configuration For Interface Page, page 88-8
- 802.1x, page 88-2

Field Reference

Table 88-1 Cisco CP—802.1x Summary Page

Element	Description
Interface	Displays the interface with 802.1x feature enabled.
Description	Displays the description of the port.
Deployment Mode	Displays the deployment mode applied to the interface.
Authentication Profile	Displays the authentication profile applied to the interface.
Host Mode	Displays the host mode of the interface.
Violation Behavior	Displays the violation behavior of the interface.
Launch Wizard	Launches the 802.1x configuration window.
Remove Dot1x	Deletes one or more interface with the 802.1x feature.

802.1x Configuration For Interface Page

This page guides you through the configuration process of 802.1x on the interface.

This section contains the following steps or screens:

- Welcome, page 88-8
- 802.1x Wizard Configuration, page 88-9
- Select Interface, page 88-17

Welcome

This screen welcomes you to the first step that leads through the configuration process of 802.1x on the interface.

How to Get to This Screen

1. Choose **Configure > Security > 802.1x**.
2. Click **Launch Wizard**.

Related Topics

- 802.1x Wizard Configuration, page 88-9
- Select Interface, page 88-17

Field Reference

Table 88-2 Cisco CP—Welcome Screen

Elements	Description
Next	Click this button to proceed with the configuration.
Cancel	Click this button to avoid saving the configuration changes that you entered.

802.1x Wizard Configuration

Use this screen to set the 802.1x parameters like Deployment Mode, Authentication profile, and VLAN Configuration on the interface using Cisco CP.

How to Get to This Screen

1. Choose **Configure > Security > 802.1x**.
2. Click **Launch Wizard**.
3. Click **Next** in the Welcome screen.

Related Topics

- To Set 802.1x Parameters, page 88-10
- 802.1x Wizard Configuration Screen, page 88-12
- Welcome, page 88-8

WEB-Authentication

Web Authentication (Web Auth) provides supplemental authentication while maintaining the benefits of an 802.1x protected network. An 802.1x is a secure, standard-based, and has Layer 2 authentication mechanism. The switch first attempts 802.1x authentication, and the end host with 802.1x supplicants are subjected to a highly secure authentication procedure while also taking advantage of 802.1x enabled features. When the switch determines that the end host does not possess an 802.1x supplicant or does not have valid credentials, the switch will fall back to Web Auth. Web Auth authenticates the user at the access edge by providing a web-based login page on which the user can enter their login credentials and thus giving minimal access to the network.

Authentication with Wake-on-LAN

The 802.1x Authentication with Wake-on-LAN (Auth with WoL) feature allows dormant PCs to be powered on when the switch receives a specific Ethernet frame, known as the magic packet. Use this feature in environments where you can connect to the systems that is powered down.

When a host that uses WoL, is attached through an 802.1x port and the host powers off, the 802.1x port becomes unauthorized. The port can only receive and send EAPOL packets, and WoL magic packets cannot reach the host. When the PC is powered off, it is not authorized, and the switch port is not opened.

When the switch uses 802.1x Auth with WoL, the switch forwards traffic to unauthorized 802.1x ports, including magic packets. While the port is unauthorized, the switch continues to block ingress traffic other than EAPOL packets. The host receives packets but will not send packets to other devices in the network.

To Set 802.1x Parameters

Procedure

Use this procedure to set the parameters in the 802.1x Wizard Configuration screen.

Step 1 Choose **Configure > Security > 802.1x > Launch Wizard**. The Welcome screen opens.

Step 2 Click **Next**. The 802.1x Wizard Configuration screen opens. See 802.1x Wizard Configuration Screen, page 88-12 for more information.

Step 3 Choose the type of Deployment Mode scrolling through the slider such as: Monitor mode, LowImpact, and HighSecurity. See 802.1x Wizard Configuration Screen, page 88-12 for more information.

Step 4 If monitor mode is selected, do the following:

a. Choose the type of authentication from the **Authentication Profile** drop-down menu like:

- 802.1x
- 802.1x then MAC Auth.

b. By default, **Multiple Auth** is enabled as the Host Mode For Access Port.

c. Choose one of the following type violation mode from the **Security Violation Behavior** drop-down menu:

- Shutdown (Default)
- Restrict
- Protect.

Step 5 If low impact mode is selected, do the following:

a. Choose the type of ACL from the **Pre-Auth Access control List** drop-down menu.

b. Choose the type of authentication from the **Authentication Profile** drop-down menu like:

- 802.1x
- 802.1x then MAC Auth
- 802.1x, then MAC Auth, then WEB Auth.

c. Select the host mode from the **Host Mode For Access Port** field such as: Multiple Auth, or Multiple Host. By default, **Single** (Auth) is enabled.

d. Choose one of the following type violation mode from the **Security Violation Behavior** drop-down menu:

- Shutdown (Default)
- Restrict
- Protect.

Step 6 If high security mode is selected, do the following:

a. Choose the type of ACL from the **Pre-Auth Access control List** drop-down menu.

b. Choose the type of authentication from the **Authentication Profile** drop-down menu like:

- 802.1x
- 802.1x then MAC Auth
- 802.1x then MAC Auth then WEB Auth.

c. Select the host mode from the **Host Mode For Access Port** field such as: Multiple Auth, or Multiple Host. By default, **Single** (Auth) is enabled.

d. Choose one of the following type of violation mode from the **Security Violation Behavior** drop-down menu:

- Shutdown (Default)
- Restrict
- Protect.

e. To set the VLAN configuration, do the following:

- Choose the VLAN ID in a range from 1 to 4094 from the **Auth-Fail VLAN**, **Guest VLAN**, **Critical VLAN** drop-down menus.
- Check the **Auth with WoL-IN** check box to restart the local device automatically on sending the magic packets uni-directional.

Note By default, the auth with WoL-IN is bi-directional.

Step 7 After the **Deployment Mode** is set with its **Authentication Profile** and **VLAN Configuration** parameters, click **Next**. The screen guides you through the next step of choosing the interface to assign the 802.1x feature. The Select Port or Interface screen opens. See Select Interface Screen, page 88-18 and To Assign 802.1x To an Interface, page 88-17 for more information.

Related Topics

- 802.1x Wizard Configuration, page 88-9
- Select Interface, page 88-17

802.1x Wizard Configuration Screen

Use this screen to set the parameters on the interface.

How to get to This Page

1. Choose **Configure > Security > 802.1x**.
2. Click **Launch Wizard**.
3. Click **Next** in the Welcome screen.

Related Topics

- Select Interface, page 88-17
- 802.1x Configuration Guidelines, page 88-2

Field Reference

Table 88-3 Port Security Wizard Configuration

Element	Description
Deployment Mode	Monitor Mode—Monitor mode allows for the deployment of identity without any impact to user or endpoint access to the network. Low Impact—In low impact mode, the user or administrator can incrementally increase the security level with the introduction of an ingress port ACL on the Open Access Identity-enable port, thus maintaining basic connectivity for guest or contractors, and unauthenticated host while selectively limiting access to introduce a higher level of access security. High Security—High security mode provides strict access controls when compared with a low impact mode that fulfills initial access security requirements for many organizations. High security mode returns to the traditional closed mode of 802.1X, in conjunction with dynamic VLAN assignment for differentiated access.
AAA Authentication	
Radius Server IP Address	Enter the radius server IP address.
Key	Enter the key for the radius server.
Confirm Key	Re-enter the key to confirm the key for the radius server.
Monitor Mode	
Authentication Profile	Choose the authentication mode from the drop-down menu: • **802.1x**—Enables 802.1X port-based authentication on the interface. • **802.1x, then MAC Auth**—On the failure or time-out of 802.1x, the authentication bypasses to MAC Auth.
Host Mode For Access Point	By default, **Multiple Auth** is enabled on a 802.1x switch port.

Table 88-3 Port Security Wizard Configuration (continued)

Element	Description
Security Violation Behavior	Choose of the violation mode from the drop-down menu: • **Shutdown (Default)**—After a security violation, the port immediately shuts down. • **Restrict**—After a security violation, a trap is sent to the network management station. • **Protect—**When the number of secure addresses reaches the maximum number allowed for that port, all packets with unknown addresses are dropped.
Low Impact	
Pre-Auth AccessControl List	Choose the type of ACL from the Default/Pre-Auth AccessControl List drop-down menu.
Authentication Profile	Choose the authentication mode from the drop-down menu: • **802.1x**—Enables 802.1x port-based authentication on the interface. • **802.1x, then MAC Auth**—On the failure or time-out of 802.1x, the authentication bypasses to MAC Auth. • **802.1x, then MAC Auth, the WEB Auth**—Enables WEB Auth on fallback of 802.1x and MAC Auth.
Host Mode For Access Point	Select one of the following host mode: • **Multiple Auth**—Allows multiple authentication on a 802.1x enabled switch port. • **Multiple Host**—Allows multiple hosts on an 802.1x-authorized port after a single host has been authenticated. **Note** By default, single authentication is enabled on 802.1x switch port.

Table 88-3 Port Security Wizard Configuration (continued)

Element	Description
Security Violation Behavior	Choose the violation mode from the drop-down menu: • **Shutdown (Default)**—After a security violation, the port immediately shuts down. • **Restrict**—After a security violation, a trap is sent to the network management station. • **Protect—**When the number of secure addresses reaches the maximum number allowed for that port, all packets with unknown addresses are dropped.
High Security	
Pre-Auth Access Control List	Choose the ACL from the drop-down menu.
Authentication Profile	Choose the authentication mode from the drop-down menu: • **802.1x**—Enables 802.1x port-based authentication on the interface. • **802.1x, then MAC Auth**—On the failure or time-out of the 802.1x, bypasses the authentication to MAC Auth. • **802.1x, then MAC Auth, the WEB Auth**—Enables WEB Auth on fallback of 802.1x and MAC Auth.
Host Mode For Access Point	Select the one of the following host mode: • **Multiple Auth**—Allows multiple authentication on a 802.1x enabled switch port. • **Multiple Host**—Allows multiple hosts on an 802.1x-authorized port after a single host has been authenticated. **Note** By default, single authentication is enabled on 802.1x switch port.

Table 88-3 Port Security Wizard Configuration (continued)

Element	Description
Security Violation Behavior	Choose of the violation mode from the drop-down menu: • **Shutdown (Default)**—After a security violation, the port immediately shuts down. • **Restrict**—After a security violation, a trap is sent to the network management station. • **Protect—**When the number of secure addresses reaches the maximum number allowed for that port, all packets with unknown addresses are dropped.
VLAN Configuration	• Choose the VLAN from the respective drop-down menu: • **Auth - Fail VLAN**—Choose a available VLAN from the **Auth - Fail VLAN** drop-down menu in a range from 1 to 4094, for the clients that are 802.1x compliant are moved into the VLAN ID when the authentication server does not receive a valid credentials. • **Guest VLAN**—Choose a available VLAN from the **Guest VLAN** drop-down menu in a range from 1 to 4094, to move the users to the selected VLAN who do not have the 802.1x client. These users are provided only with minimal access to the network. • **Critical VLAN**—Choose a available VLAN in a range from 1 to 4094 from the **Critical VLAN** drop-down menu. • **Auth with WoL-IN**—Check the **Auth with WoL-IN** check box to enable the authentication with Wake on LAN and send the magic packet in uni-directional. See Authentication with Wake-on-LAN, page 88-9 for more information.
Back	Click this button to go to the preceding configuration screen.
Next	Click this button to proceed with the configuration
Cancel	Click this button to avoid saving the configuration changes that you entered.

Select Interface

Use this screen to select the interface and assign the 802.1x feature, using Cisco CP.

Note 802.1x can be enabled only on Static access ports and they alone are displayed in the Select Interface screen.

How to Get to This Screen

1. Choose **Configure > Security > 802.1x**.
2. Click **Launch Wizard**.
3. Click **Next** in the Welcome screen.
4. Enter the parameters and click **Next** in the 802.1x Wizard Configuration Screen.

Related Topics

- To Assign 802.1x To an Interface, page 88-17
- Select Interface Screen, page 88-18
- 802.1x Wizard Configuration Screen, page 88-12

To Assign 802.1x To an Interface

Procedure

Use this procedure to assign the 802.1x feature to an interface using Cisco CP.

Step 1 Choose **Configure > Security > 802.1x > Launch Wizard**. The Welcome screen opens.

Step 2 Click **Next**. The 802.1x Wizard Configuration screen opens. See 802.1x Wizard Configuration Screen, page 88-12 for more information.

Step 3 Set the 802.1x parameters such as Deployment Mode, Authentication Profile and Vlan configuration. See 802.1x Wizard Configuration Screen, page 88-12 for more information.

Step 4 After parameters are set in the 802.1x Wizard Configuration screen, click **Next**. The Select Port or Interface screen opens. See Select Interface Screen, page 88-18 for more information.

Step 5 Check the check box corresponding to the interface in the **Enable** column. See Select Interface Screen, page 88-18 for more information.

Step 6 Click **Finish**. A Confirmation dialog box opens.

Step 7 Click **Yes** in the Confirmation dialog box. The Deliver Configure to Device dialog box opens.

Step 8 Click **Deliver** in the Deliver dialog box to deliver the configuration changes to the device.

Select Interface Screen

Use this screen to view the parameters and to assign 802.1x feature for the selected interface.

How to Get to This Screen

1. Choose **Configure > Security > 802.1x**.
2. Click **Launch Wizard**.
3. Click **Next** in the Welcome screen.
4. Enter the parameters and click **Next** in the 802.1x Wizard Configuration Screen.

Related Topics

- Welcome, page 88-8
- 802.1x Wizard Configuration Screen, page 88-12

Field Reference

Table 88-4 Select Port or Interface Screen

Elements	Description
Interface	Identifies interfaces: Fast Ethernet, Gigabit Ethernet, the module or slot number (0, 1, 2), and port number.
Enable	Check this check box to enable the corresponding interface with the 802.1x feature.
Deployment Mode	Displays the deployment mode set for an interface.
Authentication Profile	Displays the parameter set in the authentication profile for an interface.
Host Mode	Displays the host mode set for an interface.
Violation Behavior	Displays the violation mode set for an interface.
Back	Click this button to go to the preceding configuration screen.
Finish	Click this button to save the configuration changes to the device.
Cancel	Click this button to avoid saving the configuration changes that you entered.

CHAPTER 89

Security Wizard

The security wizard feature enables you to create the Access Control List (ACL) and assign it to the list of interfaces. Also, it prevents unauthorized users (host) from accessing a specific server (destination) or a specific network (destination), and restricts access to the specific protocol on the application server.

This chapter contains the following sections:

- Configuring Security Wizard, page 89-1
- Security Wizard Reference, page 89-3

Configuring Security Wizard

Procedure

Use this procedure to configure the security wizards.

Step 1 Choose **Configure > Security > Security Wizard**. The Security Wizard dialog box opens. See Security Wizard Page, page 89-3.

Step 2 Click the **Launch Wizard..** button. The Welcome page opens.

Step 3 From the Welcome page, click the **Next** button. The Select Restriction Type dialog box opens.

Step 4 To restrict the access to a server, do the following:

a. Check the **Restrict Access to a Server** radio button and click the **Next** button**.** The Specify Destination IP address dialog box opens.

b. From the Specify Destination IP Address dialog box, choose the interface through which the destination (server) can be reached and enter the server's IP address.

c. From the Select Interface dialog box, choose the interface from the **Available Interface** list. Click the >> >> button to add the chosen interface from the **Available Interfaces** area to the **Selected Interfaces** area.

d. Click the **Next** button. The Specify Source IP Addresses dialog box opens.

e. From the Specify Source IP Addresses dialog box, click the **Add** button to add the source IP address. Click the **Delete** button to delete the selected IP address from the list.

f. Click the **Finish** button to restrict the access to a server.

Step 5 To restrict the access to a network, do the following:

a. Check the **Restrict Access to a Network** radio button and click the **Next** button**.** The Select Interfaces to be Restricted dialog box opens.

b. From the Select Interfaces to be Restricted dialog box, choose the interfaces to which the security restriction needs to be applied. Click the >> >> button to add the chosen interfaces from the **Available Interfaces** area to the **Selected Interfaces** area.

c. In the Specify Network dialog box, enter the IP address and the subnet mask of the destination network.

d. Click the **Next** button. The Specify Source IP addresses dialog box opens.

e. From the Specify Source IP Addresses dialog box, click the **Add** button to add the source IP address. Click the **Delete** button to delete the selected IP address from the list.

f. Click the **Finish** button to restrict the access to a network.

Step 6 To restrict the access to an application, do the following:

a. From the Select Restriction Type dialog box, check the **Restrict Applications** radio button and click the **Next** button. The Specify Application page opens.

b. From the Specify Application dialog box, choose the applications from the **Available Applications** list. Click the >> >> button to add the chosen applications from the **Available Applications** area to the **Selected Applications** area.

c. Click the **Next** button. The Select Interfaces dialog box opens.

d. From the Select Interfaces dialog box, choose the interface from the **Available Interfaces** list to which the security restriction can be applied to the host. Click the **>> >>** button to add the chosen interface from the **Available Interfaces** area to the **Selected Interfaces** area.

e. Click the **Finish** button. The Deliver Configuration to Device page opens.

f. Click **Deliver** to deliver commands.

g. Click **Save As..** to save the configuration to your PC.

Step 7 Click the **Cancel** button to cancel the changes that you entered.

Security Wizard Reference

- Security Wizard Page, page 89-3
- Security Wizard: Welcome Page, page 89-4
- Security Wizard: Select Restriction Type, page 89-5
- Security Wizard: Specify Destination IP Addresses
- Security Wizard: Select Interfaces, page 89-7
- Security Wizard: Specify Source IP Addresses, page 89-8
- Security Wizard: Select Interfaces to be Restricted, page 89-9
- Security Wizard: Specify Source IP Addresses, page 89-10
- Security Wizard: Specify Application, page 89-11
- Security Wizard: Select Interfaces, page 89-12

Security Wizard Page

Use this page to configure the security wizards. Click the **Launch Wizard..** button. The Welcome page opens. From the Welcome page, follow the instructions to create the ACL list and assign it to the list of interfaces.

How to Get to This Page

Choose **Configure > Security > Security Wizard**.

Related Topics

- Configuring Security Wizard, page 89-1
- Security Wizard: Welcome Page, page 89-4
- Security Wizard: Select Restriction Type, page 89-5
- Security Wizard: Specify Destination IP Addresses, page 89-6
- Security Wizard: Select Interfaces, page 89-7
- Security Wizard: Specify Source IP Addresses, page 89-8
- Security Wizard: Select Interfaces to be Restricted, page 89-9
- Security Wizard: Specify Source IP Addresses, page 89-10
- Security Wizard: Specify Application, page 89-11
- Security Wizard: Select Interfaces, page 89-12

Security Wizard: Welcome Page

From the Welcome page, follow the instructions to configure the access restrictions.

How to Get to This Page

Choose **Configure > Security > Security Wizard**. Click the **Launch Wizard..** button to get to this page.

Related Topics

- Configuring Security Wizard, page 89-1
- Security Wizard: Welcome Page, page 89-4
- Security Wizard: Select Restriction Type, page 89-5
- Security Wizard: Specify Destination IP Addresses, page 89-6
- Security Wizard: Select Interfaces, page 89-7
- Security Wizard: Specify Source IP Addresses, page 89-8
- Security Wizard: Select Interfaces to be Restricted, page 89-9
- Security Wizard: Specify Source IP Addresses, page 89-10
- Security Wizard: Specify Application, page 89-11

- Security Wizard: Select Interfaces, page 89-12

Field Reference

Table 89-1 Security Wizard Welcome Page Field

Element	Description
Next	Click the **Next** button to go the Select Restriction Type dialog box.

Security Wizard: Select Restriction Type

Use the Select Restriction Type dialog box to restrict the unauthorized users from accessing a specific server or a specific network and restrict access to the specific protocol on the application server.

How to Get to This Page

Choose **Configure > Security > Security Wizard**. Click the **Next** button until you get to this page.

Related Topics

- Configuring Security Wizard, page 89-1
- Security Wizard: Welcome Page, page 89-4
- Security Wizard: Specify Destination IP Addresses, page 89-6
- Security Wizard: Select Interfaces, page 89-7
- Security Wizard: Specify Source IP Addresses, page 89-8
- Security Wizard: Select Interfaces to be Restricted, page 89-9
- Security Wizard: Specify Source IP Addresses, page 89-10
- Security Wizard: Specify Application, page 89-11
- Security Wizard: Select Interfaces, page 89-12

Field Reference

Table 89-2 Select Restriction Type Field

Element	Description
Restrict access to a server radio button	Check the **Restrict Access to a Server** radio button to restrict the access to a server.
Restrict access to a network radio button	Check the **Restrict Access to a Network** radio button to restrict the access to a network.
Restrict applications radio button	Check the **Restrict Applications** radio button to restrict the access to an application.

Security Wizard: Specify Destination IP Addresses

Use the Specify Destination IP Addresses dialog box to select the interface through which the destination (server) can be reached and to provide the server's IP address.

How to Get to This Page

Choose **Configure > Security > Security Wizard**. Check the **Restrict Access to a Server** radio button and click the **Next** button until you get to this page.

Related Topics

- Configuring Security Wizard, page 89-1
- Security Wizard: Welcome Page, page 89-4
- Security Wizard: Select Restriction Type, page 89-5
- Security Wizard: Select Interfaces, page 89-7
- Security Wizard: Specify Source IP Addresses, page 89-8
- Security Wizard: Select Interfaces to be Restricted, page 89-9
- Security Wizard: Specify Source IP Addresses, page 89-10
- Security Wizard: Specify Application, page 89-11
- Security Wizard: Select Interfaces, page 89-12

Field Reference

Table 89-3 Specify Destination IP Addresses Field

Element	Description
Interfaces	Choose the interface from the drop-down list.
Server IP address	Enter the server's Ip address.
Back	Click the **Back** button to go back to the previous wizard page.
Next	Click the **Next** button to go to the next wizard page.

Security Wizard: Select Interfaces

Use this dialog box to select the interface to which the security restriction can be applied to the host.

How to Get to This Page

Choose **Configure > Security > Security Wizard**. Check the **Restrict Access to a Server** radio button and click the **Next** button until you get to this page.

Related Topics

- Configuring Security Wizard, page 89-1
- Security Wizard: Welcome Page, page 89-4
- Security Wizard: Select Restriction Type, page 89-5
- Security Wizard: Specify Destination IP Addresses, page 89-6
- Security Wizard: Specify Source IP Addresses, page 89-8
- Security Wizard: Select Interfaces to be Restricted, page 89-9
- Security Wizard: Specify Source IP Addresses, page 89-10
- Security Wizard: Specify Application, page 89-11
- Security Wizard: Select Interfaces, page 89-12

Field Reference

Table 89-4 Select Interfaces Field

Element	Description
Available interfaces	Choose the interface from the drop-down list.
> >> button < << button	Click the **> >>** button to add the chosen application from the **Available Interfaces** area to the **Selected Interfaces** area. Click the **< <<** button to remove the chosen application from the **Selected Interfaces** area and move it to the **Available Interfaces** area.
Selected interfaces	Lists the interfaces that you selected from the Available Interfaces list.
Back	Click the **Back** button to go back to the previous wizard page.
Next	Click the **Next** button to go to the next wizard page.

Security Wizard: Specify Source IP Addresses

Use the Specify Source IP Addressed dialog box to specify the host/network IP address and the subnet mask of the source that should have the access restriction.

How to Get to This Page

Choose **Configure > Security > Security Wizard**. Check the **Restrict Access to a Server** radio button and click the **Next** button until you get to this page.

Related Topics

- Configuring Security Wizard, page 89-1
- Security Wizard: Welcome Page, page 89-4
- Security Wizard: Select Restriction Type, page 89-5
- Security Wizard: Specify Destination IP Addresses, page 89-6
- Security Wizard: Select Interfaces, page 89-7
- Security Wizard: Select Interfaces to be Restricted, page 89-9

- Security Wizard: Specify Source IP Addresses, page 89-10
- Security Wizard: Specify Application, page 89-11
- Security Wizard: Select Interfaces, page 89-12

Field Reference

Table 89-5 Specify Source IP Addresses Field

Element	Description
Source IP address	Displays the source IP address.
Subnet mask	Displays the subnet mask address.
Add	Click the **Add** button to add the source IP address and the subnet mask.
Delete	Click the **Delete** button to delete the existing source IP address.
Back	Click the **Back** button to go back to the previous wizard page.
Finish	Click the **Finish** button to save the configuration.

Security Wizard: Select Interfaces to be Restricted

Use the Select Interface to be Restricted dialog box to select the interfaces to which the security restriction needs to be applied.

How to Get to This Page

Choose **Configure > Security > Security Wizard**. Check the **Restrict Access to a Network** radio button and click the **Next** button until you get to this page.

Related Topics

- Configuring Security Wizard, page 89-1
- Security Wizard: Welcome Page, page 89-4
- Security Wizard: Select Restriction Type, page 89-5
- Security Wizard: Specify Destination IP Addresses, page 89-6
- Security Wizard: Select Interfaces, page 89-7

- Security Wizard: Specify Source IP Addresses, page 89-8
- Security Wizard: Specify Source IP Addresses, page 89-10
- Security Wizard: Specify Application, page 89-11
- Security Wizard: Select Interfaces, page 89-12

Field Reference

Table 89-6 Select Interfaces Field

Element	Description
Available interfaces	Choose the interface from the drop-down list.
> >> button < << button	Click the **> >>** button to add the chosen interface from the **Available Interfaces** area to the **Selected Interfaces** area. Click the **< <<** button to remove the chosen interface from the **Selected Interfaces** area and move it to the **Available Interfaces** area.
Selected interfaces	Lists the interfaces that you selected from the Available Interfaces list.
Destination IP address	Enter the destination IP address.
Destination subnet mask	Choose the destination subnet mask from the drop-down list.
Back	Click the **Back** button to go back to the previous wizard page.
Next	Click the **Next** button to go to the next wizard page.

Security Wizard: Specify Source IP Addresses

Use the Specify Source IP Addressed dialog box to specify the host/network IP address and the subnet mask of the source that should have the access restriction.

How to Get to This Page

Choose **Configure > Security > Security Wizard**. Check the **Restrict Access to a Network** radio button and click the **Next** button until you get to this page.

Related Topics

- Configuring Security Wizard, page 89-1
- Security Wizard: Welcome Page, page 89-4
- Security Wizard: Select Restriction Type, page 89-5
- Security Wizard: Specify Destination IP Addresses, page 89-6
- Security Wizard: Select Interfaces, page 89-7
- Security Wizard: Specify Source IP Addresses, page 89-8
- Security Wizard: Select Interfaces to be Restricted, page 89-9
- Security Wizard: Specify Application, page 89-11
- Security Wizard: Select Interfaces, page 89-12

Field Reference

Table 89-7 Specify Source IP Addresses Field

Element	Description
Source IP address	Enter the source IP address.
Server IP address	Enter the server IP address.
Add	Click the **Add** button to add the source IP address and the server's IP address.
Delete	Click the **Delete** button to delete the existing source IP address and the server's IP address.
Back	Click the **Back** button to go back to the previous wizard page.
Finish	Click the **Finish** button to save the configuration.

Security Wizard: Specify Application

Use the Specify Application dialog box to select the applications to which the ACL needs to be applied.

How to Get to This Page

Choose **Configure > Security > Security Wizard**. Check the **Restrict Applications** radio button and click the **Next** button until you get to this page.

Related Topics

- Configuring Security Wizard, page 89-1
- Security Wizard: Welcome Page, page 89-4
- Security Wizard: Select Restriction Type, page 89-5
- Security Wizard: Specify Destination IP Addresses, page 89-6
- Security Wizard: Select Interfaces, page 89-7
- Security Wizard: Specify Source IP Addresses, page 89-8
- Security Wizard: Select Interfaces to be Restricted, page 89-9
- Security Wizard: Specify Source IP Addresses, page 89-10
- Security Wizard: Select Interfaces, page 89-12

Field Reference

Table 89-8 Specify Applications

Element	Description
Available applications	Choose the application address from the drop-down list.
> >> button < << button	Click the **> >>** button to add the chosen application from the **Available Applications** area to the **Selected Applications** area. Click the **< <<** button to remove the chosen application from the **Selected Applications** area and move it to the **Available Applications** area.
Selected application	Lists the Applications that you selected from the Available Applications area.
Back	Click the **Back** button to go back to the previous wizard page.
Finish	Click the **Finish** button to save the configuration.

Security Wizard: Select Interfaces

Use Select Interfaces dialog box to select the interface to which the security restriction needs to be applied to the host.

How to Get to This Page

Choose **Configure > Security > Security Wizard**. Check the **Restrict Access to Application** radio button and click the **Next** button until you get to this page.

Related Topics

- Configuring Security Wizard, page 89-1
- Security Wizard: Welcome Page, page 89-4
- Security Wizard: Select Restriction Type, page 89-5
- Security Wizard: Specify Destination IP Addresses, page 89-6
- Security Wizard: Select Interfaces, page 89-7
- Security Wizard: Specify Source IP Addresses, page 89-8
- Security Wizard: Select Interfaces to be Restricted, page 89-9
- Security Wizard: Specify Source IP Addresses, page 89-10
- Security Wizard: Specify Application, page 89-11

Field Reference

Table 89-9 Select Interfaces Field

Element	Description
Available interfaces	Choose the interface from the drop-down list.
> >> button < << button	Click the **> >>** button to add the chosen interface from the **Available Interfaces** area to the **Selected Interfaces** area. Click the **< <<** button to remove the chosen application from the **Selected Interfaces** area and move it to the **Available Interfaces** area.
Selected interfaces	Lists the interfaces that you selected from the Available Interfaces area.
Back	Click the **Back** button to go back to the previous wizard page.
Finish	Click the **Finish** button to save the configuration.

PART 11

Monitoring Switches

This section provides information about how to monitor switches.

CHAPTER 90

Port Statistics

The Port Statistic feature provides information on ports (for example, statistics on unicast packets, multicast packets, and total collisions).

This section contains the following sections:

- Transmit Packets, page 90-1
- Receive Packets, page 90-3

Transmit Packets

In Transmit packets, the packets are transmitted by the ports in a switch to its neighboring device. Packets consist of control data, and actual data.

Related Topic

- Transmit Packets Summary Page, page 90-2

Refreshing the Transmit Packet Page

Use this procedure to refresh the page.

Step 1 Choose **Monitor > Switching > Port Statistics > Transmit Packets**.

Step 2 Click **Refresh**. The page refreshes and updates all the transmit packets.

Transmit Packets Summary Page

Use this window to view the transmission of packets of all the ports.

How to Get to This Page

Choose **Monitor > Switching > Port Statistics > Transmit Packets**.

Field Reference

Table 90-1 Cisco CP—Transmit Packets

Element	Description
Interface	Identifies interfaces: Fast Ethernet, Gigabit Ethernet, module or slot number (0, 1, 2), and port number.
Port Description	Displays the description of the port.
Unicast	Displays the total number of well-formed unicast packets transmitted by the port. It excludes packets transmitted with errors, with multicast, or for broadcast destination addresses.
Multicast	Displays the total number of well-formed multicast packets transmitted by the port. It excludes packets transmitted with errors, with unicast, or for broadcast destination addresses.
Broadcast	Displays the total number of well-formed broadcast packets transmitted by the port. It excludes packets transmitted with errors or with unicast or multicast destination addresses.
Total Collisions	Displays the total number of packets transmitted without error, after having 1 to 15 collisions. It includes packets of all the destination address types and excludes packets discarded because of insufficient resources or late collisions.
Excessive collisions	Displays the total number of packets that failed to transmit, after 16 collisions. It includes packets of all destination address types.
Late Collisions	Displays the total number of packets, discarded because of late collisions detected during transmission. It includes all transmit packets that had a collision after the transmission of 64th byte of the packet.
Refresh button	Refreshes the page.

Receive Packets

In Receive packets, the packets are received through the ports on a switch from any neighboring device.

Related Topic

- Receive Packets Summary Page, page 90-3

Refreshing the Receive Packet Page

Use this procedure to refresh the page.

Step 1 Choose **Monitor > Switching > Port Statistics > Receive Packets**.

Step 2 Click **Refresh**. The page refreshes and updates the receiving packets.

Related Topic

- Receive Packets Summary Page, page 90-3

Receive Packets Summary Page

Use this window to view the receiving of packets of all the ports.

How to Get to This Page

Choose **Monitor > Switching > Port Statistics > Receive Packets**.

Field Reference

Table 90-2 Cisco CP - Receive Packets

Elements	Description
Interface	Identifies interfaces: Fast Ethernet, Gigabit Ethernet, module or slot number (0, 1, 2), and port number.
Port Description	Displays the description of the port.
Unicast	Displays the total number of well-formed unicast packets received by the port. It excludes packets received with errors, with multicast or broadcast destination addresses, or with oversized or undersized packets. It also excludes packets discarded or without a destination address.
Multicast	Displays the total number of well-formed multicast packets received by the port. It excludes packets received with errors, with unicast or broadcast destination addresses, or with oversized or undersize packets. It also excludes packets discarded or without a destination address.
Broadcast	Displays the total number of well-formed broadcast packets received by the port. It excludes packets received with errors, with unicast or multicast destination addresses, or with oversized or undersize packets. It also excludes packets discarded or without a destination address.
Discarded	Displays the total number of packets discarded because of insufficient bandwidth or buffer space, or because the forwarding rules stipulate that they can not be forwarded.
Alignment Errors	Displays the total number of packets received with alignment errors. It includes all the packets received with both FCS errors and a non integral number of bytes.
FCS Errors	Displays the total number of packets received with FCS errors. It excludes undersized packets with FCS errors.
Collision Fragments	Displays the total number of frames, less than 64 bytes that have an integral number of bytes and bad FCS values.
Undersized	Displays the total number of packets received, fewer than 64 bytes that have good FCS values.

Table 90-2 Cisco CP - Receive Packets (continued)

Elements	Description
Oversized	Displays the total number of packets received, fewer than 1518 bytes that have good FCS values.
Refresh button	Refreshes the page.

CHAPTER 91

Resilient Ethernet Protocol Segment

Resilient Ethernet Protocol (REP) is a Cisco proprietary protocol that provides an alternative to Spanning Tree Protocol (STP) to control network loops, handle link failures, and improve convergence time. REP controls a group of ports connected in a segment, ensures that the segment does not create any bridging loops, and responds to link failures within the segment. REP is supported only on Layer 2 trunk interfaces.

A REP segment is a set of ports connected to each other and configured with a segment ID. Each segment consists of standard (non-edge) segment ports and two user-configured edge ports. A switch cannot have more than two ports that belong to the same segment, and each segment port can have only one external neighbor. A segment can go through a shared medium on any link, but only two ports can belong to the same segment.

Note This feature is supported only on Cisco 2520 series switches.

How to Get to This Page

Choose **Monitor > Switching > REP Segment**.

Related Topic

- REP Segment Summary Page, page 91-2

REP Segment Summary Page

Use this page to view the REP report of the switch. This screen is not editable.

How to Get to This Page

Choose **Monitor > Switching > REP Segment**.

Field Reference

Table 91-1 Cisco CP —REP Segment

Element	Description
Segment ID	Select the segment ID from the drop-down menu to view REP topology information for a segment at a time.
Switch Name	Displays the name of a switch that is associated with the segment ID.
Port Name	Displays all the interface in the switch which are associated to a particular segment ID.
Edge	Displays one of the following edge for the port: • Primary Edge Port • Secondary Edge Port
State	Displays the status of each port in the segment with one of the following: • Fail • Open • Alternate

CHAPTER 92

Health

Health Dash Board is a monitoring feature that monitors the health measurements of several devices to avoid downtime and to ensure that the network is running efficiently. This feature displays the measurements on the utilization of the bandwidth, CPU, memory, device temperature, and percentage of packet errors.

Related Topic

- Health Summary Page, page 92-1

Health Summary Page

Use this page to view the overall measurements of each of the categories that you monitor on all the devices in the network, using Cisco CP

How to Get to This Page

Choose **Monitor > Switching > Health**.

Field Reference

Table 92-1 Cisco CP —Health Dash Board Window

Elements	Description
Bandwidth Utilization %	Displays the average bandwidth percentage used to receive and transmit packets.
Packet Errors	Displays the overall (input and output) number of packets error.
Temperature	Displays the device temperature. Displays one of the following result: • **OK**—If the device temperature is normal. • **Faulty**—If the device temperature is below or above the normal temperature.
CPU Utilization %	Displays the percentage of CPU capacity or utilization in the last 5 seconds.
Memory Utilization %	Displays the percentage of memory in used.
Refresh button	Refresh the page.

CHAPTER 93

Reload Device

Use the Reload Device page to reload the device. To save the active or running configuration of the device in the device memory, select the **Save running configuration to device memory** check box, and click **Reload Device** button. Click **Yes** in the confirmation dialog box for a successful reload.

Note The device loads up with the configuration that is previously stored in the device memory, if the Save running configuration to device memory check box is unchecked.

How to Get to This Page

Choose **Configure > Utilities > Reload Device**.

Related Topic

- Understanding Utilities, page 63-1

PART 12

Additional Information

This section provides additional information that you might need to configure the router.

CHAPTER 94

Application Security

Application Security allows you to create security policies to govern the use of network and web applications. You can apply the policies that you create to specific interfaces, clone an existing policy to leverage the settings for a new policy, and remove policies from the router.

The Application Security feature, also referred to as Application Firewall was first supported in Cisco IOS 12.4(15)T4. Cisco Configuration Professional (Cisco CP) supports Cisco IOS 12.4(9)T and later releases. Refer to the Release Notes for Cisco Configuration Professional to learn which releases Cisco CP supports.

This chapter contains the following sections:

- Application Security Windows
- No Application Security Policy
- E-mail
- Instant Messaging
- Peer-to-Peer Applications
- URL Filtering
- HTTP
- Applications/Protocols
- Timeouts and Thresholds for Inspect Parameter Maps and CBAC

Application Security Windows

The controls in the Application Security windows allow you to associate policies with interfaces, make global settings, and add, delete and clone application security policies. The application security drawers enable you to quickly navigate to the application security area in which you need to make changes.

Policy Name List

Select the policy that you want to modify from this list. If no policies are configured, this list is empty, and the Application Security window displays a message that indicates no policies are available on the router. To create a policy, click the **Action** button, and choose **Add**.

Application Security Buttons

- **Action** button—Click to add a policy, delete the chosen policy, or clone the chosen policy. If no policies are configured on the router, **Add** is the only action available.
- **Associate** button—Click to display a dialog that allows you to associate the policy with an interface. The dialog enables you to choose the interface, and to specify the traffic direction to which the policy is to apply.
- **Global Settings** button—Click to make settings to timeout and threshold values that apply to all policies. Click Global Settings for more information.

E-mail Drawer

Click to make changes to e-mail application security settings. Click E-mail for more information.

Instant Messaging Drawer

Click to make changes to security settings for Yahoo Messenger, MSN Messenger, and other instant messaging applications. Click Instant Messaging for more information.

Peer-to-Peer Drawer

Click to make changes to security settings for KaZa A, eDonkey, and other peer-to-peer applications. Click Applications/Protocols for more information.

URL Filtering Drawer

Click to add a list of URLs that you want the application security policy to filter. You can also add filtering servers.

HTTP Drawer

Click to make changes to HTTP security settings. Click HTTP for more information.

Applications/Protocols Drawer

Click to make changes to the security settings of other applications and protocols. Click Applications/Protocols for more information.

No Application Security Policy

Cisco CP displays this window when you click the **Application Security** tab, but no Application Security policy is configured on the router. You can create a policy from this window, and view the global settings that provide default values for the parameters that you can set when you create policies.

Policy Name

Empty when no policy is configured for the router. Choosing Add from the Action context menu enables you to create a policy name and to begin to make settings for the policy.

Action

If no policy is configured on the router, you can choose **Add** from the context menu to create a policy. Once a policy is configured, the other actions, **Edit** and **Delete**, are available.

Associate

If no policy is configured this button is disabled. When a policy is created, you can click this button to associate the policy with an interface. See Associate Policy with an Interface for more information.

Global Settings

Global settings provide the default timouts, thresholds, and other values for policy parameters. Cisco CP provides defaults for each parameter, and you can change each value to define a new default that will apply unless overridden for a specific application or protocol. When you are creating a policy, you can accept the default value for a particular parameter, or choose another setting. Because the Application Security configuration windows do not display the default values you must click this button to view them in the Global Timeouts and Thresholds window. See Timeouts and Thresholds for Inspect Parameter Maps and CBAC for more information.

E-mail

Specify the e-mail applications that you want to inspect in this window. To learn about the buttons and drawers available in the Application Security tab, click Application Security Windows.

Edit Button

Click to edit the settings for the chosen application. Settings that you create override the global settings configured on the router.

Applications Column

The name of the e-mail application, for example *bliff*, *esmtp*, and *smtp*. To edit the settings for an application, check the box to the left of the application name, and click **Edit**.

Alerts, Audit, and Timeout Columns

These columns display values that have been explicitly set for an application. If a setting is not changed for an application, the column is empty. For example, if auditing has been enabled for the bliff application, but no changes have been made to the alert or to the timeout settings, the value *on* is displayed in the **Audit** column, and the **Alert** and **Timeout** columns are blank.

Options Column

This column can contain fields if other settings for the chosen application exist.

MAX Data Field

Specifies the maximum number of bytes (data) that can be transferred in a single Simple Mail Transport Protocol (SMTP) session. After the maximum value is exceeded, the firewall logs an alert message and closes the session. Default value: 20 MB.

Secure login Checkbox

Causes a user at a nonsecure location to use encryption for authentication.

Reset

Resets the TCP connection if the client enters a nonprotocol command before authentication is complete.

Router Traffic

Enables inspection of traffic destined to or originated from a router. Applicable only for H.323, TCP, and UDP protocols.

Instant Messaging

Use this window to control the traffic for Instant Messaging (IM) applications such as Yahoo Messenger, and MSN Messenger. To learn about the buttons and drawers available in the Application Security tab, click Application Security Windows.

Click Permit, Block, and Alarm Controls to learn how to specify the action the router takes if it encounters traffic with the characteristics that you specify in this window.

The following example shows traffic blocked for Yahoo Messenger traffic, and alarms generated when traffic for that application arrives:

```
Yahoo Messenger        Block          Send Alarm (checked)
```

The SDM_HIGH profile blocks IM applications. If the router uses the SDM_HIGH profile, and it does not block IM applications, those applications may have connected to a new server that is not specified in the profile. To enable the router to block these applications, check the **Send Alarm** checkbox next to the IM applications to reveal the names of the servers to which the applications connect. Then, use the CLI to block traffic from these servers. The following example uses the server name newserver.yahoo.com:

```
Router(config)# appfw policy-name SDM_HIGH
Router(cfg-appfw-policy)# application im yahoo
Router(cfg-appfw-policy-ymsgr)# server deny name newserver.yahoo.com
Router(cfg-appfw-policy-ymsgr)# exit
Router(cfg-appfw-policy)# exit
Router(config)#
```

Note

- IM applications are able to communicate over nonnative protocol ports, such as HTTP, and through their native TCP and UDP ports. Cisco CP configures block and permit actions based on the native port for the application, and always blocks communication conducted over HTTP ports.
- Some IM applications, such as MSN Messenger 7.0, use HTTP ports by default. To permit these applications, configure the IM application to use its native port.

Peer-to-Peer Applications

This page allows you to create policy settings for peer-to-peer applications such as Gnutella, BitTorrent, and eDonkey. To learn about the buttons and drawers available in the Application Security tab, click Application Security Windows.

Click Permit, Block, and Alarm Controls to learn how to specify the action that the router takes if it encounters traffic with the characteristics that you specify in this window.

The following example shows traffic blocked for BitTorrent traffic, and alarms generated when traffic for that application arrives:

Example 94-1 Blocking BitTorrent Traffic

```
BitTorrent              Block
```

Note

- Peer-to-peer applications are able to communicate over nonnative protocol ports, such as HTTP, and through their native TCP and UDP ports. Cisco CP configures block and permit actions based on the native port for the application, and always blocks communication conducted over HTTP ports.
- Application security policies will not block files if they are being provided by a paid service such as altnet.com. Files downloaded from peer-to-peer networks are blocked.

URL Filtering

URL filtering allows you to control user access to Internet websites by using URL lists. In these lists, you can specify whether a URL is to be permitted or denied. Include URL filtering capabilities in the Application Security policy by clicking **Enable URL filtering** in this window.

You can configure one local URL list on the router that is used for all Application Security policies. URL lists can also be stored on URL filter servers that the router can connect to. Information for these servers is stored in a URL filter server list. You can configure one URL filter server list on the router that is used for all Application Security policies.

The local URL list can be maintained in this window by using the **Add URL**, **Edit URL**, and **Import URL list** buttons. Because Cisco IOS software can maintain these lists with or without a configured Application Security policy, you can also maintain these lists the Additional Tasks window.

To learn how to maintain a local URL list, click Local URL List.

To learn how to maintain the URL filter server list, click URL Filter Servers.

For information on how the router uses a local URL list in combination with URL lists on URL filter servers, click URL Filtering Precedence.

For general information about URL filtering, click URL Filtering Window.

HTTP

Specify general settings for HTTP traffic inspection in this window. To learn about the buttons and drawers available in the Application Security tab, click Application Security Windows.

Click Permit, Block, and Alarm Controls to learn how to specify the action that the router takes when it encounters traffic with the characteristics that you specify in this window.

For more detailed information about how the router can inspect HTTP traffic, see *HTTP Inspection Engine* at the following link:

http://www.cisco.com/en/US/docs/ios/netmgmt/configuration/guide/nm_http_inspec_eng_ps6350_TSD_Products_Configuration_Guide_Chapter.html

Detect noncompliant HTTP traffic Checkbox

Check if you want Cisco CP to examine HTTP traffic for packets that do not comply with the HTTP protocol. Use the Permit, Block, and Alarm controls to specify the action that the router takes when this type of traffic is encountered.

Note Blocking noncompliant HTTP traffic can cause the router to drop traffic from popular websites that might not be blocked on the basis of content, if those websites do not conform to the HTTP protocol.

Detect tunneling applications Checkbox

Check if you want Cisco CP to examine HTTP traffic for packets that are generated by tunneling applications. Use the Permit, Block, and Alarm controls to specify the action that you want Cisco CP to take when it encounters this type of traffic.

Set maximum URI length inspection Checkbox

Check if you want to define a maximum length for Universal Resource Indicators (URIs). Specify the maximum length in bytes, and then use the Permit, Block, and Alarm controls to specify the action that the router takes if it encounters an URL that is longer than this value.

Enable HTTP inspection Checkbox

Check if you want the router to inspect HTTP traffic. If you want to block traffic from Java applications, you can specify a Java blocking filter by clicking the ... button and either specifying an existing ACL, or creating a new ACL for Java inspection.

Enable HTTPS inspection checkbox

Check if you want the router to inspect HTTPS traffic.

Set time out value checkbox

Check if you want to set a time out for HTTP sessions, and enter the number of seconds in the Time-Out field. Sessions will be dropped that exceed this amount of time.

Enable audit trail

You can make CBAC audit trail settings for HTTP traffic that will override the setting in the Global Timeouts and Thresholds window. **Default** means that the current global setting will be used. **On** explicitly enables the CBAC audit trail for HTTP traffic and for HTTPS traffic if HTTPS inspection is enabled, and overrides the global audit trail setting. **Off** explicitly disables the CBAC audit trail for HTTP traffic and for HTTPS traffic if HTTPS inspection is enabled, and overrides the global audit trail setting.

Header Options

You can have the router permit or deny traffic based on HTTP header length and the request method contained in the header. Request methods are the commands sent to HTTP servers to fetch URLs, web pages, and perform other actions. To learn about the buttons and drawers available in the Application Security tab, click Application Security Windows.

Set maximum header length checkbox

Check if you want the router to permit or deny traffic based on HTTP header length, and specify the maximum Request and maximum Response header length. Use the **Permit**, **Block**, and **Alarm** controls to specify the action the router takes if header length exceeds these lengths.

Configure Extension Request Method checkboxes

If you want the router to permit or deny HTTP traffic based on an extension request method, check the box next to that request method. Use the **Permit**, **Block**, and **Alarm** controls to specify the action the router takes if it encounters traffic using that request method.

Configure RFC Request Method checkboxes

If you want the router to permit or deny HTTP traffic based on one of the HTTP request methods specified in RFC 2616, *Hypertext Transfer Protocol—HTTP/1.1*, check the box next to that request method. Use the **Permit**, **Block**, and **Alarm** controls to specify the action the router takes if it encounters traffic using that request method.

Content Options

You can have the router examine the content of HTTP traffic and permit or block traffic, and generate alarms based on what things that you make the router check. To learn about the buttons and drawers available in the Application Security tab, click Application Security Windows.

Click Permit, Block, and Alarm Controls to learn how to specify the action that the router takes if it encounters traffic with the characteristics that you specify in this window.

Verify Content Type checkbox

Check if you want the router to verify the content of HTTP packets by matching the response with the request, by enabling an alarm for unknown content types, or by using both of these methods. Use the permit, block, and alarm controls to specify the action the router takes if requests cannot be matched with responses, and when it encounters an unknown content type.

Set Content Length checkbox

Check this box to set a minimum and maximum length for the data in an HTTP packet, and enter the values in the fields provided. Use the permit, block, and alarm controls to specify the action the router takes if the amount of data falls below the minimum length or when it exceeds the maximum length.

Configure Transfer Encoding Checkbox

Check this box to have the router verify how the data in the packet is encoded, and use the permit, block, and alarm controls to specify the action the router takes if it encounters the transfer encodings that you choose.

Chunk checkbox

The Encoding format specified in RFC 2616, Hypertext Transfer Protocol—HTTP/1. The body of the message is transferred in a series of chunks; each chunk contains its own size indicator.

Compress checkbox

The encoding format produced by the UNIX “compress” utility.

Deflate checkbox

The “ZLIB” format defined in RFC 1950, ZLIB Compressed Data Format Specification version 3.3, combined with the “deflate” compression mechanism described in RFC 1951, DEFLATE Compressed Data Format Specification version 1.3.

gzip checkbox

The encoding format produced by the GNU zip (“gzip”) program.

Identity checkbox

Default encoding, which indicates that no encoding has been performed.

Applications/Protocols

This window allows you to create policy settings for applications and protocols that are not found in the other windows. To learn about the buttons and drawers available in the Application Security tab, click Application Security Windows.

Applications/Protocols Tree

The Applications/Protocols tree enables you to filter the list on the right according to the type of applications and protocols that you want to view. First choose the branch for the general type that you want to display. The frame on the right displays the available items for the type that you chose. If a plus (+) sign appears to the left of the branch, there are subcategories that you can use to refine the filter. Click on the + sign to expand the branch and then select the subcategory that you want to display. If the list on the right is empty, there are no applications or protocols available for that type. To choose an application, you can check the box next to it in the tree, or you can check the box next to it in the list.

Example: If you want to display all Cisco applications, click the **Applications** branch folder, and then click the **Cisco** folder. You will see applications like *clp*, *cisco-net-mgmt*, and *cisco-sys*.

Edit Button

Click this button to edit the settings for the chosen application. Settings that you make override the global settings configured on the router.

Applications Column

The name of the application or protocol, for example *tcp*, *smtp, or ms-sna*. To edit the settings for an item, check the box to the left of the item name, and click **Edit**.

Alerts, Audit, and Timeout Columns

These columns display explicitly-set values for an item. If a setting is not changed for an item, the column is empty. For example, if auditing has been enabled for the ms-sna application, but no changes have been made to the alert or to the timeout settings, the value *on* is displayed in the **Audit** column, but the **Alert** and **Timeout** columns are blank.

Options Column

This column can contain fields if other settings were made for the chosen item.

MAX Data

Specifies the maximum number of bytes (data) that can be transferred in a single Simple Mail Transport Protocol (SMTP) session. After the maximum value is exceeded, the firewall logs an alert message and closes the session. Default value: 20 MB.

Secure login

Causes a user at a nonsecure location to use encryption for authentication.

Reset

Resets the TCP connection if the client enters a nonprotocol command before authentication is complete.

Router Traffic

Enables inspection of traffic destined to or originated from a router. Applicable only for H.323, TCP, and UDP protocols.

Timeouts and Thresholds for Inspect Parameter Maps and CBAC

Use this information to help you create or edit a parameter map for inspection purposes, or to set Context-Based Access Control (CBAC) global timeouts and thresholds. CBAC uses timeouts and thresholds to determine how long to manage state information for a session and to determine when to drop sessions that do not become fully established. These timeouts and thresholds apply to all sessions.

Global Timer values can be specified in seconds, minutes, or hours.

TCP Connection Timeout Value

Amount of time to wait for a TCP connection to be established. The default value is 30 seconds.

TCP FIN Wait Timeout Value

Amount of time that a TCP session will still be managed after the firewall detects a FIN exchange. The default value is 5 seconds.

TCP Idle Timeout Value

Amount of time that a TCP session will still be managed after no activity has been detected. The default value is 3600 seconds.

UDP Idle Timeout Value

Amount of time that a User Datagram Protocol (UDP) session will still be managed after no activity has been detected. The default value is 30 seconds.

DNS Timeout Value

Amount of time that a Domain Name System (DNS) name lookup session will be managed after no activity has been detected. The default value is 5 seconds

SYN Flooding DoS Attack Thresholds

An unusually high number of half-open sessions may indicate that a Denial of Service (DoS) attack is under way. DoS attack thresholds allow the router to start deleting half-open sessions after the total number of them has reached a maximum threshold. By defining thresholds, you can specify when the router should start deleting half-open sessions and when it can stop deleting them.

One-minute session thresholds. These fields let you specify the threshold values for new connection attempts.

Low	Stop deleting new connections after the number of new connections drops below this value. The default value is 400 sessions.

High	Start deleting new connections when the number of new connections exceeds this value. The default value is 500 sessions

Maximum incomplete session thresholds. These fields let you specify the threshold values for the total number of existing half-open sessions.

Low	Stop deleting new connections after the number of new connections drops below this value. The default value is 400 sessions for Cisco IOS releases older than 12.4(11)T. When a Low value is not explicitly set, Cisco IOS will stop deleting new sessions when the number of sessions drops to 400. For Cisco IOS release 12.4(11)T and later, the default value is unlimited. When a Low value is not explicitly set, Cisco IOS will not stop deleting new connections.
High	Start deleting new connections when the number of new connections exceeds this value. The default value is 500 sessions for Cisco IOS releases older than 12.4(11)T. When a High value is not explicitly set, Cisco IOS starts deleting sessions when more than 500 new sessions have been established. For Cisco IOS release 12.4(11)T and later, the default value is unlimited. When a High value is not explicitly set, Cisco IOS will not start deleting new connections.

TCP Maximum Incomplete Sessions per Host:

The router starts deleting half-open sessions for the same host when the total number for that host exceeds this number. The default number of sessions is 50. If you check the **Blocking Time** field and enter a value, the router will continue to block new connections to that host for the number of minutes that you specify.

Enable audit globally

Check if you want to turn on CBAC audit trail messages for all types of traffic.

Enable alert globally

Check if you want to turn on CBAC alert messages for all types of traffic.

Associate Policy with an Interface

In this window, select the interface to which you want to apply the selected policy. Also specify whether the policy is to apply to incoming traffic, to outgoing traffic, or to traffic in both directions.

For example, if the router has FastEthernet 0/0 and FastEthernet 0/1 interfaces, and you want to apply the policy to the FastEthernet 0/1 interface, on traffic flowing in both directions, check the box next to FastEthernet 0/1, and check the boxes in both the Incoming and the Outgoing columns. To have only incoming traffic inspected, only check the box in the Incoming column.

Edit Inspection Rule

Use this window to specify custom inspection rule settings for an application. Settings made here and applied to the router's configuration override the global settings.

Click the **Global Settings** button in the Application Security window to display the global settings for the parameters that you can set in this window. See Timeouts and Thresholds for Inspect Parameter Maps and CBAC for more information.

Alert Field

Choose one of the following values:

- **default**—Use the global setting for alerts.
- **on**—Generate an alert when traffic of this type is encountered.
- **off**—Do not generate an alert when traffic of this type is encountered.

Audit Field

Choose one of the following values:

- **default**—Use the global setting for audit trails.
- **on**—Generate an audit trail when traffic of this type is encountered.
- **off**—Do not generate an audit trail when traffic of this type is encountered.

Timeout Field

Enter the number of seconds that a session for this application should be managed after no activity has been detected. The timeout value that you enter sets the TCP Idle Timeout value if this is a TCP application, or the UDP timeout value if this is a UDP application.

Other Options

Certain applications can have additional options set. Depending on the application, you may see the options described next.

MAX Data field

Specifies the maximum number of bytes (data) that can be transferred in a single Simple Mail Transport Protocol (SMTP) session. After the maximum value is exceeded, the firewall logs an alert message and closes the session. Default value: 20 MB.

Secure Login Checkbox

Causes a user at a nonsecure location to use encryption for authentication.

Reset Checkbox

Resets the TCP connection if the client enters a nonprotocol command before authentication is complete.

Router Traffic Checkbox

Enables inspection of traffic destined to or originated from a router. Applicable only for H.323, TCP, and UDP protocols.

Permit, Block, and Alarm Controls

Use the Permit, Block, and Alarm controls to specify what the router is to do when it encounters traffic with the characteristics that you specify. To make a policy setting for an option with these controls, check the box next to it. Then, in the Action column, choose **Permit** to allow traffic related to that option, or choose **Block** to deny traffic. If you want an alarm to be sent to the log when this type of traffic is encountered, check **Send Alarm**. The Send Alarm control is not used in all windows.

Logging must be enabled for Application Security to send alarms to the log. For more information go to this link: Application Security Log.

CHAPTER 95

Tools Menu Commands

The following options are available from the Cisco Configuration Professional (Cisco CP) Tools menu.

- Ping
- Telnet
- Internal Access Point Screens
- Security Audit
- USB Token PIN Settings
- Wireless Application
- CCO Login

Ping

In this screen, test the connectivity to another device on the network by pinging the device. You can select both the source and destination of the ping operation. You may want to ping a remote peer after you reset a VPN tunnel.

How to Get to this Screen

In the menu bar, click **Tools** > **Ping**.

Field Reference

Table 95-1 Ping Screen

Element	Description
Source	Select or enter the IP address where you want the ping to originate. If the address you want to use is not in the list, you can enter a different one in the field. The ping can originate from any interface on the router. By default, the **ping** command originates from the outside interface with the connection to the remote device.
Destination	Select the IP address that you want to ping. If the address you want to use is not in the list, you can enter a different one in the field.
Clear	To clear the output of the ping command, click **Clear**.

Telnet

Displays the Windows Telnet dialog box, letting you connect to your router and access the Cisco IOS command-line interface (CLI) using the Telnet protocol.

Internal Access Point Screens

When you launch the internal access point from Cisco CP, several screens or warning messages may appear. This section describes those screens.

This section contains the following parts:

- IP Address
- Warning Message

IP Address

In this screen provide an IP address for the internal access point BVI interface. This is done to support IRB bridging.

How to Get to this Screen

This screen is displayed automatically when you are attempting to launch the internal access point software, but the internal access point needs an IP address.

Field Reference

Table 95-2 Configure IP Address

Element	Description
IP Address Type	In this field, choose one of the following types: • Static—To configure the interface with a static IP address and subnet mask, choose **Static**. • Dynamic—To configure the interface to use an IP address from a DHCP server, choose **Dynamic**. There must be a DHCP server on the network that the access point can connect to in order to obtain an IP address.
IP Address	If you chose Static in the IP Address Type field, enter the IP address for the interface. For more information, see IP Addresses and Subnet Masks.
Subnet Mask	If you chose Static in the IP Address Type field, enter the subnet mask for the interface. For more information, see IP Addresses and Subnet Masks.
DHCP Server	If you chose Dynamic in the IP Address Type field, enter the IP address of the DHCP server from which the access point will obtain an IP address.

Warning Message

This help topic provides additional information concerning warning messages that may be generated when trying to connect to the router internal access point.

How to Get to this Screen

The warning message screen is displayed automatically when a problem occurs connecting to the access point.

Message Reference

Table 95-3 Warning Messages

Message	Remedy
Null IP address entered	No IP address has been entered for the internal access point. Enter an IP address for the module and try again.
Invalid IP address entered	Enter the IP address of the access point module in dotted-decimal format, for example, 192.168.7.5.
No HTTP or HTTPS configured on internal access point.	Login to the internal access point, enter privileged EXEC mode, and then enter the **config terminal** command. Then, enter the command **ip http-server**, or **ip http-secure-server**.
Connection error	This problem may have one of the following causes and remedies. After you take the necessary remedial steps, try connecting to the internal access point again. • The internal access point login credentials are invalid or the enable password is invalid. Login to the internal access point and verify the username and passwords, and then correct them in Cisco CP if necessary. • The internal access point is not in privileged EXEC mode. Login to the internal access point, verify the operating mode, and place it in privileged EXEC mode if necessary. • The internal access point is generating unexpected messages. Login to the internal access point, direct logging messages to the internal access point console, and determine if there is an error condition. If an error condition exists, fix this problem before attempting to connect again. • Communication with the internal access point has timed out. Login to the internal access point, direct logging messages to the internal access point console, and determine if there is an error condition. If an error condition exists, fix this problem before attempting to connect again.

Table 95-3 Warning Messages

Message	Remedy
Access Point Module not in Autonomous mode	The internal access point Cisco IOS image does not enable it to operate in Autonomous mode. To correct this problem, you must load a Cisco IOS image on the internal access point that enables it to operate in Autonomous mode.
Unsupported device.	The device or module that you are trying to connect to is not supported for this Cisco CP feature.

Security Audit

Displays the Cisco CP Security Audit screen. See Security Audit for more information.

USB Token PIN Settings

The USB Token PIN Settings dialog box allows you to set PINs for USB tokens connected to your router.

Select a PIN Type

Choose **User PIN** to set a user PIN, or **Admin PIN** to set an administrator PIN.

A user PIN is used to log into a router. If you connect a USB token to a router, and the token's name and user PIN match an entry in **Configure > VPN Components > Public Key Infrastructure > USB Tokens**, you are automatically logged into that router.

An administrator PIN is used to manage USB token settings using the manufacturer's software. Cisco CP allows you to change the administrator PIN for a USB token if you can supply the current administrator PIN.

Token Name

Enter the USB token's name.

The token's name is set by the manufacturer. For example, USB tokens manufactured by Aladdin Knowledge Systems are named eToken.

You can also use the name "usbtoken*x*", where *x* is the number of the USB port to which the USB token is connected. For example, a USB token connected to USB port 0 is named usbtoken0.

Current PIN

Enter the existing user or administrator PIN. If you do not know the existing PIN, you must use the USB token manufacturer's software to find it.

New PIN

Enter a new PIN for the USB token. The existing PIN will be replaced by the new PIN. The new PIN must be at least 4 digits long.

Confirm PIN

Reenter the new PIN to confirm it.

Save the New PIN to Router

Check the **Save the new PIN to router** checkbox if you want to save the new PIN as an entry in **Configure > VPN Components > Public Key Infrastructure > USB Tokens**. If an entry with the same name already exists in **Configure > Security > VPN Components > Public Key Infrastructure > USB Tokens**, it is replaced with the new one.

The **Save the new PIN to router** checkbox is available only for user PINs.

Wireless Application

If the router has radio interfaces, you can launch the Wireless Application to configure and monitor those interfaces. Cisco CP can help you configure and display the IP address or bridging details about a radio interface, but you must use the Wireless Application to set other configuration parameters.

CCO Login

You must provide a CCO login and password to access this web page. Provide a username and password, and then click OK.

If you do not have a CCO login and password, you can obtain one by opening a web browser and going to the Cisco website at the following link:

http://www.cisco.com

When the webpage opens, click Register and provide the necessary information to obtain a username and password. Then, try this operation again.

CHAPTER 96

URL Filtering

URL filtering allows you to control access to Internet websites by permitting or denying access to specific websites based on information contained in a URL list. You can maintain a local URL list on the router, and you can use URL lists stored on Websense or Secure Computing URL filter list servers. URL filtering is enabled by configuring an Application Security policy that enables it.

Even if no Application Security policy is configured on the router, you can still maintain a local URL list and a URL filter server list that can be used for URL filtering when a policy is created that enables it.

This chapter contains the following sections:

- URL Filtering Window
- Local URL List
- URL Filter Servers

For more information on URL filtering, go to the document *Firewall Websense URL Filtering* at the following link:

http://www.cisco.com/en/US/docs/ios/12_2t/12_2t15/feature/guide/ftwebsen.html

To learn how URL filtering policies are used, click URL Filtering Precedence.

URL Filtering Window

This window displays the global settings for URL filtering on the router. You can maintain the local URL list and the URL filter server list in the Additional Tasks screens or in the Application Security windows. The Global settings for URL filtering can only be maintained from this Additional Tasks window. Use the **Edit Global Settings** button to change these values.

For a description of each setting that appears in this window, Click Edit Global Settings.

See the introductory information in URL Filtering for a description of the URL filtering features that Cisco CP provides.

Edit Global Settings

Edit URL filtering global settings in this window.

Note Logging must be enabled for the router to report URL filter alerts, audit trail messages, and system messages pertaining to the URL filter server.

Allow Mode

Check this box to enable the router to enter allow mode when the router cannot connect to any of the URL filtering servers in the server list. When the router is in allow mode, all HTTP requests are allowed to pass if the router cannot connect to any server in the URL filter server list. Allow mode is disabled by default.

URL Filter Alert

Check this box to enable the router to log URL filtering alert messages. URL filtering alert messages report events such as a URL filtering server going down, or an HTTP request containing a URL that is too long for a lookup request. This option is disabled by default.

Audit Trail

Check this box to enable the router to maintain an audit trail in the log. The router will record URL request status messages that indicate whether an HTTP request has been permitted or denied and other audit trail messages. This option is disabled by default.

URL Filter Server Log

Check this box to enable the router to record system messages that pertain to the URL filter server in the log. This option is disabled by default.

Cache Size

You can set the maximum size of the cache that stores the most recently requested IP addresses and their respective authorization status. The default size of this cache is 5000 bytes. The range is from 0 bytes to 2147483647. The cache is cleared every 12 hours.

Maximum buffered HTTP requests

You can set the maximum number of outstanding HTTP requests that the router can buffer. By default, the router buffers up to 1000 requests. You can specify from 1 to 2147483647 requests.

Maximum buffered HTTP responses

You can set the number of HTTP responses from the URL filtering server that the router can buffer. After this number is reached, the router drops additional responses. The default value is 200. You can set a value from 0 to 20000.

General Settings for URL Filtering

Name the URL filter, specify what the router is to do when it detects a match, and configure log and cache size parameters. You can also specify a source interface if you do not want the URL filtering parameter map to apply to all router interfaces.

URL Filter Name

Enter a name that will convey how this URL filter is configured or used. For example, if you specify a source interface of Fast Ethernet 1, you might enter the name **fa1-parmap**. If the filter uses a Websense URL filter server at IP address 192.128.54.23, you might enter **websense23-parmap** as the name.

Allow Mode

Check this box to enable the router to enter allow mode when the router cannot connect to any of the URL filtering servers in the server list. When the router is in Allow mode, all HTTP requests are allowed to pass if the router cannot connect to any server in the URL filter server list. Allow mode is disabled by default.

URL Filter Alert

Check this box to enable the router to log URL filtering alert messages. URL filtering alert messages report events such as a URL filtering server going down, or an HTTP request containing a URL that is too long for a lookup request. This option is disabled by default.

Audit Trail

Check this box to enable the router to maintain an audit trail in the log. The router will record URL request status messages that indicate whether an HTTP request has been permitted or denied and other audit trail messages. This option is disabled by default.

URL Filter Server Log

Check this box to enable the router to record system messages that pertain to the URL filter server in the log. This option is disabled by default.

Cache Size

You can set the maximum size of the cache that stores the most recently-requested IP addresses and their respective authorization status. The default size of this cache is 5000 bytes. The range is from 0 bytes to 2147483647. The cache is cleared every 12 hours.

Maximum Buffered HTTP Requests

You can set the maximum number of outstanding HTTP requests that the router can buffer. By default, the router buffers up to 1000 requests. You can specify from 1 to 2147483647 requests.

Maximum Buffered HTTP Responses

You can set the number of HTTP responses from the URL filtering server that the router can buffer. After this number is reached, the router drops additional responses. The default value is 200. You can set a value from 0 to 20000.

Advanced

The Advanced box allows you to choose the source interface. Choose the interface from the Source Interface list.

Local URL List

If the Cisco IOS image on the router supports URL filtering but does not support Zone-based Policy Firewall (ZPF), you can maintain one local URL list on the router. This list is used by all Application Security policies in which URL filtering is enabled. Cisco IOS images of release 12.4(9)T and later support all the ZPF features that Cisco CP supports. In a ZPF configuration, a local URL list can be created for each URL filtering parameter map.

You can use Cisco CP to create list entries and you can import entries from a list stored on your PC. When a local URL list is used in combination with URL filter servers, local entries are used first. See URL Filtering Precedence for more information.

Maintaining the Local URL List

You can use Cisco CP to maintain a local URL list by adding and deleting entries one-by-one, and by importing a URL list from your PC and specifying what you want Cisco CP to do with each entry. Use the **Add** and the **Delete** buttons to manage specific entries in the list on the router, and click the **Import URL List** button to import a URL list from your PC.

Note If an entry is deleted from the local list and the router is configured to use URL filtering servers, entries that match ones that you are deleting from the local list may exist on those servers.

Use the **Delete All** button to delete all entries on the router. If no local list is configured on the router, the router must rely on the configured URL filter servers. If you want to retrieve the URL list you are deleting at a later time, use the **Export URL List** button to save the URL list to your PC before deleting all the entries. When you save a URL list to your PC the list is given a .CSV extension.

Importing URL Lists from your PC

Click the **Import URL List** button to import a URL list from your PC to the router. The URL list that you select must have a .txt or .CSV extension. After you select the list on your PC, Cisco CP displays a dialog that allows you to specify what you want to do with each entry in the list. See Import URL List for more information.

Add or Edit Local URL

Use this window to add or edit a URL entry for the local URL list on the router. Enter a full domain name or a partial domain name and choose whether to **Permit** or **Deny** requests for this URL.

If you enter a full domain name, such as www.somedomain.com, all requests that include that domain name, such as www.somedomain.com/news or www.somedomain.com/index will be permitted or denied based on the setting you choose in this dialog. These requests will not be sent to the URL filtering servers that the router is configured to use.

If you enter a partial domain name, such as .somedomain.com, all requests that end with that string, such as www.somedomain.com/products or wwwin/somedomain.com/eng will be permitted denied based on the setting you choose in this dialog. These requests will not be sent to the URL filtering servers that the router is configured to use.

Import URL List

This dialog allows you to examine the URL list you are importing from your PC to the router and specify what you want to do with each entry. If a URL entry in this dialog is not already present on the router, you can add it to the list on the router by clicking **Append**. If a URL entry is already present on the router but you want to replace it with the entry in this dialog, click **Replace**.

All boxes in the **Import** column are checked by default.If there are entries that you do not want to be sent to the router, uncheck the box next to those entries.If you want to remove the checks from all the boxes, click **Unselect All**. Clicking **Select All** places checkmarks in all the boxes.

Append adds any checked entry to the URL list that is not already present in the list If you attempt to add an entry that is already in the URL list, it will not be added even if the action specified for the domain in the entry is different from the action that is already in the list.

Use the **Replace** button to specify a different action for an entry that is already in the router's URL list.If the entry you checked is not already in the router's list, **Replace** has no effect.

URL Filter Servers

The router can send HTTP requests to URL filtering servers that are capable of storing much larger URL lists than the router can store. If the router is configured with a URL filter server list, the router sends requests that do not match entries in the local list to the URL filter server it has a connection to, and permits or denies the request based on the response it receives from the server. When the server that the router is connected to goes down, the router contacts the next server in the list until it establishes a connection.

Lists on URL filter servers can be used along with local URL lists. Click URL Filtering Precedence to learn how the router uses both of these resources.

Click **Add**, and choose either **Secure Computing** or **Websense** to specify the type of server that you are adding.

Note Cisco IOS software can only use one type of URL filtering server, and does not allow you to add a server to the list if it is of a different type. For example, if a URL filter server list containing Websense servers is configured on the router, you

will receive an error message if you attempt to add an Secure Computing server to the list. If the URL filter server list currently contains one type of server and you want to change to the other type, you must delete all the server entries in the list before adding an entry of the new type.

This window displays the configuration for each URL filter server in the list. See Add or Edit a URL Filter Server for a description of each configuration value.

Add or Edit a URL Filter Server

Specify the information for the Websense or Secure Computing URL filter server.

IP Address/Hostname

Enter the IP address or the hostname for the server. If you enter a hostname, the router must have a connection to a DNS server in order to resolve the hostname to an IP address.

Direction

Choose **Inside** if the URL filter server is part of the inside network. This is usually one of the networks that the router LAN interfaces connect to. Choose **Outside** if the router is in the outside network. This is usually one of the networks that the router WAN interfaces connect to. The default value is **Inside**.

Port Number

Automatically contains the default port number for the type of URL filter server you are adding. If you are adding a Websense server, the default value is 15868. If you are adding an Secure Computing server, the default value is 4005. Change this number to the number of the port that the server listens on if that number is different from the default. This field accepts values from 1 to 65535.

Retransmission Count

Optional field. Enter the number of times that you want the router to attempt to retransmit the request if no response arrives from the server. The default value is 2 times. This field accepts values from 1 to 10.

Retransmission Timeout

Optional field. Enter the number of seconds that the router should wait for a response from the server before retransmitting the request. The default value is 5 seconds.

URL Filtering Precedence

URL filtering must be enabled by going to **Configure > Security > Firewall and ACL > Application Security > URL Filtering** and clicking **Enable URL filtering**. This can only be done when an Application security policy is configured on the router.

When URL filtering is enabled, the router determines how to handle an HTTP request as follows:

- If the URL in the request matches an entry in the local URL list on the router, the router permits or denies the request based on that entry.
- If the URL in the request does not match any entry in the local URL list, the router passes the HTTP request to the URL filtering server to which it has a connection. It permits or denies the request based on the information that the server returns.
- If allow mode is disabled, and the router cannot establish a connection with a URL filter server, the router denies the request. Allow mode is disabled by default.
- If allow mode is enabled and the router cannot establish a connection with a URL filter server, the router permits the request. Allow mode can be enabled in the Edit Global Settings dialog.

Only one URL list and one URL filter server list can be configured on the router. All configured Application Security policies use the same URL list and URL filter server list. These lists can be maintained in the Application Security windows, or by going to **Additional Tasks > URL Filtering**. If all Application Security policies are deleted, the URL list and URL filter server list can still be maintained in the Additional Tasks windows. However, the router does not perform URL filtering unless URL filtering is enabled in an Application Security policy.

CHAPTER 97

More About....

These topics provide more information about subjects that Cisco CP online help discusses.

IP Addresses and Subnet Masks

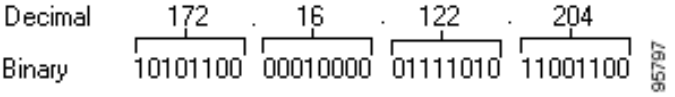
This topic provides background information about IP addresses and subnet masks, and shows you how to use this information when entering addresses and masks in Cisco CP.

IP version 4 addresses are 32 bits, or 4 bytes, in length. This address "space" is used to designate the following:

- Network number
- Optional subnetwork number
- A host number

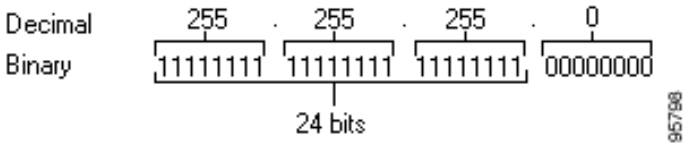
Note Cisco CP does not support IP version 6.

Cisco CP requires you to enter IP addresses in dotted-decimal format. This format makes addresses easier for people to read and manipulate, by grouping the 32 bits into 4 octets which are displayed in decimal, separated by periods or "dots," for example, 172.16.122.204. The decimal address 172.16.122.204 represents the binary IP address shown in the following figure.



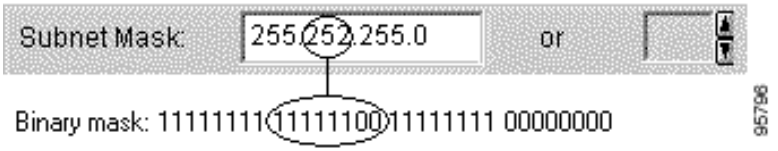
The subnet mask is used to specify how many of the 32 bits are used for the network number and, if subnetting is used, the subnet number. It is a binary mask with a 1 bit in every position used by the network and subnet numbers. Like the IP address, it is a 32-bit value, expressed in decimal format. The following figure shows a subnet mask entered in Cisco CP. Cisco CP shows the subnet mask and the equivalent number of bits in the mask.

These values entered Cisco CP represent the binary mask shown in the following figure:



This subnet mask specifies that the first 24 bits of the IP address represent the network number and subnet mask, and that the last 8 bits represent the host number within that network and subnet. You can enter the mask in the dotted decimal format shown in the Subnet Mask field, or you can select the number of bits in the bits field. When you enter or select a value in one field, Cisco CP automatically adjusts the other.

Cisco CP displays a warning window if you enter a decimal mask that results in binary zeros (0s) in the network/subnet area of the mask. The following subnet mask field contains a decimal value that would result in binary zeros in the network/subnet number portion of the mask. Note that the bits field on the right is empty, indicating that an invalid value has been entered in the Subnet Mask field.



When a network address is displayed in Cisco CP windows, the IP address and subnet mask for it may be shown in network address/subnet bits format, as in the following example:

```
172.28.33.0/24
```

The network address in this example is 172.28.33.0. The number 24 indicates the number of subnet bits used. You can think of it as shorthand for the corresponding subnet mask of 255.255.255.0.

Addresses used on the public Internet must be completely unique for the period of time they are being used. On private networks, addresses may be unique only to the private network or subnetwork.

Addresses may also be translated by using schemes such as NAT and PAT, and they may be temporarily assigned using DHCP. You can use Cisco CP to configure NAT, PAT and DHCP.

Host and Network Fields

This topic explains how to supply host or network information in windows that allow you to specify a network or host address, or a host name.

Specify the network or the host.

Type

One of the following:

- **A Network**—If you select this, provide a network address in the IP address field. Note that the wildcard mask enables you to enter a network number that may specify multiple subnets.
- **A Host Name or IP Address**—If you select this, provide a host IP address or host name in the next field.
- **Any IP address**—The action you specified is to apply to any host or network.

IP Address/Wildcard Mask

Enter a network address, and then the wildcard mask to specify how much of the network address must match exactly.

For example, if you entered a network address of 10.25.29.0 and a wildcard mask of 0.0.0.255, any java applet with a source address containing 10.25.29 would be filtered. If the wildcard mask were 0.0.255.255, any java applet with a source address containing 10.25 would be filtered.

Host Name/IP

This field appears if you selected **A Host Name or IP Address** as Type. If you enter a host name, ensure that there is a DNS server on the network capable of resolving the host name to an IP address.

Available Interface Configurations

The types of configurations available for each interface type are shown in the following table.

If you have selected:	You can add a:
An Ethernet interface	• PPPoE connection • Tunnel interface • Loopback interface
Any of the following: • Ethernet with a PPPoE connection • Dialer Interface associated with an ADSL or G.SHDSL configuration • Serial interface with a PPP or HDLC configuration • Serial subinterface with a Frame Relay configuration • Unsupported WAN interface	• Tunnel interface • Loopback Interface

An ATM interface without any encapsulation	• An ADSL interface • A G.SHDSL interface • A tunnel or loopback for either of the above
A serial interface	• A Frame Relay connection • A PPP connection • A tunnel interface • A loopback interface
ATM subinterface An Ethernet subinterface A dialer interface not associated with an ATM interface A loopback A tunnel	• A tunnel interface • A loopback interface

DHCP Address Pools

The IP addresses that the DHCP server assigns are drawn from a common pool that you configure by specifying the starting IP address in the range and the ending address in the range.

The address range that you specify should be within the following private address ranges:

- 10.1.1.1 to 10.255.255.255
- 172.16.1.1 to 172.31.255.255

The address range that you specify must also be in the same subnet as the IP address of the LAN interface. The range can represent a maximum of 254 addresses. The following examples are valid ranges:

- 10.1.1.1 to 10.1.1.254 (assuming LAN IP address is in 10.1.1.0 subnet)
- 172.16.1.1 to 172.16.1.254 (assuming LAN IP address is in 172.16.1.0 subnet)

Cisco CP configures the router to automatically exclude the LAN interface IP address in the pool.

Reserved Addresses

You must not use the following addresses in the range of addresses that you specify:

- The network/subnetwork IP address.
- The broadcast address on the network.

Meanings of the Permit and Deny Keywords

Rule entries can be used in access rules, NAT rules, IPSec rules, and in access rules associated with route maps. Permit and Deny have various meanings depending on which type of rule is using it.

Rule Type	Meaning of Permit	Meaning of Deny
Access rule	Allow matching traffic in or out of the interface to which the rule has been applied.	Drop matching traffic.
NAT rule	Translate the IP address of matching traffic to the specified inside local address or outside local address.	Do not translate the address.
IPSec rule (Extended only)	Encrypt traffic with matching address.	Do not encrypt traffic. Allow it to be sent unencrypted.
Access rule used in route map	Protect matching addresses from NAT translation.	Do not protect matching addresses from NAT translation.

Services and Ports

This topic lists services you can specify in rules, and their corresponding port numbers. It also provides a short description of each service.

This topic is divided into the following areas:

- TCP Services
- UDP Services
- ICMP Message Types

- IP Services
- Services That Can Be Specified in Inspection Rules

TCP Services

TCP Service	Port Number	Description
bgp	179	Border Gateway Protocol.BGP exchanges reachability information with other systems that use the BGP protocol
chargen	19	Character generator.
cmd	514	Remote commands. Similar to exec except that cmd has automatic authentication
daytime	13	Daytime
discard	9	Discard
domain	53	Domain Name Service. System used on the Internet for translating names of network nodes into addresses.
echo	7	Echo request. Message sent when ping command is issued.
exec	512	Remote process execution
finger	79	Finger. Application that determines whether a person has an account at a particular internet site.
ftp	21	File Transfer Protocol. Application-layer protocol used for transferring files between network nodes.
ftp-data	20	FTP data connections
gopher	70	Gopher. A distributed document delivery system.
hostname	101	NIC hostname server
ident	113	Ident Protocol
irc	194	Internet Relay Chat. A world-wide protocol that allows users to exchange text messages with each other in real time.
klogin	543	Kerberos login. Kerberos is a developing standard for authenticating network users.
kshell	544	Kerberos shell
login	513	Login

TCP Service	Port Number	Description
lpd	515	Line Printer Daemon. A protocol used to send print jobs between UNIX systems.
nntp	119	Network News Transport Protocol.
pim-auto-rp	496	Protocol-Independent Multicast Auto-RP. PIM is a multicast routing architecture that allows the addition of multicast IP routing on existing IP networks.
pop2	109	Post Office Protocol v2. Protocol that client e-mail applications use to retrieve mail from mail servers.
pop3	110	Post Office Protocol v3
smtp	25	Simple Mail Transport Protocol. Internet protocol providing e-mail services.
sunrpc	111	SUN Remote Procedure Call. See rpc.
syslog	514	System log.

UDP Services

UDP Service	Port Number	Description
biff	512	Used by mail system to notify users that new mail is received
bootpc	69	Bootstrap Protocol (BOOTP) client
bootps	67	Bootstrap Protocol (BOOTP) server
discard	9	Discard
dnsix	195	DNSIX security protocol auditing
domain	53	Domain Name Service (DNS)
echo	7	See echo.
isakmp	500	Internet Security Association and Key Management Protocol
mobile-ip	434	Mobile IP registration
nameserver	42	IEN116 name service (obsolete)
netbios-dgm	138	NetBios datagram service. Network Basic Input Output System. An API used by applications to request services from lower-level network processes.

UDP Service	Port Number	Description
netbios-ns	137	NetBios name service
netbios-ss	139	NetBios session service
ntp	123	Network Time Protocol. TCP protocol that ensures accurate local timekeeping with reference to radio and atomic clocks located on the Internet.
pim-auto-rp	496	Protocol Independent Multicast, reverse path flooding, dense mode
rip	520	Routing Information Protocol. A protocol used to exchange route information between routers.
snmp	161	Simple Network Management Protocol. A protocol used to monitor and control network devices.
snmptrap	162	SNMP trap. A system management notification of some event that occurred on the remotely managed system.
sunrpc	111	SUN Remote Procedure Call. RPCs are procedure calls that are built or specified by clients and executed on servers, with the results returned over the network to the client.
syslog	514	System log service.
tacacs	49	Terminal Access Controller Access Control System. Authentication protocol that provides remote access authentication and related services, such as logging.
talk	517	Talk. A protocol originally intended for communication between teletype terminals, but now a rendezvous port from which a TCP connection can be established.
tftp	69	Trivial File Transfer Protocol. Simplified version of FTP that allows files to be transferred between network nodes.
time	37	Time.
who	513	Port to databases showing who is logged in to machines on a local net and the load average of the machine
xdmcp	177	X-Display Manager Client Protocol. A protocol used for communications between X-Displays (clients) and X Display Managers.
non500-isakmp	4500	Internet Security Association and Key Management Protocol. This keyword is used when NAT-traversal port floating is required.

ICMP Message Types

ICMP Messages	Port Number	Description
alternate-address	6	Alternate host address.
conversion-error	31	Sent to report a datagram conversion error.
echo	8	Type of message sent when ping command is issued.
echo-reply	0	Response to an echo-request (ping) message.
information-reply	16	Obsolete. Response to message sent by host to discover number of the network it is on. Replaced by DHCP.
information-request	15	Obsolete. Message sent by host to discover number of the network it is on. Replaced by DHCP.
mask-reply	18	Response to message sent by host to discover network mask for the network it is on.
mask-request	17	Obsolete. Message sent by host to discover network mask for the network it is on.
mobile-redirect	32	Mobile host redirect. Sent to inform a mobile host of a better first-hop node on the path to a destination.
parameter-problem	12	Message generated in response to packet with problem in its header.
redirect	5	Sent to inform a host of a better first-hop node on the path to a destination.
router-advertisement	9	Sent out periodically, or in response to a router solicitation.
router-solicitation	10	Messages sent in order to prompt routers to generate router advertisements messages quickly.
source-quench	4	Sent when insufficient buffer space is available to queue packets for transmission to next hop, or by destination router when packets are arriving too quickly to be processed.
time-exceeded	11	Sent to indicate received packet't time to live field has reached zero.
timestamp-reply	14	Reply to request for timestamp to be used for synchronization between two devices.

ICMP Messages	Port Number	Description
timestamp-request	13	Request for timestamp to be used for synchronization between two devices.
traceroute	30	Message sent in reply to a host that has issued a traceroute request.
unreachable	3	Destination unreachable. Packet cannot be delivered for reasons other than congestion.

IP Services

IP Services	Port Number	Description
aahp	51	
eigrp	88	Enhanced Interior Gateway Routing Protocol. Advanced version of IGRP developed by Cisco.
esp	50	Extended Services Processor.
icmp	1	Internet Control Message Protocol. Network layer protocol that reports errors and provides other information relevant to IP packet processing.
igmp	2	Internet Group Management Protocol. Used by IP hosts to report their multicast group memberships to adjacent multicast routers.
ip	0	Internet Protocol. Network layer protocol offering connectionless internetwork service.
ipinip	4	IP-in-IP encapsulation.
nos	94	network operating system. A distributed file system protocol.
ospf	89	Open Shortest Path First. A link-state hierarchical routing algorithm.
pcp	108	Payload Compression Protocol
pim	103	Protocol-Independent Multicast. PIM is a multicast routing architecture that allows the addition of multicast IP routing on existing IP networks.

IP Services	Port Number	Description
tcp	6	Transmission Control Protocol. Connection-oriented transport layer protocol that provides reliable full-duplex data transmission.
udp	17	User Datagram Protocol. Connectionless transport layer protocol in the TCP/IP protocol stack.

Services That Can Be Specified in Inspection Rules

Protocol	Description
cuseeme	Video conferencing protocol.
fragment	Specifies that the rule perform fragment inspection.
ftp	See ftp.
h323	See H.323.
http	See HTTP.
icmp	See icmp.
netshow	NetShow. A streaming video protocol.
rcmd	Remote Comman d. A protocol used when commands are executed on a remote system by a local system.
realaudio	RealAudio. A streaming audio protocol.
rpc	Remote Procedure Call. RPCs are procedure calls that are built or specified by clients and executed on servers, with the results returned over the network to the client
rtsp	Real-Time Streaming Protocol. An application-level protocol used to control delivery of data with real-time properties.
sip	Session Initiation Protocol. Sip is a telephony protocol used to integrate telephony services and data services.
skinny	A telephony protocol enabling telephony clients to be H.323 compliant.
smtp	See smtp.
sqlnet	Protocol for network enabled databases.
streamworks	StreamWorks protocol. Streaming video protocol.

Protocol	Description
tcp	See tcp.
tftp	See tftp.
udp	See udp.
vdolive	VDOLive protocol. A streaming video protocol.

More About NAT

This section provides scenario information that may help you in completing the NAT Translation Rule windows, and other information that explains why NAT rules created using the CLI may not be editable in Cisco CP.

Static Address Translation Scenarios

The following scenarios show you how you can use the static address translation rules.

Scenario 1

You need to map an IP address for a single host to a public address. The address of the host is 10.12.12.3. The public address is 172.17.4.8.

The following table shows how the fields in the Add Address Translation Rule window would be used.

	Translate from Interface Fields		Translate to Interface Fields	
Static/Dynamic	IP Address	Net Mask	IP Address	Redirect Port
Static	10.12.12.3	Leave blank	172.17.4.8	Leave unchecked.

Result

The source address 10.12.12.3 is translated to the address 172.17.4.8 in packets leaving the router. If this is the only NAT rule for this network, 10.12.12.3 is the only address on the network that gets translated.

Scenario 2

You need to map each IP address in a network to a unique public IP address, and you do not want to create a separate rule for each mapping. The source network number is 10.l2.12.0, and the target network is 172.17.4.0. However, in this scenario, it is not necessary to know the source or target network numbers. It is sufficient to enter host addresses and a network mask.

The following table shows how the fields in the Add Address Translation Rule window would be used.

	Translate from Interface Fields		Translate to Interface Fields	
Static/Dynamic	**IP Address**	**Net Mask**	**IP Address**	**Redirect Port**
Static	10.12.12.35 (host)	255.255.255.0	172.17.4.8 (host)	Leave unchecked.

Result

NAT derives the “Translate from” network address from the host IP address and the subnet mask. NAT derives the “Translate to” network address from the net mask entered in the “Translate from” fields, and the “Translate to” IP address. The source IP address in any packet leaving the original network is translated to an address in the 172.17.4.0 network.

Scenario 3

You want to use the same global IP address for several hosts on the trusted network. Inbound traffic will contain a different port number based on the destination host.

The following table shows how the fields in the Add Address Translation Rule window would be used.

	Translate from... fields		Translate to... fields	
Static/Dynamic	**IP Address**	**Net Mask**	**IP Address**	**Redirect Port**
Static	10.12.12.3	Leave blank	172.17.4.8	UDP Original Port 137 Translated Port 139

Result

The source address 10.12.12.3 is translated to the address 172.17.4.8 in packets leaving the router. The port number in the Redirect port field is changed from 137 to 139. Return traffic carrying the destination address 172.17.4.8 is routed to port number 137 of the host with the IP address 10.12.12.3.

You need to create a separate entry for each host/port mapping that you want to create. You can use the same “Translated to” IP address in each entry, but you must enter a different “Translated from” IP address in each entry, and a different set of port numbers.

Scenario 4

You want source-"Translate from"-addresses to use the IP address that is assigned to the router's Fast Ethernet 0/1 interface 172.17.4.8. You also want to use the same global IP address for several hosts on the trusted network. Inbound traffic will contain a different port number based on the destination host. The following table shows how the fields in the Add Address Translation Rule window would be used:

	Translate from... fields		Translate to... fields	
Static/Dynamic	**IP Address**	**Net Mask**	**IP Address**	**Redirect Port**
Static	10.12.12.3	Leave blank	FastEthernet 0/1	UDP Original Port 137 Translated Port 139

Result

The source address 10.12.12.3 is translated to the address 172.17.4.8 in packets leaving the router. The port number in the Redirect port field is changed from 137 to 139. Return traffic carrying the destination address 172.17.4.8 & port 139 is routed to port number 137 of the host with the IP address 10.12.12.3.

Dynamic Address Translation Scenarios

The following scenarios show you how you can use dynamic address translation rules. These scenarios are applicable whether you select from inside-to-outside, or from outside-to-inside.

Scenario 1

You want source–"Translate from"–addresses to use the IP address that is assigned to the router's Fast Ethernet 0/1 interface 172.17.4.8. Port Address Translation (PAT) would be used to distinguish traffic associated with different hosts. The ACL rule you use to define the "Translate from" addresses is configured as shown below:

```
access-list 7 deny host 10.10.10.1
access-list 7 permit 10.10.10.0 0.0.0.255
```

When used in a NAT rule this access rule would allow any host in the 10.10.10.0 network, except the one with the address 10.10.10.1 to receive address translation.

The following table shows how the fields in the Add Address Translation Rule window would be used.

	Translate from... fields	Translate to... fields		
Static/Dynamic	ACL Rule	Type	Interface	Address Pool
Dynamic	7	Interface	FastEthernet0/1	Disabled

Result

Traffic from all hosts on the 10.10.10.0 network would have the source IP address translated to 172.17.4.8. PAT would be used to distinguish traffic associated with different hosts.

Scenario 2

You want the host addresses specified in access-list 7 in the previous scenario to use addresses from a pool you define. If the addresses in the pool become depleted, you want the router to use PAT to satisfy additional requests for addresses from the pool.

The following table shows how the fields in the Address Pool window would be used for this scenario.

Pool Name	Port Address Translation	IP Address fields		Network Mask
Pool 1	Checked	172.16.131.2	172.16.131.10	255.255.255.0

The following table shows how the fields in the Add Address Translation Rule window would be used for this scenario.

	Translate from... fields	Translate to... fields		
Static/Dynamic	ACL Rule	Type	Interface	Address Pool
Dynamic	7	Address Pool	Disabled	Pool 1

Result

Hosts IP addresses in the network 10.10.10.0 are translated to IP address in the range 172.16.131.2 to 172.16.131.10. When there are more requests for address translation than available addresses in Pool 1, the same address is used to satisfy subsequent requests, and PAT is used to distinguish between the hosts using the address.

Reasons that Cisco CP Cannot Edit a NAT Rule

A previously configured NAT rule will be read-only and will not be configurable when a NAT static rule is configured with any of the following:

- The **inside source static** and **destination** Cisco IOS commands

- The **inside source static network** command with one of the keywords “extendable”, “no-alias”, or “no-payload”
- The **outside source static network** command with one of the keywords “extendable”, “no-alias”, or “no-payload”
- The **inside source static tcp** command with one of the keywords “no-alias” or “no-payload”
- The **inside source static udp** command with one of the keywords “no-alias” or “no-payload”
- The **outside source static tcp** command with one of the keywords “no-alias” or “no-payload”
- The **outside source static udp** command with one of the keywords “no-alias” or “no-payload”
- The **inside source static** command with one of the keywords “no-alias”, “no-payload”, “extendable”, “redundancy”, “route-map”, or “vrf”
- The **outside source static** command with one of the keywords “no-alias”, “no-payload”, “extendable”, or “add-route”
- The **inside source static** command with the keyword “esp”
- The **inside source static** command with the **interface** command

A NAT dynamic rule is configured with the Loopback interface

More About VPN

These topics contain more information about VPN, DMVPN, IPSec and IKE.

Cisco.com Resources

The following documents provide TAC resources and other information on VPN issues.

- How Virtual Private Networks Work—This document is available at the following link:

  http://www.cisco.com/en/US/tech/tk583/tk372/technologies_tech_note09186a0080094865.shtml

- Dynamic Multipoint IPSec VPNs (Using Multipoint GRE/NHRP to Scale IPSec VPNs)—This document is available at the following link:

  http://www.cisco.com/en/US/tech/tk583/tk372/technologies_white_paper09186a008018983e.shtml

- IPSecurity Troubleshooting–Understanding and Using Debug Commands—This document is available at the following link:

  http://www.cisco.com/en/US/tech/tk583/tk372/technologies_tech_note09186a00800949c5.shtml

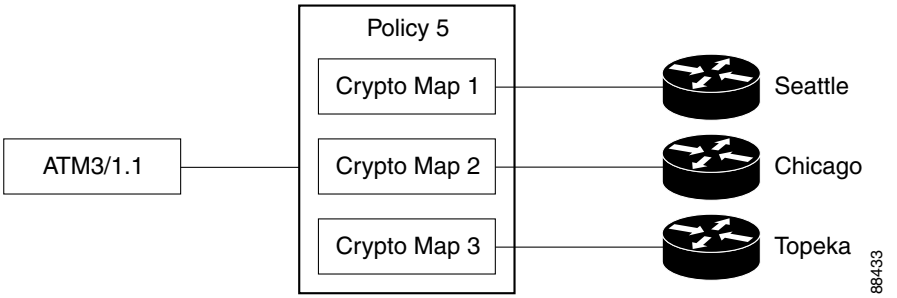
- Field Notices—Field notices are available at the following link:

  http://www.cisco.com/en/US/support/tsd_products_field_notice_summary.html

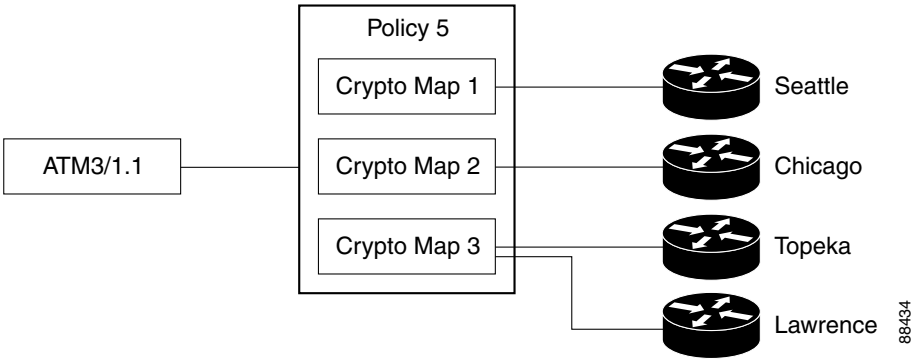
More about VPN Connections and IPSec Policies

A VPN connection is an association between a router interface and an IPSec policy. The building block of an IPSec policy is the crypto map. A crypto map specifies the following: a transform set and other parameters to govern encryption, the identity of one or more peers, and an IPSec rule that specifies which traffic will be encrypted. An IPSec policy can contain multiple crypto maps.

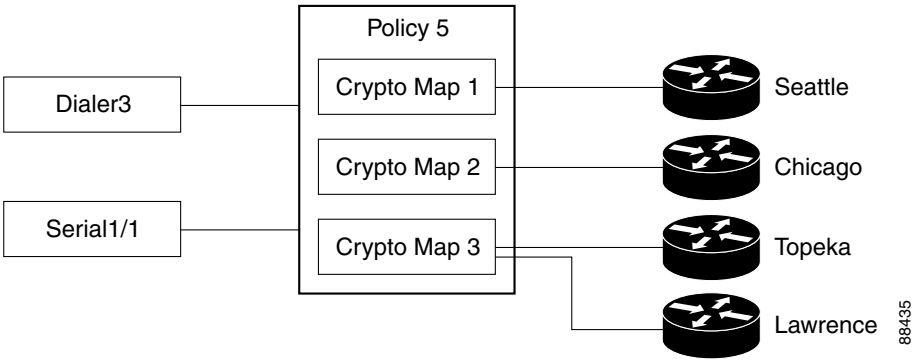
The following diagram shows an interface (ATM 3/1.1) associated with an IPSec policy. The policy has three crypto maps, each specifying a different peer system. The ATM 3/1.1 interface is thus associated with three VPN connections.



A crypto map can specify more than one peer for a connection. This may be done to provide redundancy. The following diagram shows the same interface and policy, but crypto map CM-3 specifies two peers: Topeka and Lawrence.



A router interface can be associated with only one IPSec policy. However, an IPSec policy can be associated with multiple router interfaces, and a crypto map can specify more than one peer for a connection. The following diagram shows two router interfaces associated with a policy, and a crypto map specifying two peers.



There are six VPN connections in this configuration, as both Dialer 3 and Serial 1/1 have connections to Seattle, Chicago, Topeka, and Lawrence. Cisco CP would show the links to Topeka and Lawrence as one connection for both interfaces.

More About IKE

IKE handles the following tasks:

- Authentication
- Session Negotiation
- Key Exchange
- IPSec Tunnel Negotiation and Configuration

Authentication

Authentication is arguably the most important task that IKE accomplishes, and it certainly is the most complicated. Whenever you negotiate something, it is of utmost importance that you know with whom you are negotiating. IKE can use one of several methods to authenticate negotiating parties to each other.

- **Pre-shared Key**. IKE uses a hashing technique to ensure that only someone who possesses the same key could have sent the IKE packets.
- **DSS or RSA digital signatures**. IKE uses public-key digital-signature cryptography to verify that each party is whom he or she claims to be.
- **RSA encryption**. IKE uses one of two methods to encrypt enough of the negotiation to ensure that only a party with the correct private key could continue the negotiation.

Note Cisco CP supports the pre-shared key method of authentication.

Session Negotiation

During session negotiation, IKE allows parties to negotiate how they will conduct authentication and how they will protect any future negotiations (that is, IPSec tunnel negotiation). The following items are negotiated:

- **Authentication Method**. This is one of the authentication methods listed above.
- **Key Exchange Algorithm**. This is a mathematical technique for securely exchanging cryptographic keys over a public medium (that is, Diffie-Hellman). The keys are used in the encryption and packet-signature algorithms.

- **Encryption Algorithm**: DES, 3DES, or AES
- **Packet Signature Algorithm**: MD5 or SHA-1

Key Exchange

IKE uses the negotiated key-exchange method (see "Session Negotiation" above) to create enough bits of cryptographic keying material to secure future transactions. This method ensures that each IKE session will be protected with a new, secure set of keys.

Authentication, session negotiation, and key exchange constitute phase 1 of an IKE negotiation.

IPSec Tunnel Negotiation and Configuration

After IKE has finished negotiating a secure method for exchanging information (phase 1), we use IKE to negotiate an IPSec tunnel. This is accomplished in IKE phase 2. In this exchange, IKE creates fresh keying material for the IPSec tunnel to use (either using the IKE phase 1 keys as a base or by performing a new key exchange). The encryption and authentication algorithms for this tunnel are also negotiated.

More About IKE Policies

When the IKE negotiation begins, IKE looks for an IKE policy that is the same on both peers. The peer that initiates the negotiation will send all its policies to the remote peer, and the remote peer will try to find a match. The remote peer looks for a match by comparing its own highest priority policy against the other peer's received policies. The remote peer checks each of its policies in order of its priority (highest first) until a match is found.

A match is made when both policies from the two peers contain the same encryption, hash, authentication, and Diffie-Hellman parameter values, and when the remote peer's policy specifies a lifetime less than or equal to the lifetime in the policy being compared. If the lifetimes are not identical, the shorter lifetime-from the remote peer's policy will be used.

Allowable Transform Combinations

To define a transform set, you specify one to three transforms. Each transform represents an IPSec security protocol (AH or ESP) plus the algorithm that you want to use. When the particular transform set is used during negotiations for IPSec security associations, the entire transform set (the combination of protocols, algorithms, and other settings) must match a transform set at the remote peer.

The following table lists the acceptable transform combination selections for the AH and ESP protocols.

AH Transform (***Pick up to one***)	**ESP Encryption Transform** (***Pick up to one***)	**Authentication Transform** (***Pick up to one***)	**IP Compression Transform** (***Pick up to one***)	**Examples** *(Total of 3 transforms allowed)*
ah-md5-hmac ah-sha-hmac	esp-des esp-3des esp-null es-aes-128 esp-aes-192 esp-aes-256 esp-seal	esp-md5-hmac esp-sha-hmac	comp-lzs	1. ah-md5-hmac 2. esp-3des and esp-md5-hmac 3. ah-sha-hmac, esp-des, and esp-sha-hmac

The following table describes each of the transforms.

Transform	Description
ah-md5-hmac	AH with the MD5 (HMAC variant) authentication algorithm.
ah-sha-hmac	AH with the SHA (HMAC variant) authentication algorithm.
esp-des	ESP with the 56-bit DES encryption algorithm.
esp-3des	ESP with the 168-bit DES encryption algorithm (3DES or Triple DES)
esp-null	Null encryption algorithm.
esp-seal	ESP with the 160-bit encryption key Software Encryption Algorithm (SEAL) encryption algorithm.

Transform	Description
esp-md5-hmac	ESP with the MD5 (HMAC variant) authentication algorithm.
es-aes-128	ESP with Advanced Encryption Standard (AES). Encryption with a 128-bit key
esp-aes-192	ESP with AES. Encryption with a 192-bit key.
esp-aes-256	ESP with AES. Encryption with a 256-bit key.
esp-sha-hmac	ESP with the SHA (HMAC variant) authentication algorithm.
comp-lzs	IP compression with the LZS algorithm.

Examples

The following are examples of permissible transform combinations:

- ah-md5-hmac
- esp-des
- esp-3des and esp-md5-hmac
- ah-sha-hmac, esp-des, and esp-sha-hmac
- comp-lzs

Reasons Why a Serial Interface or Subinterface Configuration May Be Read-Only

A previously configured Serial interface or subinterface will be read-only and will not be configurable in the following cases:

- The interface is configured with the **encapsulation ppp** and **ppp multilink ...** Cisco IOS commands.
- The interface is configured with the **encapsulation hdlc** and **ip address negotiated** commands.
- The interface is part of a SERIAL_CSUDSU_56K WIC.
- The interface is part of a Sync/Async WIC configured with the **physical-layer async** command.

- The interface is configured with the **encapsulation frame-relay** command with an IP address on the main interface.
- The interface encapsulation is not “hdlc,” “ppp,” or “frame-relay.”
- The **encapsulation frame-relay ...** command contains the **mfr ...** option.
- The interface is configured with the **encapsulation ppp** command, but the PPP configuration contains unsupported commands.
- The interface is configured with the **encapsulation frame-relay** and **frame-relay map ...** commands.
- The main interface is configured with the **encapsulation frame-relay** and **frame-relay interface-dlci ...** commands.
- The main interface is configured with the **encapsulation frame-relay** command and the subinterface is configured with the **frame-relay priority-dlci-group ...** command.
- The subinterface is configured with the **interface-dlci ...** command that contains any of the keywords “ppp,” “protocol,” or “switched.”
- The subinterface type is “multipoint,” instead of “point-to-point.”
- The subinterface is configured with any encapsulation other than “frame-relay.”

Reasons Why an ATM Interface or Subinterface Configuration May Be Read-Only

A previously configured ATM interface or subinterface will be read-only and will not be configurable in the following cases:

- It has a PVC with the **dialer pool-member** command.
- It has a PVC in which the protocol specified in the **protocol** command is not **ip.**
- It has a PVC with multiple **protocol ip** commands.
- The encapsulation on the PVC is neither “aal5mux,” nor “aal5snap.”
- If the encapsulation protocol on aal5mux is not “ip.”
- If the IP Address is not configured on the PVC in the **protocol ip** command.

- If the “dial-on-demand” option is configured on the **pppoe-client** command.
- If there is more than 1 PVC configured on the interface.
- If the encapsulation on the associated dialer is blank or is not “ppp.”
- If no IP address is configured on the associated dialer.
- If VPDN is required (which is determined dynamically from the Cisco IOS image) but is not configured for this connection.
- If the operating mode is “CO” on an SHDSL interface (ATM main interfaces only).
- If no IP address is configured on the interface and the interface is not configured for PPPoE (ATM subinterfaces only).
- The interface has an IP address but no associated PVC.
- The interface has a PVC but no associated IP address and is not configured for PPPoE.
- The **bridge-group** command is configured on the interface.
- If the main interface has one or move PVCs as well as one or more subinterfaces.
- If the main interface is not configurable (ATM subinterfaces only).
- It is a multipoint interface (ATM subinterfaces only).

Reasons Why an Ethernet Interface Configuration May Be Read-Only

A previously configured Ethernet LAN or WAN interface or will be read-only and will not be configurable in the following cases:

- If the LAN interface has been configured as a DHCP server, and has been configured with an IP-helper address.

Reasons Why an ISDN BRI Interface Configuration May Be Read-Only

A previously configured ISDN BRI interface will be read-only and will not be configurable in the following cases:

- An IP address is assigned to the ISDN BRI interface.
- Encapsulation other than ppp is configured on the ISDN BRI interface.
- The **dialer-group** or **dialer string** command is configured on the ISDN BRI interface.
- **dialer pool-member** <*x*> is configured on the ISDN BRI interface, but the corresponding dialer interface <*x*> is not present.
- Multiple dialer pool-members are configured on the ISDN BRI interface.
- The **dialer map** command is configured on the ISDN BRI interface.
- Encapsulation other than ppp is configured on the dialer interface.
- Either **dialer-group** or **dialer-pool** is not configured on the dialer interface.
- **dialer-group** <*x*> is configured on the dialer interface, but the corresponding **dialer -list** <*x*> **protocol** command is not configured.
- **dialer idle-timeout** <*num*> with optional keyword (either/inbound) is configured on the dialer interface.
- **dialer string** command with optional keyword **class** is configured on the dialer interface.
- If using the ISDN BRI connection as a backup connection, once the backup configuration is through Cisco CP, if any of the conditions below occur, the backup connection will be shown as read only:
  - The default route through the primary interface is removed
  - The backup interface default route is not configured
  - ip local policy is removed
  - **track /rtr** or **both** is not configured
  - route-map is removed
  - Access-list is removed or access-list is modified (for example, tracking ip address is modified)

  - The Cisco CP-supported interfaces are configured with unsupported configurations
  - The primary interfaces are not supported by Cisco CP

Reasons Why an Analog Modem Interface Configuration May Be Read-Only

A previously configured analog modem interface or will be read-only and will not be configurable in the following cases:

- An IP address is assigned to the asynchronous interface.
- Encapsulation other than ppp is configured on the asynchronous interface.
- The **dialer-group** or **dialer string** command is configured on the asynchronous interface.
- Async mode **interactive** is configured on the asynchronous interface.
- **dialer pool-member** <*x*> is configured on the asynchronous interface, but the corresponding dialer interface <*x*> is not present.
- Multiple dialer pool-members are configured on the asynchronous interface.
- Encapsulation other than ppp is configured on the dialer interface.
- Either **dialer-group** or **dialer-pool** is not configured on the dialer interface.
- **dialer-group** <*x*> is configured on the dialer interface, but the corresponding **dialer -list** <*x*> **protocol** command is not configured.
- **dialer idle-timeout** <*num*> with optional keyword (either/inbound) is configured on the dialer interface.
- In line configuration collection mode, **modem input** is not configured.
- In line configuration collection mode, **autoselect ppp** is not configured.
- If using the analog modem connection as a backup connection, once the backup configuration is through Cisco CP, if any of the conditions below occur, the backup connection will be shown as read only:
  - The default route through the primary interface is removed
  - The backup interface default route is not configured
  - ip local policy is removed

- **track /rtr** or **both** is not configured
- route-map is removed
- Access-list is removed or access-list is modified (for example, tracking ip address is modified)
- The Cisco CP-supported interfaces are configured with unsupported configurations
- The primary interfaces are not supported by Cisco CP

DMVPN Configuration Recommendations

This help topic contains recommendations on how you should proceed when configuring routers in a DMVPN.

Configure the Hub First

It is important to configure the hub first because spokes must be configured using information about the hub. If you are configuring a hub, you can use the Spoke Configuration feature available in the Summary window to generate a text file that contains a procedure that you can send to spoke administrators so that they can configure the spokes with the correct hub information. If you are configuring a spoke, you must obtain the correct information about the hub before you begin.

Assigning Spoke Addresses

All routers in the DMVPN must be in the same subnet. Therefore, the hub administrator must assign addresses in the subnet to the spoke routers so that address conflicts do not occur, and so that everyone is using the same subnet mask.

Recommendations for Configuring Routing Protocols for DMVPN

The following are guidelines that you should note when configuring routing protocols for DMVPN. You can choose to ignore these guidelines, but Cisco CP has not been tested in scenarios outside the guidelines and may not be able to let you edit configurations within Cisco CP after you enter them.

These recommendations are listed in best-choice order:

- If a routing process exists that advertises inside networks, use this process to advertise networks to the DMVPN.
- If a routing process exists that advertises tunnel networks for VPNs, for example GRE over IPSec tunnels, use this process to advertise the DMVPN networks.
- If a routing process exists that advertises networks for the WAN interfaces, then be sure to use an AS number or process ID that the WAN interfaces do not use to advertise networks.
- When you configure DMVPN routing information Cisco CP checks whether the Autonomous System number (EIGRP) or area ID (OSPF) you enter is already used to advertise networks for the router's physical interface. If the value is already in use, Cisco CP informs you of this and recommends that you either use a new value, or that you select a different routing protocol to advertise networks on the DMVPN.

Using Interfaces with Dialup Configurations

Selecting an interface that uses a dialup connection may cause the connection to be always up. You can examine supported interfaces in Interfaces and Connections to determine if a dialup connection, such as an ISDN or Async connection has been configured for the physical interface you selected.

Ping the Hub Before You Start Spoke Configuration

Before configuring a spoke router, you should test connectivity to the hub by issuing the ping command. If the ping does not succeed, you must configure a route to the hub.

Routing and Security White Papers

A number of white papers are available that describe how Cisco CP Routing and Security features can be used. These white papers are available at the following link.

http://www.cisco.com/en/US/products/sw/secursw/ps5318/prod_technical_reference_list.html

The routing and security features available in Cisco CP were first made available in Cisco Router and Security Device Manager.

GLOSSARY

Symbols and Numerics

3DES Triple DES. An encryption algorithm that uses three 56-bit DES encryption keys (effectively 168 bits) in quick succession. An alternative 3DES version uses just two 56-bit DES keys, but uses one of them twice, resulting effectively in a 112-bit key length. Legal for use only in the United States. See DES.

802.1x 802.1x is an IEEE standard for media-level access control, offering the capability to permit or deny network connectivity, control VLAN access and apply traffic policy, based on user or machine identity.

A

AAA Authentication, Authorization, and Accounting. Pronounced “triple-A.”

AAL5-SNAP ATM Adaptation Layer 5 Subnetwork Access Protocol.

AAL5-MUX ATM Adaptation Layer 5 Multiplexing.

access control, access control rule information entered into the configuration which allows you to specify what type of traffic to permit or deny into an the interface. By default, traffic that is not explicitly permitted is denied. Access control rules are composed of access control entries (ACEs).

ACE access control entry. An entry in an ACL that specifies a source host or network and whether or not traffic from that host is permitted or denied. An ACE can also specify a destination host or network, and the type of traffic.

ACL access control list. Information on a device that specifies which entities are permitted to access that device or the networks behind that device. Access control lists consist of one or more access control entries (ACE).

ACS Cisco Secure Access Control Server. Cisco software that can implement a RADIUS server or a TACACS+ server. The ACS is used to store policy databases used by Easy VPN, NAC and other features to control access to the network.

address translation The translation of a network address and/or port to another network address/or port. See also IP address, NAT, PAT, Static PAT.

ADSL asymmetric digital subscriber line.

aggressive mode A mode of establishing ISAKMP SAs that simplifies IKE authentication negotiation (phase 1) between two or more IPSec peers. Aggressive mode is faster than main mode, but is not as secure. See main mode, quick mode.

AES Advanced Encryption Standard

AES-CCMP Advanced Encryption Standard-Counter Mode with Cipher Block Chaining Message Authentication Code Protocol. AES-CCMP is required for Wi-Fi Protected Access 2 (WPA2) and IEEE 802.11i wireless LAN security.

AH Authentication Header. This is an older IPSec protocol that is less important in most networks than ESP. AH provides authentication services but does not provide encryption services. It is provided to ensure compatibility with IPSec peers that do not support ESP, which provides both authentication and encryption.

AH-MD5-HMAC Authentication Header with the MD5 (HMAC variant) hash algorithm.

AH-SHA-HMAC Authentication Header with the SHA (HMAC variant) hash algorithm.

AHP Authentication Header Protocol. A protocol that provides source host authentication, and data integrity. AHP does not provide secrecy.

AIM Advanced Integrated Module.

algorithm A logical sequence of steps for solving a problem. Security algorithms pertain to either data encryption or authentication.

DES and 3DES are two examples of data encryption algorithms.

Examples of encryption-decryption algorithms include block cipher, CBC, null cipher, and stream cipher.

Authentication algorithms include hashes such as MD5 and SHA.

AMI alternate mark inversion.

ARP Address Resolution Protocol—A low-level TCP/IP protocol that maps a node hardware address (called a *MAC address*) to its IP address.

ASA Adaptive Security Algorithm. Allows one-way (inside to outside) connections without an explicit configuration for each internal system and application.

asymmetric encryption Also called *public key systems*, this approach allows anyone to obtain access to anyone else's public key and therefore send an encrypted message to that person using the public key.

asymmetric keys A pair of mathematically related cryptographic keys. The public key encrypts information that only the private key can decrypt, and vice versa. Additionally, the private key signs data that only the public key can authenticate.

ATM Asynchronous Transfer Mode. International standard for cell relay in which multiple service types (such as voice, video, and data) are conveyed in fixed-length (53-byte) cells. Fixed-length cells allow cell processing to occur in hardware, thereby reducing transit delays.

authenticate To establish the truth of an identity.

authentication In security, the verification of the identity of a person or process. Authentication establishes the integrity of a data stream, ensuring that it was not tampered with in transit, and providing confirmation of the data stream’s origin.

B

BC Committed Burst. BC is a QoS policing parameter that specifies in bits (or bytes) per burst how much traffic can be sent within a given unit of time to not create scheduling concerns.

BE Excess Burst. BC is a QoS policing parameter that specifies how large traffic bursts can be before all traffic exceeds the rate limit. Traffic that falls between the normal burst size and the excess burst size exceeds the rate limit with a probability that increases as the burst size increases.

BOOTP Bootstrap Protocol. The protocol used by a network node to determine the IP address of its Ethernet interfaces to affect network booting.

BSSID Basic Service Set Identifier. BSSIDs are identifiers used in 802.11g radios. They are similar to MAC addresses

burst rate The number of bytes that a traffic burst must not exceed.

BVI Bridge Group Virtual Interface. Logical Layer 3-only interface associated with a bridge group when IRB is configured.

C

C3PL Cisco Common Classification Policy Language. C3PL is a structured replacement for feature-specific configuration commands and allows configurable functionality to be expressed in terms of an event, a condition, and an action.

CA Certification Authority. A trusted third-party entity that issues and/or revokes digital certificates. Sometimes referred to as a *notary* or a *certifying authority.* Within a given CA's domain, each device needs only its own certificate and the CA's public key to authenticate every other device in that domain.

CA certificate A digital certificate granted to one certification authority (CA) by another certification authority.

CA server Certification Authority server. A network host that is used to issue and/or revoke digital certificates.

cache A temporary repository of information accumulated from previous task executions that can be reused, decreasing the time required to perform the tasks.

CBAC Context-based Access Control. Protocol that provides internal users with secure access control for each application and for all traffic across network perimeters. CBAC scrutinizes both source and destination addresses and tracks each application connection status.

CBWFQ Class-Based Weighted Fair Queuing. CBWFQ provides support for user-defined traffic classes. For CBWFQ, you define traffic classes based on match criteria including protocols, access control lists (ACLs), and input interfaces.

CDP Cisco Discovery Protocol. A media- and protocol-independent device-discovery protocol that runs on all Cisco-manufactured equipment including routers, access servers, bridges, and switches. Using CDP, a device can advertise its existence to other devices and receive information about other devices on the same LAN or on the remote side of a WAN.

CDP Certificate Revocation List Distribution Point. A location from where a Certificate Revocation List can be retrieved. A CDP is usually an HTTP or LDAP URL

CEP Certificate Enrollment Protocol. A certificate management protocol. CEP is an early implementation of Certificate Request Syntax (CRS), a standard proposed to the Internet Engineering Task Force (IETF). CEP specifies how a device communicates with a CA, including how to retrieve the public key of the CA, how to enroll a device with the CA, and how to retrieve a certificate revocation list (CRL). CEP uses PKCS (Public Key Cryptography Standards) 7 and 10 as key component technologies. The public key infrastructure working group (PKIX) of the IETF is working to standardize a protocol for these functions, either CRS or an equivalent. When an IETF standard is stable, Cisco will add support for it. CEP was jointly developed by Cisco Systems and VeriSign, Inc.

certificate See digital certificate.

certificate identity An X.509 certificate contains within it information regarding the identity of whichever device or entity possesses that certificate. The identification information is then examined during each subsequent instance of peer verification and authentication. However, certificate identities can be vulnerable to spoofing attacks.

CET Cisco Encryption Technology. Proprietary network layer encryption introduced in Cisco IOS Release 11.2. CET provides network data encryption at the IP packet level and implements the following standards: DH, DSS, and 40- and 56-bit DES.

CHAP Challenge Handshake Authentication Protocol. Security feature supported on lines using PPP encapsulation that prevents unauthorized access. CHAP does not itself prevent unauthorized access, it merely identifies the remote end. The router or access server then determines whether that user is allowed access. See also PAP.

chargen Character Generation. Via TCP, a service that sends a continual stream of characters until stopped by the client. Via UDP, the server sends a random number of characters each time the client sends a datagram.

checksum Computational method for checking the integrity of transmitted data, computed from a sequence of octets taken through a series of arithmetic operations. The recipient recomputes the value and compares it for verification.

Cisco CP Cisco Configuration Professional. Cisco CP is an Internet browser-based software tool designed to configure LAN, WAN, and security features on a router.

cipher An encryption-decryption algorithm.

ciphertext Encrypted, unreadable data, prior to its decryption.

CIR Committed Information Rate. A configured long-term average committed rate to enforce.

class map

class maps Used by zone-based firewall policies to specify traffic that is to be handled according to the actions specified in a policy map. A class map can specify a type of traffic, and can also specify an ACL to define the source and designating of the traffic.

clear channel A clear channel is one through which non-encrypted traffic can flow. Clear channels place no security restrictions on transmitted data.

cleartext Decrypted text. Also called *plaintext*.

CLI command-line interface. The primary interface for entering configuration and monitoring commands to the router. Refer to the Configuration Guide for the router you are configuring for information on what commands you can enter from the CLI.

client/server computing Term used to describe distributed computing (processing) network systems in which transaction responsibilities are divided into two parts: client (front end) and server (back end). Also called distributed computing. See also RPC.

WCM WAAS Central Manager. Each WAE-E must register with the WCM in order to be able to communicate with the WAE-C.

Cisco Unified CME Cisco Manager Express. Cisco Unified CME provides call-processing services to voice over IP (VoIP) gateways.

CNS Cisco Networking Services. A suite of services that support scalable network deployment, configuration, service-assurance monitoring, and service delivery.

comp-lzs An IP compression algorithm.

Configuration, Config, Config File The file on the router that holds the settings, preferences, and properties you can administer using Cisco CP.

content engine In the context of a WAAS solution, a cache of web content located on the network.

cookie A cookie is a web browser feature which stores or retrieves information, such as a user's preferences, to persistent storage. In Netscape and Internet Explorer, cookies are implemented by saving a small text file on your local hard drive. The file can be loaded the next time you run a Java applet or visit a website. In this way information unique to you as a user can be saved between sessions. The maximum size of a cookie is approximately 4KB.

CPE customer premises equipment.

CRL certificate revocation list. A list maintained and signed by a certificate authority (CA) of all the unexpired but revoked digital certificates.

cryptography Mathematical and scientific techniques for keeping data private, authentic, unmodified, and non-repudiated.

crypto map — In Cisco CP, crypto maps specify which traffic should be protected by IPSec, where IPSec-protected traffic should be sent, and what IPSec transform sets should be applied to this traffic.

cTCP — Cisco Tunneling Control Protocol. cTCP is also called TCP over IPSec, or TCP traversal. cTCP is a protocol that encapsulates ESP and IKE traffic in the TCP header, so that firewalls in between the client and the server or headend device permit this traffic, considering it as TCP traffic.

CUE — Cisco Unity Express. Cisco Unity Express offers voicemail and automated-attendant capabilities for IP phone users connected to Cisco Unified Call Manager Express

D

data confidentiality — The result of data encryption that prevents the disclosure of information to unauthorized individuals, entities, or processes. This information can be either data at the application level, or communication parameters. See traffic flow confidentiality or traffic analysis.

data integrity — The presumed accuracy of transmitted data — signifying the sender's authenticity and the absence of data tampering.

data origin authentication — One function of a non-repudiation service.

decryption — Reverse application of an encryption algorithm to encrypted data, thereby restoring that data to its original, unencrypted state.

default gateway — The gateway of last resort. The gateway to which a packet is routed when its destination address does not match any entries in the routing table.

delta file — A file that Cisco IOS IPS creates to store changes made to signatures.

DES — Data Encryption Standard. Standard cryptographic algorithm developed and standardized by the U.S. National Institute of Standards and Technology (NIST). Uses a secret 56-bit encryption key. The DES algorithm is included in many encryption standards.

DHCP Dynamic Host Configuration Protocol. Provides a mechanism for allocating IP addresses to hosts dynamically, so that addresses can be reused when hosts no longer need them.

DH, Diffie-Hellman A public key cryptography protocol that allows two parties to establish a shared secret over insecure communications channels. Diffie-Hellman is used within Internet Key Exchange (IKE) to establish session keys. Diffie-Hellman is a component of Oakley key exchange.

Diffie-Hellman key exchange A public key cryptography protocol that allows two parties to establish a shared secret over insecure communication channels. Diffie-Hellman is used within Internet Key Exchange (IKE) to establish session keys. Diffie-Hellman is a component of Oakley key exchange. Cisco IOS software supports 768-bit and 1024-bit Diffie-Hellman groups.

digest The output of a hash function.

digital certificate A cryptographically signed, digital representation of user or device attributes that binds a key to an identity. A unique certificate attached to a public key provides evidence that the key has not been compromised. A certificate is issued and signed by a trusted certification authority, and binds a public key to its owner. Certificates typically include the owner's name, the owner's public key, the certificate's serial number, and the certificate's expiration date. Other information might also be present. See X.509.

digital signature An authentication method that permits the easy discovery of data forgery, and prevents repudiation. Additionally, the use of digital signatures allows for verification that a transmission has been received intact. Typically includes a transmission time stamp.

distributed key A shared cryptographic key that is divided into pieces, with each piece provided to a different participant.

DLCI data-link connection identifier. In Frame Relay connections, the identifier for a particular data link connection between two endpoints.

DMVPN Dynamic multipoint virtual private network. A virtual private network in which routers are arranged in a logical hub and spoke topology, and in which the hubs have point-to-point GRE over IPSec connections with the hub. DMVPN uses GRE and NHRP to enable the flow of packets to destinations in the network.

single DMVPN A router with a single DMVPN configuration has a connection to one DMVPN hub, and has one configured GRE tunnel for DMVPN communication.The GRE tunnel addresses for the hub and spokes must be in the same subnet.

DMZ demilitarized zone. A DMZ is a buffer zone between the Internet, and your private networks. It can be a public network typically used for Web, FTP and E-Mail servers that are accessed by external clients on the Internet. Placing these public access servers on a separate isolated network provides an extra measure of security for your internal network.

DN Distinguished Name. A unique identifier for a Certification Authority customer, included in each of that customer's certificates received from that Certification Authority. The DN typically includes the user's common name, the name of that user's company or organization, the user's two-letter country code, an e-mail address used to contact the user, the user's telephone number, the user's department number, and the city in which the user resides.

DNS Domain Name System (or Service). An Internet service that translates domain names, which are composed of letters, into IP addresses, which are composed of numbers.

domain name The familiar, easy-to-remember name of a host on the Internet that corresponds to its IP address.

DPD dead peer detection. DPD determines if a peer is still active by sending periodic keepalive messages to which the peer is supposed to respond. If the peer does not respond within a specified amount of time, the connection is terminated.

DRAM dynamic random access memory. RAM that stores information in capacitors that must be periodically refreshed.

DSCP Differentiated Services Code Point. DSCP markings can be used to classify traffic for QoS. See also NBAR

DSLAM digital subscriber line access multiplexer.

DSS digital signature standard. Also called *digital signature algorithm* (DSA), the DSS algorithm is part of many public-key standards for cryptographic signatures.

DVTI Dynamic Virtual Tunnel Interface. A DVTI is a routable interface that is able to selectively send traffic to different destinations. DVTIs are not statically mapped to physical interfaces. Thus they are able to send and receive encrypted data over any physical interface.

dynamic routing Routing that adjusts automatically to network topology or traffic changes. Also called adaptive routing.

E

E1 A wide-area digital transmission scheme used predominantly in Europe that carries data at a rate of 2.048 Mbps.

EAPoUDP Extensible Authentication Protocol over User Datagram Protocol. Sometimes shortened to EOU. The protocol used by a client and a NAD to perform posture validation.

EAP-FAST Extensible Authentication Protocol-Flexible Authentication via Secure Tunneling. A 802.1x EAP type developed by Cisco Systems to enable customers who cannot enforce strong password policies to deploy an 802.1x EAP type that does not require digital certificates.

Easy VPN A centralized VPN management solution based on the Cisco Unified Client Framework.A Cisco Easy VPN consists of two components: a Cisco Easy VPN Remote client, and a Cisco Easy VPN server.

ECHO See ping, ICMP.

eDonkey Also known as eDonkey 2000 or ED2K is an extremely large peer-to-peer file sharing network. eDonkey implements the (Multisource File Transmission Protocol (MFTP).

EIGRP Enhanced Interior Gateway Routing Protocol. Advanced version of IGRP developed by Cisco Systems. Provides superior convergence properties and operating efficiency, and combines the advantages of link state protocols with those of distance vector protocols.

encapsulation Wrapping of data in a particular protocol header. For example, Ethernet data is wrapped in a specific Ethernet header before network transit. Also, when bridging dissimilar networks, the entire frame from one network is simply placed in the header used by the data link layer protocol of the other network.

encrypt To crytographically produce ciphertext from plaintext.

encryption Application of a specific algorithm to data so as to alter the appearance of the data, making it incomprehensible to those who are not authorized to see the information.

enrollment proxy host The proxy server for a certificate enrollment server.

enrollment URL The enrollment URL is the HTTP path to a certification authority (CA) that your Cisco IOS router should follow when sending certificate requests. The URL includes either a DNS name or an IP address, and may be followed by a full path to the CA scripts.

ERR Event Risk Rating. ERR is used to control the level at which a user chooses to take actions in an effort to minimize false positives.

ESN Electronic Serial Numbers.

ESP Encapsulating Security Payload. An IPSec protocol that provides both data integrity and confidentiality. Also known as Encapsulating Security Payload, ESP provides confidentiality, data origin authentication, replay-detection, connectionless integrity, partial sequence integrity, and limited traffic flow confidentiality.

ESP_SEAL ESP with the 160-bit key SEAL (Software Encryption Algorithm) encryption algorithm. This feature was introduced in 12.3(7)T. The router must not have hardware IPSec encryption enabled in order to use this feature.

esp-3des ESP (Encapsulating Security Payload) transform with the 168-bit DES encryption algorithm (3DES or Triple DES).

esp-des ESP (Encapsulating Security Payload) transform with the 56-bit DES encryption algorithm.

ESP-MD5-HMAC ESP (Encapsulating Security Payload) transform using the MD5-variant SHA authentication algorithm.

esp-null ESP (Encapsulating Security Payload) transform that provides no encryption and no confidentiality.

ESP-SHA-HMAC ESP (Encapsulating Security Payload) transform using the HMAC-variant SHA authentication algorithm.

Ethernet A widely used LAN protocol invented by Xerox Corporation, and developed by Xerox, Intel, and Digital Equipment Corporation. Ethernet networks use CSMA/CD, and run over a variety of cable types at 10 Mbps, or at 100 Mbps. Ethernet is similar to the IEEE 802.3 series of standards.

Event action override Event action overrides are used in IOS IPS 5.x. They allow you to change the actions associated with an event based on the RR of that event.

event action override

expiration date The expiration date within a certificate or key indicates the end of its limited lifetime. The certificate or key is not trusted after its expiration date passes.

exception list In a NAC implementation, a list of hosts with static addresses that are allowed to bypass the NAC process. These hosts may be placed on the exception list because they do not have posture agents installed, or because they are hosts such as printers or Cisco IP phones.

extended rules A type of Access rule. Extended rules extended rules can examine a greater variety of packet fields to determine a match. Extended rules can examine both the packet's source and destination IP addresses, the protocol type, the source and destination ports, and other packet fields.

SDP Secure Device Provisioning. SDP uses Trusted Transitive Introduction (TTI) to easily deploy public key infrastructure (PKI) between two end devices, such as a Cisco IOS client and a Cisco IOS certificate server.

F

fasttrack A file-sharing network in which indexing functions are dynamically assigned to connected peers, called supernodes.

fidelity rating A number from 1 to 100 that indicates the confidence the rater has that a signature will generate an accurate alert.

finger A software tool for determining whether a person has an account at a particular Internet site. Many sites do not allow incoming finger requests.

fingerprint The fingerprint of a CA certificate is the string of alphanumeric characters that results from an MD5 hash of the whole CA certificate. Entities receiving a CA certificate can verify its authenticity by comparing it to its known fingerprint. This authentication is intended to ensure the integrity of communication sessions by preventing "man-in-the-middle" attacks.

firewall A router or access server, or several routers or access servers, designated as a buffer between any connected public networks and a private network. A firewall router uses access lists and other methods to ensure the security of the private network.

Flash

Flash memory A memory chip which retains data without power. Software images can be stored in, booted from, and written to Flash as necessary.

Frame Relay Industry standard, switched data link layer protocol that handles multiple virtual circuits using HDLC encapsulation between connected devices. Frame Relay is more efficient than X.25, the protocol for which it is generally considered a replacement.

FTP File Transfer Protocol. Part of the TCP/IP protocol stack, used for transferring files between hosts.

G

glob Pattern matching. A glob parameter map is a parameter map created to match specified patterns.

global IKE policy An IKE policy that is global to a device, rather than affecting only a single interface on that device.

gnutella A decentralized P2P file sharing protocol. Using an installed Gnutella client, users can search, download and upload files across the Internet.

GRE generic routing encapsulation. Tunneling protocol developed by Cisco that can encapsulate a wide variety of protocol packet types inside IP tunnels, creating a virtual point-to-point link to Cisco routers at remote points over an IP internetwork. By connecting multi-protocol subnetworks in a single-protocol backbone environment, IP tunneling using GRE allows network expansion across a single-protocol backbone environment.

GRE over IPSec This technology uses IPSec to encrypt GRE packets.

G.SHDSL Also known as G.991.2, G.SHDSL is an international standard for symmetric DSL developed by the International Telecommunications Union. G.SHDSL provides for sending and receiving high-speed symmetrical data streams over a single pair of copper wires at rates between 192 kbps and 2.31 Mbps.

H

H.323 An ITU-T standard that enables video conferencing over local-area networks (LANs) and other packet-switched networks, as well as video over the Internet.

hash One-way process that converts input of any size into checksum output of a fixed size, called a *message digest*, or just a *digest*. This process is not reversible, and it is not feasible to create or modify data to result in a specific digest.

hash algorithm A hash algorithm is used to generate a hash value, also known as a message digest, ensures that message contents are not changed during transmission. The two most widely used types of hash algorithms are Secure Hash Algorithm (SHA) and MD5)

HDLC High-Level Data Link Control. Bit-oriented synchronous data link layer protocol developed by the International Standards Organization (ISO). HDLC specifies a data encapsulation method on synchronous serial links using frame characters and checksums.

headend The upstream, transmit end of a tunnel.

HMAC Hash-based Message Authentication Code. HMAC is a mechanism for message authentication using cryptographic hash functions. HMAC can be used with any iterative cryptographic hash function, e.g., MD5, SHA-1, in combination with a secret shared key. The cryptographic strength of HMAC depends on the properties of the underlying hash function.

HMAC-MD5 Hashed Message Authentication Codes with MD5 (RFC 2104). A keyed version of MD5 that enables two parties to validate transmitted information using a shared secret.

host A computer, such as a PC, or other computing device, such as a server, associated with an individual IP address and optionally a name. The name for any device on a TCP/IP network that has an IP address. Also any network-addressable device on any network. The term *node* includes devices such as routers and printers which would not normally be called *hosts*.

HSPA High-Speed Packet Access.

HSPA-A High-Speed Packet Access for Americas.

HSPA-G High-Speed Packet Access for Global.

HTTP
HTTPS Hypertext Transfer Protocol, Hypertext Transfer Protocol, Secure. The protocol used by Web browsers and Web servers to transfer files, such as text and graphic files.

hub In a DMVPN network, a hub is a router with a point-to-point IPSec connection to all spoke routers in the network. The hub is the logical center of a DMVPN network.

HWIC High-Speed WAN Interface Card.

I

ICMP Internet Control Message Protocol. Network layer Internet protocol that reports errors and provides other information relevant to IP packet processing.

Identical Addressing The ability to reach devices having identical IP addresses over an EasyVPN connection through the use of Network Address Translation.

IDS Intrusion Detection System. The Cisco IPS performs a real time analysis of network traffic to find anomalies and misuse, using a library of signatures it can compare traffic against. When it finds unauthorized activity or anomalies, it can terminate the condition, block traffic from attacking hosts, and send alerts to the IDM.

IDS Sensor An IDS sensor is hardware on with the Cisco IDS runs. IDS sensors can be stand-alone devices, or network modules installed on routers.

IDM IDS Device Manager. IDM is software used to manage an IDS sensor.

IEEE Institute of Electrical and Electronics Engineers.

IETF Internet Engineering Task Force.

IGMP Internet Group Management Protocol. IGMP is a protocol used by IPv4 systems to report IP multicast memberships to neighboring multicast routers

IKE Internet Key Exchange. IKE is a key management protocol standard used in conjunction with IPSec and other standards. IPSec can be configured without IKE, but IKE enhances IPSec by providing additional features, flexibility, and ease of configuration for the IPSec standard. IKE provides authentication of the IPSec peers, negotiates IPSec keys, and negotiates IPSec security associations.

Before any IPSec traffic can be passed, each router/firewall/host must be able to verify the identity of its peer. This can be done by manually entering preshared keys into both hosts or by a CA service. IKE is a hybrid protocol that implements the Oakley key exchange and Skeme key exchange inside the Internet Security Association and Key Management Protocol (ISAKMP) framework. (ISAKMP, Oakley, and Skeme are security protocols implemented by IKE.)

IKE negotiation A method for the secure exchange of private keys across non-secured networks.

IKE profile A group of ISAKMP parameters that can be mapped to different IP Security tunnels.

IM Instant Messaging. A real-time communication service in which both parties are online at the same time. Popular IM services include Yahoo! Messenger (YM), Microsoft Networks Messenger, and AOL Instant Messenger (AIM).

IMAP Internet Message Access Protocol. A protocol used by clients to communicate with an e-mail server. Defined in RFC 2060, IMAP enables clients to delete, change the status, and otherwise manipulate messages on the e-mail server as well as retrieve them.

implicit rule An access rule automatically created by the router based on default rules or as a result of user-defined rules.

inside global The IP address of a host inside a network as it appears to devices outside the network.

inside local The configured IP address assigned to a host inside the network.

inspection rule A CBAC inspection rule allows the router to inspect specified outgoing traffic so that it can allow return traffic of the same type that is associated with a session started on the LAN. If a firewall is in place, incoming traffic that is associated with a session started inside the firewall might be dropped if an inspection rule has not been configured.

interface The physical connection between a particular network and the router. The router's LAN interface connects to the local network that the router serves. The router has one or more WAN interfaces that connect to the Internet.

Internet The global network which uses IP, Internet protocols. Not a LAN. See also intranet.

intranet Intranetwork. A LAN which uses IP, and Internet protocols, such as SNMP, FTP, and UDP. See also network, Internet.

IOS Cisco IOS software. Cisco system software that provides common functionality, scalability, and security for all products under CiscoFusion architecture. Cisco IOS allows centralized, integrated, and automated installation and management of internetworks, while ensuring support for a wide variety of protocols, media, services and platforms.

IOS IPS

IPS

Cisco IOS Intrusion Prevention System. IOS IPS compares traffic against an extensive database of intrusion signatures, and can drop intruding packets and take other actions based on configuration. Signatures are built in to IOS images supporting this feature, and additional signatures can be stored in local or remote signature files.

IP

Internet Protocol. The Internet protocols are the world's most popular open-system (nonproprietary) protocol suite because they can be used to communicate across any set of interconnected networks and are equally well suited for LAN and WAN communications.

IP address

IP version 4 addresses are 32 bits, or 4 bytes, in length. This address "space" is used to designate the network number, the optional subnetwork number, and a host number. The 32 bits are grouped into four octets (8 binary bits), represented by 4 decimal numbers separated by periods or "dots." The part of the address used to specify the network number, the subnetwork number, and the host number is specified by the subnet mask.

IPSec

A framework of open standards that provides data confidentiality, data integrity, and data authentication between participating peers. IPSec provides these security services at the IP layer. IPSec uses IKE to handle negotiation of protocols and algorithms based on local policy and to generate the encryption and authentication keys to be used by IPSec. IPSec can be used to protect one or more data flows between a pair of hosts, between a pair of security gateways, or between a security gateway and a host.

IPSec policy

In Cisco CP, an IPSec policy is a named set of crypto map associated with a VPN connection.

IPSec rule

A rule used to specify which traffic is protected by IPSec.

IRB

Integrated Routing and Bridging. IRB allows you to route a given protocol between routed interfaces and bridge groups within a single switch router.

ISAKMP

The Internet Security Association Key Management Protocol is the basis for IKE. ISAKMP authenticates communicating peers, creates and manages security associations, and defines key generation techniques.

K

kazaa2 A peer-to-peer file sharing service.

key A string of bits used to encrypt or decrypt data, or to compute message digests.

key agreement The process whereby two or more parties agree to use the same secret symmetric key.

key escrow A trusted third party who holds the cryptographic keys.

key exchange The method by which two or more parties exchange encryption keys. The IKE protocol provides one such method.

key lifetime An attribute of a key pair that specifies a time span, during which the certificate containing the public component of that key pair is considered valid.

key management The creation, distribution, authentication, and storage of encryption keys.

key pair See public key encryption.

key recovery A trusted method by which encrypted information can be decrypted if the decryption key is lost or destroyed.

L

L2F Protocol Layer 2 Forwarding Protocol. Protocol that supports the creation of secure virtual private dial-up networks over the Internet.

L2TP Layer 2 Tunneling Protocol. An Internet Engineering Task Force (IETF) standards track protocol defined in RFC 2661 that provides tunneling of PPP. Based upon the best features of L2F and PPTP, L2TP provides an industry-wide interoperable method of implementing VPDN. L2TP is proposed as an IPSec alternative, but is used sometimes alongside IPSec to provide authentication services.

LAC L2TP access concentrator. Device terminating calls to remote systems and tunneling PPP sessions between remote systems and the LNS.

LAN Local Area Network. A network residing in one location or belonging to one organization, typically, but not necessarily using IP and other Internet protocols. Not the global Internet. *See also* intranet, network, Internet.

LAPB Link Access Procedure, Balanced.

Layer 3 Interface Layer 3 interfaces support internetwork routing. A VLAN is an example of a logical layer 3 interface. An Ethernet port is an example of a physical layer 3 interface.

LBO Line Build Out.

LEFS low-end file system.

life cycle See expiration date.

LLQ Low Latency Queuing (LLQ) allows delay-sensitive data such as voice to be dequeued and sent first (before packets in other queues are dequeued), giving delay-sensitive data preferential treatment over other traffic.

LNS L2TP network server. Device able to terminate L2TP tunnels from a LAC and able to terminate PPP sessions to remote systems through L2TP data sessions.

local subnet Subnetworks are IP networks arbitrarily segmented by a network administrator (by means of a subnet mask) in order to provide a multilevel, hierarchical routing structure while shielding the subnetwork from the addressing complexity of attached networks. The local subnet is the subnet associated with your end of a transmission.

logical interface An interface that has been created solely by configuration, and that is not a physical interface on the router. Dialer interfaces and tunnel interfaces are examples of logical interfaces.

loopback In a loopback test, signals are sent and then redirected back toward their source from some point along the communications path. Loopback tests are often used to determine network interface usability.

M

MAC

message authentication code. The cryptographic checksum of the message used to verify message authenticity. See hash.

mask

subnet mask

netmask

network mask

A 32-bit mask which specifies how an Internet address is to be divided into network, subnet, and host parts. The net mask has ones (1's) in the bit positions in the 32-bit address that are to be used for the network and subnet parts, and has zeros (0's) for the host part. The mask should contain at least the standard network portion (as determined by the address class), and the subnet field should be contiguous with the network portion. The mask is configured using the decimal equivalent of the binary value.

Examples:

Decimal: 255.255.255.0
Binary: 11111111 11111111 11111111 00000000
The first 24 bits provide the network and subnetwork address, and the last 8 provide the host address.

Decimal: 255.255.255.248
Binary: 11111111 11111111 11111111 11111000
The first 29 bits provide the network and subnetwork address, and the last 3 provide the host address.

See also IP Address, TCP/IP, host, host/network.

MD5

Message Digest 5. A one-way hashing function that produces a 128-bit hash. Both MD5 and Secure Hashing Algorithm (SHA) are variations on MD4 and are designed to strengthen the security of the MD4 hashing algorithm. Cisco uses hashes for authentication within the IPSec framework. MD5 verifies the integrity and authenticates the origin of a communication.

message digest

A string of bits that represents a larger data block. This string defines a data block, based on the processing of its precise content through a 128-bit hash function. Message digests are used in the generation of digital signatures. See hash.

MD5 Message Digest 5. A one-way hashing algorithm that produces a 128-bit hash. Both MD5 and Secure Hash Algorithm (SHA) are variations on MD4 and are designed to strengthen the security of the MD4 hashing algorithm. Cisco uses hashes for authentication within the IPSec framework. Also used for message authentication in SNMP v.2. MD5 verifies the integrity of the communication, authenticates the origin, and checks for timeliness.

mGRE multipoint GRE.

MTU maximum transmission unit. The maximum packet size, in bytes that an interface can transmit or receive.

N

NAC Network Admission Control. A method of controlling access to a network in order to prevent the introduction of computer viruses. Using a variety of protocols and software products, NAC assesses the condition of hosts when they attempt to log onto the network, and handles the request based on the host's condition, called its *posture*. Infected hosts can be placed in quarantine; hosts without up-to-date virus protection software can be directed to obtain updates, and uninfected hosts with up-to-date virus protection can be allowed onto the network. See also ACL, posture, and EAPoUDP.

NAD Network Access Device. In a NAC implementation, the device that receives a host's request to log on to the network. A NAD, usually a router, works with posture agent software running on the host, virus protection software, and ACS and posture/remediation servers on the network to control access to the network in order to prevent infection by computer viruses.

NAS Network Access Server. Platform that interfaces between the Internet and the public switched telephone network (PSTN).

Gateway that connects asynchronous devices to a LAN or WAN through network and terminal emulation software. Performs both synchronous and asynchronous routing of supported protocols.

NAT

Network Address Translation

Network Address Translation. Mechanism for reducing the need for globally unique IP addresses. NAT allows an organization with addresses that are not globally unique to connect to the Internet by translating those addresses into globally routable address space.

NBAR

Network-based Application Recognition. A method used to classify traffic for QoS.

NBMA

nonbroadcast multiaccess. Term describing a multiaccess network that either does not support broadcasting (such as X.25) or in which broadcasting is not feasible (for example, an SMDS broadcast group or an extended Ethernet that is too large).

NetFlow

A feature of some routers that allows them to categorize incoming packets into flows. Because packets in a flow often can be treated in the same way, this classification can be used to bypass some of the work of the router and accelerate its switching operation.

network

A network is a group of computing devices which share part of an IP address space and not a single host. A network consists of multiple “nodes” or devices with IP address, any of which may be referred to as *hosts*. See also Internet, Intranet, IP, LAN.

network bits

In a subnet mask, the number of bits set to binary 1. A subnet mask of 255.255.255.0 has 24 network bits, because 24 bits in the mask are set to 1. A subnet mask of 255.255.248 has 17 network bits.

network module

A network interface card that is installed in the router chassis to add functionality to the router. Examples are Ethernet network modules, and IDS network modules.

NHRP

Next Hop Resolution Protocol. A client and server protocol used in DMVPN networks, in which the hub router is the server and the spokes are the clients. The hub maintains an NHRP database of the public interface addresses of the each spoke. Each spoke registers its real address when it boots and queries the NHRP database for real addresses of the destination spokes in order to build direct tunnels to them.

NID

Network Identification Number.

non-repudiation service A third-party security service that stores evidence for later, possible retrieval, regarding the origin and destination of all data included in a communication — without storing the actual data. This evidence can be used to safeguard all participants in that communication against false denials by any participant of having sent information, as well as false denials by any participant of having received information.

NTP Network Time Protocol. A protocol to synchronize the system clocks on network devices. NTP is a UDP protocol.

NVRAM Non-volatile random access memory.

O

Oakley A protocol for establishing secret keys for use by authenticated parties, based on Diffie-Hellman and designed to be a compatible component of ISAKMP.

OFB output feedback. An IPSec function that feeds encrypted output (generally, but not necessarily, DES-encrypted) back into the original input. Plaintext is encrypted directly with the symmetric key. This produces a pseudo-random number stream.

outside global The IP address assigned to a host on the outside network by the host's owner. The address was allocated from globally routable address or network space.

outside local The IP address of an outside host as it appears to the inside network. Not necessarily a legitimate address, it was allocated from an address space routable on the inside.

OSPF Open Shortest Path First. Link-state, hierarchical IGP routing algorithm proposed as a successor to RIP in the Internet community. OSPF features include least-cost routing, multipath routing, and load balancing.

P

P2P See peer-to-peer.

PAD packet assembler/disassembler. Device used to connect simple devices (like character-mode terminals) that do not support the full functionality of a particular protocol to a network. PADs buffer data and assemble and disassemble packets sent to such end devices.

padding In cryptosystems, *padding* refers to random characters, blanks, zeros, and nulls added to the beginning and ending of messages, to conceal their actual length or to satisfy the data block size requirements of some ciphers. Padding also obscures the location at which cryptographic coding actually starts.

PAM Port to Application Mapping. PAM allows you to customize TCP or UDP port numbers for network services or applications. PAM uses this information to support network environments that run services using ports that are different from the registered or well-known ports associated with an application.

PAP Password Authentication Protocol. An authentication protocol that allows peers to authenticate one another. PAP passes the password and hostname or username in unencrypted form. See also CHAP.

parameter map Parameter-maps specify inspection behavior for Zone-Policy Firewall, for parameters such as Denial-of-Service Protection, session and connection timers, and logging settings. Parameter-maps are also applied with Layer 7 class- and policy-maps to define application-specific behavior, such as HTTP objects, POP3 and IMAP authentication requirements, and other application-specific information.

password A protected and secret character string (or other data source) associated with the identity of a specific user or entity.

password aging

Password aging The ability of a system to notify a user that their password has expired, and to provide them with the means to create a new password.

PAT

Dynamic PAT Port Address Translation. Dynamic PAT lets multiple outbound sessions appear to originate from a single IP address. With PAT enabled, the router chooses a unique port number from the PAT IP address for each outbound translation slot (xlate). This feature is valuable when an Internet service provider cannot allocate enough unique IP addresses for your outbound connections. The global pool addresses always come first, before a PAT address is used.

PCEX PC Express.

PDP Packet Data Protocol (PDP).

peer In IKE, peers are routers acting as proxies for the participants in an IKE tunnel. In IPSec, peers are devices or entities that communicate securely either through the exchange of keys or the exchange of digital certificates.

peer-to-peer A type of network design where all hosts share roughly equivalent capabilities. Also called P2P, peer-to-peer networking is used by many file sharing networks.

PEM Privacy Enhanced Mail format. A format for storing digital certificates.

PFS perfect forward secrecy. A property of some asymmetric key agreement protocols that allows for the use of different keys at different times during a session, to ensure that the compromising of any single key will not compromise the session as a whole.

physical interface A router interface supported by a network module that is installed in the router chassis, or that is part of the router's basic hardware.

ping An ICMP request sent between hosts to determine whether a host is accessible on the network.

PKCS7 Public Key Cryptography Standard Number 7.

PKCS12 Public Key Cryptography Standard Number 12. A format for storing digital certificate information. See also PEM.

PKI public-key infrastructure. A system of certification authorities (CAs) and registration authorities (RAs) that provides support for the use of asymmetric key cryptography in data communication through such functions as certificate management, archive management, key management, and token management.

Alternatively, any standard for the exchange of asymmetric keys.

This type of exchange allows the recipient of a message to trust the signature in that message, and allows the sender of a message to encrypt it appropriately for the intended recipient. See key management.

plaintext Ordinary, unencrypted data.

police rate The rate of bits per second that traffic must not exceed.

policing Traffic policing propagates bursts. When the traffic rate reaches the configured maximum rate, excess traffic is dropped, or remarked.

policy map

policy maps A policy map consists of configured actions to be taken on traffic. Traffic is defined in a class map. More than one class map can be associated with a policy map.

POP3 Post Office Protocol version 3. A protocol used to retrieve e-mail from an e-mail server.

posture In a NAC implementation, the condition of a host attempting access to the network. Posture agent software running on the host communicates with the NAD to report on the host's compliance with the network security policy.

PPP Point-to-Point Protocol. A protocol that provides router-to-router, and host-to-network connections over synchronous and asynchronous circuits. PPP has built in security mechanisms, such as CHAP and PAP.

PPPoA Point-to-Point Protocol over Asynchronous Transfer Mode (ATM). Primarily implemented as part of ADSL, PPPoA relies on RFC1483, operating in either Logical Link Control-Subnetwork Access Protocol (LLC-SNAP) or VC-Mux mode.

PPPoE Point-to-Point Protocol over Ethernet. PPP encapsulated in Ethernet frames. PPPoE enables hosts on an Ethernet network to connect to remote hosts through a broadband modem.

PPTP Point-to-Point Tunneling Protocol. Creates client-initiated tunnels by encapsulating packets into IP datagrams for transmission over TCP/IP-based networks. Can be used as an alternative to the L2F and L2TP tunneling protocols. Proprietary Microsoft protocol.

pre-shared key

One of three authentication methods offered in IPSec, with the other two methods being RSA encrypted nonces, and RSA signatures. Pre-shared keys allow for one or more clients to use individual shared secrets to authenticate encrypted tunnels to a gateway using IKE. Pre-shared keys are commonly used in small networks of up to 10 clients. With pre-shared keys, there is no need to involve a CA for security.

The Diffie-Hellman key exchange combines public and private keys to create a shared secret to be used for authentication between IPSec peers. The shared secret can be shared between two or more peers. At each participating peer, you would specify a shared secret as part of an IKE policy. Distribution of this pre-shared key usually takes place through a secure out-of-band channel. When using a pre-shared key, if one of the participating peers is not configured with the same pre-shared key, the IKE SA cannot be established. An IKE SA is a prerequisite to an IPSec SA. You must configure the pre-shared key at all peers.

Digital certification and wildcard pre-shared keys (which allow for one or more clients to use a shared secret to authenticate encrypted tunnels to a gateway) are alternatives to pre-shared keys. Both digital certification and wildcard pre-shared keys are more scalable than pre-shared keys.

private key

See public key encryption.

pseudo random

An ordered sequence of bits that appears superficially similar to a truly random sequence of the same bits. A key generated from a pseudo random number is called a nonce.

public key encryption

In public key encryption systems, every user has both a public key and a private key. Each private key is maintained by a single user and shared with no one. The private key is used to generate a unique digital signature and to decrypt information encrypted with the public key. In contrast, a user's public key is available to everyone to encrypt information intended for that user, or to verify that user's digital signature. Sometimes called public key cryptography.

PVC

permanent virtual circuit (or connection). Virtual circuit that is permanently established. PVCs save bandwidth associated with circuit establishment and tear down in situations where certain virtual circuits must exist all the time. In ATM terminology, called a permanent virtual connection.

Q

QoS Quality of Service. A method of guaranteeing bandwidth to specified types of traffic.

queuing Traffic queuing aggregates packet streams to multiple queues and provides different service to each queue. See also LLQ and CBWFQ.

quick mode In Oakley, the name of the mechanism used after a security association has been established to negotiate changes in security services, such as new keys.

R

RA registration authority. An entity serving as an optional component in PKI systems to record or verify some of the information that certification authorities (CAs) use when issuing certificates or performing other certificate management functions. The CA itself might perform all RA functions, but they are generally kept separate. RA duties vary considerably, but may include assigning distinguished names, distributing tokens, and performing personal authentication functions.

RADIUS Remote Authentication Dial-In User Service. An access server authentication and accounting protocol that uses UDP as the transport protocol. See also TACACS+

RCP remote copy protocol. Protocol that allows users to copy files to and from a file system residing on a remote host or server on the network. The rcp protocol uses TCP to ensure the reliable delivery of data

remote subnet Subnetworks are IP networks arbitrarily segmented by a network administrator (by means of a subnet mask) in order to provide a multilevel, hierarchical routing structure while shielding the subnetwork from the addressing complexity of attached networks. A “remote subnet” is the subnet that is *not* associated with your end of a transmission.

replay-detection A standard IPSec security feature that combines sequence numbers with authentication, so the receiver of a communication can reject old or duplicate packets in order to prevent replay attacks.

repudiation In cryptographic systems, repudiation is the denial by one of the entities involved in a communication of having participated in all or part of that communication.

revocation password The password that you provide to a CA when you request that it revoke a router's digital certificate. Sometimes called a *challenge password*.

RFC 1483 routing RFC1483 describes two different methods for carrying connectionless network interconnect traffic over an ATM network: routed protocol data units (PDUs) and bridged PDUs. Cisco CP supports the configuration of RFC 1483 routing, and enables you to configure two encapsulation types: AAL5MUX, and AAL5SNAP.

AAL5MUX: AAL5 MUX encapsulation supports only a single protocol (IP or IPX) per PVC.

AAL5SNAP: AAL5 Logical Link Control/Subnetwork Access Protocol (LLC/SNAP) encapsulation supports Inverse ARP and incorporates the LLC/SNAP that precedes the protocol datagram. This allows the multiple protocols to transverse the same PVC.

RIP Routing Information Protocol. A routing protocol that uses the number of routers a packet must pass through to reach the destination, as the routing metric.

root CA Ultimate certification authority (CA), which signs the certificates of the subordinate CAs. The root CA has a self-signed certificate that contains its own public key.

route A path through an internetwork.

route map Route maps enable you to control information that is added to the routing table. Cisco CP automatically creates route maps to prevent NAT from translating specific source addresses when doing so would prevent packets from matching criteria in an IPSec rule.

RPC remote procedure call. RPCs are procedure calls that are built or specified by clients and executed on servers, with the results returned over the network to the clients. See also client/server computing.

RR Risk Rating. An RR is a value between 0 and 100 that represents a numerical quantification of the risk associated with a particular event on the network.

RSA Rivest, Shamir, and Adelman, the inventors of this cryptographic key exchange technique, which is based on factoring large numbers. RSA is also the name of the technique itself. RSA may be used for encryption and authentication, and is included in many security protocols.

RSA keys An RSA asymmetric key pair is a set of matching public and private keys.

RSA signatures One of three authentication methods offered in IPSec, with the other two methods being RSA encrypted nonces, and pre-shared keys. Also, one of the three Federal Information Processing Standards (FIPS)–approved algorithms for generating and verifying digital signatures. The other approved algorithms are DSA and Elliptic Curve DSA.

rule Information added to the configuration to define your security policy in the form of conditional statements that instruct the router how to react to a particular situation.

S

SA security association. A set of security parameters agreed upon by two peers to protect a specific session in a particular tunnel. Both IKE and IPSec use SAs, although SAs are independent of one another.

IPSec SAs are unidirectional and are unique in each security protocol. An IKE SA is used by IKE only, and unlike the IPSec SA, it is bidirectional. IKE negotiates and establishes SAs on behalf of IPSec. A user can also establish IPSec SAs manually.

A set of SAs is needed for a protected data pipe, one per direction per protocol. For example, if you have a pipe that supports Encapsulating Security Protocol (ESP) between peers, one ESP SA is required for each direction. SAs are uniquely identified by destination (IPSec endpoint) address, security protocol (AH or ESP), and security parameter index (SPI).

SAID security association ID. Numeric identifier for the SA of a given link.

salt A string of pseudorandom characters used to enhance cryptographic complexity.

SCCP Skinny Client Control Protocol. SCCP is a proprietary terminal control protocol owned by Cisco Systems. It is used as a messaging protocol between a skinny client and Cisco Call Manager.

SDEE Security Device Event Exchange. A message protocol that can be used to report on security events, such as alarms generated when a packet matches the characteristics of a signature.

SDF Signature Definition File. A file, usually in XML format, containing signature definitions that can be used to load signatures on a security device.

SEAF Signature Event Action Filter. A filter that allows you to subtract actions from an event whose parameters fall within those defined. For example, a SEAF can be created to subtract the action Reset TCP Connection from an event associated with a particular attacker address.

SEAO Signature Event Action Override. An SEAO allows you to assign a risk rating (RR) range to an IPS event action type, such as alarm. If an event occurs with an RR in the range you have assigned to the action type, then that action is added to the event. In this case, an alarm would be added to the event.

SEAP Signature Event Action Processor. SEAP allows filtering and overrides based on Event Risk Rating (ERR) feedback.

secret key See symmetric key.

security association lifetime The predetermined length of time in which an SA is in effect.

security zone A group of interfaces to which a policy can be applied. Security zones should consist of interfaces that share similar functions or features. For example, on a router, interfaces Ethernet 0/0 and Ethernet 0/1 may be connected to the local LAN. These two interfaces are similar because they represent the internal network, so they can be grouped into a zone for firewall configurations.

session key A key that is used only once.

SFR Signature Fidelity Rating. A weight associated with how well this signature might perform in the absence of specific knowledge of the target.

SHA Some encryption systems use the Secure Hashing Algorithm to generate digital signatures, as an alternative to MD5.

SHA-1 Secure Hashing Algorithm 1. Algorithm that takes a message of less than 264 bits in length and produces a 160-bit message digest. The large message digest provides security against brute-force collision and inversion attacks. SHA-1 [NIS94c] is a revision to SHA that was published in 1994.

shaping Traffic shaping retains excess packets in a queue and then reschedules the excess for later transmission over increments of time.

shared key The secret key that all users share in a symmetric key-based communication session.

shared secret A crytographic key.

signature A data element in IOS IPS that detects a specific pattern of misuse on the network.

signature engine A signature engine is a component of Cisco IOS IPS designed to support many signatures in a certain category. An engine is composed of a parser and an inspector. Each engine has a set of legal parameters which have allowable ranges or sets of values.

signing certificate Used to associate your digital signature with your messages or documents, and to ensure that your messages or files are conveyed without changes.

SIP Session Initiation Protocol. Enables call handling sessions, particularly two-party audio conferences, or "calls." SIP works with Session Description Protocol (SDP) for call signaling. SDP specifies the ports for the media stream. Using SIP, the router can support any SIP Voice over IP (VoIP) gateways and VoIP proxy servers.

site-to-site VPN Typically, a site-to-site VPN is one that connects two networks or subneworks and that meets several other specific criteria, including the use of static IP addresses on both sides of the tunnel, the absence of VPN client software on user end-stations, and the absence of a central VPN hub (as would exist in hub-and-spoke VPN configurations). Site-to-site VPNs are not intended to replace dial-in access by remote or traveling users.

SMTP Simple Mail Transfer Protocol. Internet protocol providing e-mail services.

SNMP Simple Network Management Protocol. Network management protocol used almost exclusively in TCP/IP networks. SNMP provides a means to monitor and control network devices, and to manage configurations, statistics collection, performance, and security.

SPD Selective Packed Discard. SPD provides priority to routing protocol packets and other important traffic control Layer 2 keepalives during periods of queue congestion.

Split DNS Split DNS enables Cisco routers to answer DNS queries using the internal hostname cache specified by a selected virtual DNS name server. Queries that cannot be answered by the information in the hostname cache, are redirected to specified back-end DNS name servers.

spoke In a DMVPN network, a spoke router is a logical end point in the network, and has a point-to-point IPSec connection with a DMVPN hub router.

spoofing

spoof The act of a packet illegally claiming to be from an address from which it was not actually sent. Spoofing is designed to foil network security mechanisms such as filters and access lists.

SRB source-route bridging. Method of bridging originated by IBM and popular in Token Ring networks. In an SRB network, the entire route to a destination is predetermined, in real time, prior to the sending of data to the destination.

SSH Secure Shell. An application running on top of a reliable transport layer, such as TCP/IP, that provides strong authentication and encryption capabilities. Up to five SSH clients are allowed simultaneous access to the router console.

SSID Service Set Identifier (also referred to as Radio Network Name). A unique identifier used to identify a radio network and which stations must use to be able to communicate with each other or to an access point. The SSID can be any alphanumeric entry up to a maximum of 32 characters.

SSL Secure Socket Layer. Encryption technology for the Web used to provide secure transactions, such as the transmission of credit card numbers for e-commerce.

SSL VPN Secure Socket Layer Virtual Private Networks. SSL VPN is a feature that enables a supported Cisco router to provide remote clients secure access to network resources by creating an encryption tunnel across the Internet using the broadband or ISP dial connection that the remote client uses.

SSL VPN context An SSL VPN context provides the resources needed to configure secure access to a corporate intranet and other types of private networks. An SSL VPN context must include an associated WebVPN gateway. An SSL VPN context can serve one or more SSL VPN group policies.

SSL VPN gateway An SSL VPN gateway provides an IP address and a certificate for an SSL VPN context.

SSL VPN group policy SSL VPN group policies define the portal page and links for the users included in those policies. An SSL VPN group policy is configured under an SSL VPN context.

standard rule In Cisco CP, a type of access rule or NAT rule. Standard rules compare a packet's source IP address against its IP address criteria to determine a match.Standard rules use a wildcard mask to determine which portions of the IP address must match.

state, stateful, stateful Inspection Network protocols maintain certain data, called state information, at each end of a network connection between two hosts. State information is necessary to implement the features of a protocol, such as guaranteed packet delivery, data sequencing, flow control, and transaction or session IDs. Some of the protocol state information is sent in each packet while each protocol is being used. For example, a web browser connected to a web server uses HTTP and supporting TCP/IP protocols. Each protocol layer maintains state information in the packets it sends and receives. Routers inspect the state information in each packet to verify that it is current and valid for every protocol it contains. This is called stateful inspection and is designed to create a powerful barrier to certain types of computer security threats

Static PAT Static Port Address Translation. A static address maps a local IP address to a global IP address. Static PAT is a static address that also maps a local port to a global port. See also PAT.

static route Route that is explicitly configured and entered into the routing table. Static routes take precedence over routes chosen by dynamic routing protocols.

subnet, subnetwork In IP networks, a network sharing a particular subnet address. Subnetworks are networks arbitrarily segmented by the network administrator in order to provide a multilevel, hierarchical routing structure while shielding the subnetwork from the addressing complexity of attached networks. See also IP address, subnet bits, subnet mask.

subnet bits

subnet mask 32-bit address mask used in IP to indicate the bits of an IP address that are being used for the network and optional subnet address. Subnet masks are expressed in decimal. The mask 255.255.255.0 specifies that the first 24 bits of the address Sometimes referred to simply as mask. See also address mask and IP address.

SUNRPC SUN Remote Procedure Call. RPC is a protocol that allows clients to run programs or routines on remote servers. SUNRPC is the version of RPC originally distributed in the SUN Open Network Computing (ONC) library.

symmetric key A symmetric key is used to decrypt information that it previously encrypted.

SID System Identification Number.

T

T1 A T1 link is a data link capable of transmitting data at a rate of 1.5 MB per second.

TACACS+ Terminal Access Controller Access Control System plus. An access server authentication and accounting protocol that uses TCP as the transport protocol.

tail-end The downstream, receive end of a tunnel.

TCP Transmission Control Protocol. Connection-oriented transport layer protocol that provides reliable full-duplex data transmission.

TCP Syn Flood Attack A SYN-flooding attack occurs when a hacker floods a server with a barrage of requests for connection. Because these messages have unreachable return addresses, the connections cannot be established. The resulting volume of unresolved open connections eventually overwhelms the server and can cause it to deny service to valid requests, thereby preventing legitimate users from connecting to a website, accessing e-mail, using FTP service, and so on.

Telnet A terminal emulation protocol for TCP/IP networks such as the Internet. Telnet is a common way to control web servers remotely.

TFTP Trivial File Transfer Protocol. TFTP is a simple protocol used to transfer files. It runs on UDP and is explained in depth in Request For Comments (RFC) 1350.

traffic flow confidentiality or traffic analysis Security concept that prevents the unauthorized disclosure of communication parameters. The successful implementation of this concept hides source and destination IP addresses, message length, and frequency of communication from unauthorized parties

transform Description of a security protocol and its corresponding algorithms.

transform set A transform set is an acceptable combination of security protocols, algorithms and other settings to apply to IPSec protected traffic. During the IPSec security association negotiation, the peers agree to use a particular transform set when protecting a particular data flow.

tunnel A virtual channel through a shared medium such as the Internet, used for the exchange of encapsulated data packets.

tunneling The process of piping the stream of one protocol through another protocol.

TVR Target Value Rating. The TVR is a user-defined value that represents the user's perceived value of the target host. This allows the user to increase the risk of an event associated with a critical system and to de-emphasize the risk of an event on a low-value target.

U

UDP User Datagram Protocol. Connectionless transport layer protocol in the TCP/IP protocol that belongs to the Internet protocol family.

unencrypted Not encrypted.

Unity Client A client of a Unity Easy VPN Server.

URI Uniform Resource Identifier. Type of formatted identifier that encapsulates the name of an Internet object, and labels it with an identification of the name space, thus producing a member of the universal set of names in registered name spaces and of addresses referring to registered protocols or name spaces. [RFC 1630]

URL Universal Resource Locator. A standardized addressing scheme for accessing hypertext documents and other services using a browser. Two examples follow:

http://www.cisco.com.

ftp://10.10.5.1/netupdates/sig.xml

V

verification Identity confirmation of a person or process.

VCI virtual channel identifier. A virtual path may carry multiple virtual channels corresponding to individual connections. The VCI identifies the channel being used. The combination of VPI and VCI identifies an ATM connection.

VFR Virtual Fragment Reassembly. VFR enables IOS Firewall to dynamically create ACLs to block IP fragments. IP fragments often do not contain enough information for static ACLs to be able to filter them.

VoIP Voice over IP. The capability to carry normal telephony-style voice over an IP-based internet with POTS-like functionality, reliability, and voice quality. VoIP enables a router to carry voice traffic (for example, telephone calls and faxes) over an IP network.

VPI virtual path identifier. Identifies the virtual path used by an ATM connection.

VPDN virtual private dial-up network. A system that permits dial-in networks to exist remotely to home networks, while giving the appearance of being directly connected. VPDNs use L2TP and L2F to terminate the Layer 2 and higher parts of the network connection at the home gateway, instead of the network access server (NAS).

VPN Virtual Private Network. Provides the same network connectivity for users over a public infrastructure as they would have over a private network. VPNs enable IP traffic to travel securely over a public TCP/IP network by encrypting all traffic from one network to another. A VPN uses tunneling to encrypt all information at the IP level.

VPN connection A site-to-site VPN. A site-to-site VPN consists of a set of VPN connections between peers, in which the defining attributes of each connection include the following device configuration information:

- A connection name
- Optionally, an IKE policy and pre-shared key
- An IPSec peer
- A list of one or more remote subnets or hosts that will be protected by the connection
- An IPSec rule that defines which traffic is to be encrypted.
- A list of transform sets that define how protected traffic is encrypted
- A list of the device network interfaces to which the connection is applied

VPN mirror policy A VPN policy on a remote system that contains values that are compatible with a local policy and that enable the remote system to establish a VPN connection to the local system. Some values in a mirror policy must match values in a local policy, and some values, such as the IP address of the peer, must be the reverse of the corresponding values in the local policy.

You can create mirror policies for remote administrators to use when you configure site-to-site VPN connections. For information on generating a mirror policy, refer to Generate Mirror....

VTI Virtual Template Interface.

vty virtual type terminal. Commonly used as virtual terminal lines.

W

WAN Wide Area Network. A network that serves users across a broad geographical area, and often uses transmission devices provided by common carriers. See also LAN.

WAAS Wide Area Application Services. A Cisco solution that optimizes the performance of TCP-based applications across a wide area network.

WAAS-NM WAAS Network Module. It goes into the Cisco ISR.

WAAS-SM WAAS Service Module. It goes into the Cisco ISR.

WCCP Web Cache Communication Protocol. Also known as Web Cache Control Protocol and Web Cache Coordination Protocol. WCCP allows the use of a Content Engine to reduce Web traffic to reduce transmission costs and download time from Web servers.

WAE Wide Area Application Engine. The term refers to Cis co network appliances that enable WAN optimization and application acceleration.

WAE-C WAE-Core. The core WAE component is installed on a server at the data center. It connects directly to one or more file servers or network-attached storage (NAS) devices.

WAE-E WAE-Edge. The edge WAE is installed on clients. It is a file caching device that serves client requests at remote sites and branch offices.

WFQ Weighted Fair Queuing. A flow-based queuing algorithm that does two things simultaneously: It schedules interactive traffic to the front of the queue to reduce response time, and it fairly shares the remaining bandwidth between high bandwidth flows.

wildcard mask A bit mask used in access rules, IPSec rules, and NAT rules to specify which portions of the packet's IP address must match the IP address in the rule. A wildcard mask contains 32 bits, the same number of bits in an IP address. A wildcard bit value of 0 specifies that the bit in that same position of the packet's IP address must match the bit in the IP address in the rule. A value of 1 specifies that the corresponding bit in the packet's IP address can be either 1 or 0, that is, that the rule "doesn't care" what the value of the bit is. A wildcard mask of 0.0.0.0 specifies that all 32 bits in the packet's IP address must match the IP address in the rule. A wildcard mask of 0.0.255.0 specifies that the first 16 bits, and the last 8 bits must match, but that the third octet can be any value. If the IP address in a rule is 10.28.15.0, and the mask is 0.0.255.0, the IP address 10.28.88.0 would match the IP address in the rule, and the IP address 10.28.15.55 would not match.

WINS Windows Internet Naming Service. A Windows system that determines the IP address associated with a particular network computer.

WMM Wi-Fi Multimedia. An IEEE 802.11e Quality of Service (QoS) draft standard. WMM compliant equipment is designed to improve the user experience for audio, video, and voice applications over a Wi-Fi wireless connection.

WRED Weighted Random Early Detection. A queueing method that ensures that high-precedence traffic has lower loss rates than other traffic during times of congestion.

X

X.509 A digital certificate standard, specifying certificate structure. Main fields are ID, subject field, validity dates, public key, and CA signature.

X.509 certificate A digital certificate that is structured according to the X.509 guidelines.

X.509 certificate revocation list (CRL) A list of certificate numbers that have been revoked. An X.509 CRL is one that meets either of the two CRL formatting definitions in X.509.

XAuth IKE Extended Authentication. Xauth allows all Cisco IOS software AAA authentication methods to perform user authentication in a separate phase after the IKE authentication phase 1 exchange. The AAA configuration list-name must match the Xauth configuration list-name for user authentication to occur.

Xauth is an extension to IKE, and does not replace IKE authentication.

Z

zone In a Zone-Based Policy Firewall, a zone is a group of interfaces that have similar functions or features. For example, if the interfaces FastEthernet 0/0 and FastEthernet 0/1 are both connected to the LAN, they could be grouped together in a single zone for the LAN.

zone pair A zone-pair allows you to specify a unidirectional traffic flow between two security zones. See also security zone

ZPF Zone-Based Policy Firewall. In a ZPF configuration interfaces are assigned to zones, and an inspection policy is applied to traffic moving between the zones.

INDEX

Symbols

$ETH-LAN$ 4-1

$ETH-WAN$ 5-4

.CSV file

- Call Forward Busy 55-5
- Call Forward No Answer 55-5
- Call Forward No Answer timeout 55-5
- correcting data conflicts in 55-9
- description 55-1
- downloading template 55-6
- extension label 55-5
- first name 55-3
- last name 55-3
- line mode 55-5
- MAC address 55-3
- mailbox 55-5
- mandatory fields 55-7
- phone type 55-4
- primary extension number 55-4
- secondary extension number 55-4
- user ID 55-3
- using the template to create 55-6
- version field 55-3

Numerics

3DES 25-9

911 emergency access (SRST) 50-1

A

About information 1-3

access list rule set 63-16

access rule

- in NAT translation rule 18-24, 18-27
- making changes in firewall policy 23-7

Access Rules window 15-3

acl

- creating with object groups 16-10

acl object groups

- basic workflow 16-2
- reference 16-11
- understanding 16-1

acl object groups reference

- Add an Extended Rule Entry dialog box 16-34, 16-37
- Select Network Object Groups dialog box 16-37

Select Service Object Groups dialog box 16-38

address pools 18-8, 18-15

ADSL

operating mode 5-20, 6-28

ADSL operating mode

adls2 6-29

adsl2+ 6-29

ansi-dmt 6-28

itu-dmt 6-28

splitterless 6-29

ADSL over ISDN

default operating mode 5-20

operating modes 6-31

AES encryption 25-9

After-Hours Tollbar

call blocking restrictions 59-3

calling restrictions 59-4

fast busy 59-2

holiday 59-5

override softkey login 59-6

reset to system defaults 59-7

unauthorized use of phones 59-2

weekly schedule 59-4

AH authentication 25-12

analog trunk 12-3

ansi-dmt 6-28

Application Traffic

viewing activity 70-17

ATM

subinterface 3-2

audience 1-65

audio paging 59-49

authentication

AH 25-12

digital signatures 97-21

ESP 25-11

MD5 25-9

password 2-17, 2-23

SHA_1 25-9

autoanswer (intercom) 59-31

auto attendant 61-1

auto-complete (Cisco Unity Express Call-In Number) 61-13

autodial 59-31

AutoSecure 46-25

B

back up IP phone calls 50-1

banner, configuring 46-14, 46-30

blocked call

override (softkey login) 59-6

prefixes 59-4

BOOTP, disabling 46-8

bulk data

using Cisco CP to import 55-8

bulk import

.CSV file 55-1

Apply Data screen 55-14

Finish screen 55-15
main screen 55-10
Select .CSV file screen 55-11
summary screen 55-12

C

call blocking
override 59-2, 59-6
PIN 59-2
call control 47-2
caller-ID
intercom 59-39, 59-41
paging name 59-51
calling restrictions (After-Hours Tollbar) 59-4
call-in number (Cisco Unity Express) 61-11
call park
Advanced tab 59-9, 59-12
directed 59-10
general purpose 59-10
General tab 59-9, 59-11
name 59-11
reminder 59-12
reminder ring 59-11
slot number 59-11
slots 59-11
termination 59-13
call pickup (night service bell) 59-44
call pickup groups
description 59-13
number 59-15
call-waiting 59-44
call waiting on overlay line
creating 56-31
CBAC, enabling 46-22
CBAC inspection rules 23-1, 23-12
CDP, disabling 46-9
CEF, enabling 46-12
cellular WAN 9-1
Challenge Handshake Authentication Protocol, see CHAP
CHAP 5-11
Cisco Communications Manager (CCM)
gateway mode 51-1
Cisco IOS Intrusion Prevention System (IPS), see IPS
Cisco IP Auto Attendant 59-25
Cisco Unified Communications Manager Express (Cisco Unified CME) 47-2
Cisco Unity Express
Call-In Number 61-13
IP configuration 61-14
launch 61-14
mailbox 56-50
service engine 61-15
Class of Restrictions (COR) 57-4
Client Mode 26-10
clock settings 5-13, 6-39, 6-43
CME as SRST 48-1

comma-separated-value file 55-1
community
adding 2-4
adding devices 2-3, 2-8
basic workflow 2-1
changing name 2-5
choose 1-3
create 1-3
creating 2-2, 2-3
deleting 2-5
deleting device 2-11
editing 2-8
exporting 2-6
importing 2-6
importing and exporting 2-6
information display 2-19
managing devices in 2-8
understanding 2-2
working with 2-2
working with devices in 2-8
community reference
Add or Edit Devices page 2-22
Change Default Credential dialog box 2-18
Discovery Details page 2-24
Router Status page 2-26
Select/Manage Community Dialog Box 2-15
COMP-LZS 25-12
content pane 1-2
conventions, typographical 1-66
crypto map 25-27
dynamic 36-2
IPSec rule 36-10
peers in 36-6, 36-7
protected traffic 36-9
security association lifetime 36-5
sequence number 36-5
transform set 36-7

D

date format 53-3, 53-5
default rules, Cisco CP 63-19
default static route 13-4
definitions of key terms and acronyms 1-1
deliver configuration to router 1-19
DES 25-9
device
connection type 2-21
discovering 2-12
discovery details 2-22
discovery status 2-21
hardware, software and feature details 2-22
hostname 2-20
IP address 2-16, 2-20, 2-23
login 2-17, 2-23
password 2-17, 2-23
DHCP 5-16, 6-24
D-H Group 25-10

dialer interface, added with PPPoE 5-5
Diffie-Hellman group 25-10
digital trunk 12-9
Direct Inward Dialing (DID) 12-2
directory numbers (night service bell) 59-44
directory services 59-16
discover
  devices 2-12
  process details 2-14
discovery
  Cisco CP overwriting existing credentials 2-36
  configuration requirements 2-28
  details 2-14, 2-22
  Secure Shell version problem 2-30
  status 2-21
display
  filtering 2-20
distance metric 13-4
DLCI 5-12, 6-38
DMVPN 29-1
  Fully Meshed Network 29-23
  hub 29-6
  Hub and Spoke Network 29-23
  pre-shared key 29-13
  primary hub 29-9
  routing information 29-16
  spoke 29-6
DMZ network 22-7
  permitting specific traffic through 22-19
  services 22-7
DMZ service 22-8
  address range 22-8
documentation
  audience 1-65
  conventions 1-66
do-not-disturb (DND) 53-3, 53-6
DSS digital signature 97-21
dynamic IP address 5-16, 6-24
Dynamic Multipoint VPN 29-1
dynamic routing protocol
  configuring 3-8

E

Easy VPN 26-4
  auto tunnel control 26-9, 26-39
  Client Mode 26-10
  configuring a backup 26-45
  Digital certificates 26-12, 26-34
  editing existing connection 26-44
  group key 26-27
  group name 26-27, 26-34
  interfaces 26-7
  IPSec group key 26-12
  IPSec group name 26-12
  manual tunnel control 26-9, 26-40
  Network Extension Mode 26-10
  Network Extension Plus 26-11, 26-29, 26-30

number of interfaces supported 26-8, 26-39
Preshared key 26-12, 26-34
SSH logon ID 26-15
traffic-based tunnel control 26-9, 26-40
Unity Client 26-26, 26-28, 26-31
Xauth logon 26-15
EIGRP route 13-7
emergency access (SRST) 50-1
enable secret 46-15, 46-30
encapsulation
Frame Relay 5-19
HDLC 5-19
IETF 5-12, 6-39
PPP 5-19
PPPoE 5-18, 6-30, 6-33, 7-5, 7-9
RFC 1483 Routing 5-18, 6-30, 6-33, 7-5, 7-9
encryption
3DES 25-9
AES 25-9
DES 25-9
energywise 11-1
ESP authentication and encryption 25-11
extended rules 15-5
numbering ranges 15-7
extensions
cloning 56-4
configure 56-3
creating 56-4
deleting 56-4
editing 56-4
understanding 56-2
extensions reference
Create Extension dialog box
General tab 56-12
Edit Extension dialog box
General tab 56-12
Extensions summary page 56-7
Externally Defined Rules window 15-4

F

fast busy (After-Hours Tollbar) 59-2
feature bar 1-2
finger service, disabling 46-6
firewall 22-1
ACL 23-1
add application entry 23-14
add fragment entry 23-15
add http application entry 23-16
add RPC entry 23-14
configuring NAT passthrough 22-21
configuring on an unsupported interface 22-18
enabling CBAC 46-22
permitting specific traffic 22-19, 22-20
permitting traffic from specific hosts or networks 22-20
permitting traffic to a VPN concentrator 22-21

policy 23-1
SDM warning 23-20
traffic flow, see traffic flow
traffic-flow display controls 23-3
viewing activity 22-16, 70-22
Firewall Rules window 15-3
Flash 63-1
Frame Relay 5-19
clock settings 6-39
DLCI 6-38
IETF encapsulation 6-39
LMI type 6-38
Fully Meshed Network 29-23
FXO 12-2, 53-3, 53-5
FXS 12-1

G

G.SHDSL
equipment type 6-35
equipment type, default value 5-20
line rate, default 5-20
operating mode 6-35
operating mode, default value 5-20
gateway
Cisco Communications Manager (CCM) 51-1
type 51-2
glossary definitions 1-1
gratuitous ARP requests, disabling 46-12
greeting 56-54
GRE over IPSec tunnel 25-16
GRE tunnel 25-16
pre-shared key 25-17
split tunnelling 25-21

H

H.323 47-3, 51-1
HDLC 5-19
help system
display 1-3
hook flash 53-3, 53-5
hosting CME 47-2
HTTP service
configuring an access class 46-23
Hub-and-Spoke network 29-23
hunt groups 59-18
Advanced tab 59-29
creating 59-19
deleting 59-20
editing 59-20
extension timeout 59-28
General tab 59-24
limit ephone-hunt group calls 59-31
logout 53-3, 53-6
number of hops 59-30
on-hook time stamp 59-31
pilot number 59-23

preference order for the backup number 59-30

primary and secondary pilot numbers 59-30

reference 59-22

unsanswered call message 59-30

working with 59-19

hunt groups reference

Edit or Create Hunt Group Page

Advanced Tab 59-29

General Tab 59-24

Edit or Create Hunt Group page 59-24

Hunt Groups Summary page 59-22

Set Extension Timeout dialog box 59-28

hunt group type

longest idle 59-18

parallel 59-18

peer 59-18

sequential 59-18

I

ICMP host unreachable messages, disabling 46-20, 46-21

ICMP mask reply messages, disabling 46-20

ICMP redirect messages, disabling 46-18

IETF encapsulation 5-12, 6-39

IKE 97-21

authentication 97-21

authentication algorithms 25-9

description 37-1

D-H Group 25-10

policies 25-8, 37-1

policy 25-5

pre-shared keys 37-5

shared key 97-21

state 70-30

viewing activity 70-25

inspection rule

SDM warning 23-19

Integrated Services Router (ISR) 47-2

intercom 59-31

mute 59-40, 59-42

interfaces

available configurations for each type 97-4

editing associations 6-10

statistics 70-6

unsupported 3-2

viewing activity 70-6

Internet Key Exchange 97-21

Intrusion Prevention System (IPS)

IP address

dynamic 5-16, 6-24

for ATM or Ethernet with PPPoE 5-16

for ATM with RFC 1483 routing 5-17

for Ethernet without PPPoE 5-4

for Serial with HDLC or Frame Relay 5-10

for Serial with PPP 5-9

negotiated 5-17, 6-25

next hop 5-6

unnumbered 5-16, 6-25
IP compression 25-12
IP directed broadcasts, disabling 46-19
IP Identification service, disabling 46-9
IP phones, configure 56-36
IPS
about 41-1
built-in signatures 41-19
buttons for configuration and management 41-10
Create IPS 41-2
disabling (on all interfaces) 41-12
disabling (on specified interface) 41-12
filter (ACL)
choose 41-14
details 41-13
inbound 41-14
outbound 41-14
global settings 41-15
interface selection 41-14
reload (recompile) signatures 41-18
rules 41-2
Rule wizard 41-2
SDF 41-66
in router memory 41-64
IPS supplied 41-63
loading 41-57
SDF locations 41-17, 41-19
Security Dashboard 41-64
deploying signatures 41-66
top threats 41-65
signatures
about 41-44, 41-50
actions on match 41-58
adding 41-46
defining 41-61
disabling 41-47, 41-52
enabling 41-46
importing 41-59
information on new 41-63
signature tree 41-44, 41-50, 41-60
TrendMicro OPACL 41-46
viewing 41-47, 41-52
syslog server 41-18, 41-26
traffic directions 41-13
VFR 41-13, 41-15
IPSec 25-14
description 36-1
group key 26-12, 26-27
group name 26-27, 26-34
policy type 36-2
rule 36-10
statistics 70-26
tunnel status 70-26
viewing activity 70-25
IPSec Rules window 15-3
IP source routing, disabling 46-10
ISDN BRI 12-9
ISDN PRI

configure trunk 12-9
Voice mode support 12-9

J

Jafa applets, blocking 23-17

L

license
telephony 53-1
license management
understanding 78-1
line types
call waiting on overlay 56-31, 56-34
configuring 56-26
monitor 56-30
overlay 56-31, 56-34
regular 56-26
shared 56-27
LMI 5-12, 6-38
load balancing 41-19, 41-27
logging
configuring 46-30
enabling 46-14
enabling sequence numbers and time stamps 46-11
viewing events 70-10

M

mailbox 56-50
defaults 61-9
tab 56-50
user settings 56-50
MD5 25-9
media access control (MAC) address (IP phone) 56-36
Media Gateway Control Protocol (MGCP) 12-9, 51-1
media translation 47-2
menu bar 1-2
mGRE 29-9
mirror configuration, VPN 25-33
mobility
enable 56-17
mode
demo 1-15
offline 1-15
module
configuration 10-1
module configuration 10-1
monitor line
creating 56-30
Monitor mode 70-1
Firewall Status 70-22
Interface Status 70-6
Logging 70-10
Overview 70-2

Traffic Status 70-17

VPN Status 70-25

MOP service, disabling 46-20

Multipoint Generic Routing Encapsulation 29-9

N

NAC Rules window 15-3

name, call park 59-11

NAT 18-1

address pools 18-8, 18-15

affect on DMZ service configuration 22-8

and VPN connections 25-29

configuring on unsupported interface 3-8, 22-20

configuring with a VPN 25-37

designated interfaces 18-8

DNS timeout 18-12

dynamic address translation rule, inside to outside 18-23

dynamic NAT timeout 18-13

ICMP timeout 18-12

max number of entries 18-13

permitting through a firewall 22-21

PPTP timeout 18-13

redirect port 18-20, 18-23

route map 18-26

route maps 18-13

static address translation rule 18-17

static address translation rule, outside to inside 18-20

TCP flow timeouts 18-13

translate from interface,dynamic rule 18-24, 18-27

translate from interface,static rule 18-18, 18-21

translate to interface,dynamic rule 18-25, 18-27

translate to interface,static rule 18-19, 18-22

translation direction,static rule 18-17

translation rules 18-9

translation timeouts 18-9, 18-12

UDP flow timeouts 18-13

Wizard 18-1

NAT Rules window 15-3

NBAR

viewing activity 70-17

Netflow

viewing activity 70-17

NetFlow, enabling 46-17

network object groups

creating 16-3

deleting 16-5

editing 16-4

understanding 16-3

working with 16-3

network object groups reference

Create Network Object Groups dialog box 16-13

Edit Network Object Groups dialog box 16-15

Network Object Groups summary page 16-12

next hop IP address 5-6

NHRP

authentication string 29-11

hold time 29-12

network ID 29-11

night service, enable 56-55

night service bell

annual schedule 59-46

call pickup 59-44

code 59-48

daily schedule 59-47

directory numbers 59-44

silent ring 59-44

weekly schedule 59-46

O

offline or demo mode 1-15

One-Step Lockdown 46-2

one-way voice path 59-49

OSPF route 13-5

overlay line

creating 56-31

overlay line to monitor line

changing 56-33

overlay line to regular line

changing 56-33

override call blocking 59-2

P

PAD service, disabling 46-7

paging

multicast IP address 59-52, 59-53, 59-58

name 59-51

numbers 59-49

PAP 5-11

passive interface 13-5, 13-6, 13-7

Password Authentication Protocol, see PAP

passwords

enabling encryption 46-10

setting minimum length 46-12

PAT

configuring in WAN wizard 5-6

use in NAT address pools 18-16

Perfect Forwarding Secrecy 36-6

permanent route 13-5

personal identification number (After-Hours Tollbar) 59-2

phone

associating with softkey template 59-71

operating system 60-1

softkey template 59-66

phone firmware

display the registered phones 60-6

download link 60-2

reset phone 60-5
phone load 60-1
phone registration source IP address 53-5
phones 56-22
configure 56-21
creating 56-22
deleting 56-22
editing 56-22
ring behavior 56-47
pilot number 59-25
ping
sending to VPN peer 95-1
place a call on hold 59-10
plain old telephone service (POTS) 47-3
Point-to-Point-Protocol over Ethernet, see PPPoE
PPP 5-19
PPPoE 5-18, 6-30, 6-33, 7-5, 7-9
in Ethernet WAN wizard 5-5
pre-shared key 25-7, 25-17, 29-13
pre-shared keys 37-5
primary hub 29-9
procedure
displaying device information 2-14
Protocol Traffic
viewing activity 70-17
proxy ARP, disabling 46-18
public switched telephone network (PSTN) 47-2
PVC 5-19

Q

QoS
viewing activity 70-17
QoS Rules window 15-4

R

redirect port 18-20, 18-23
reference
device community 2-15
regular line
creating 56-26
reminder, call park 59-12
reminder ring
call park 59-11
remote worker 56-55
Report Card screen 46-5
resetting
phones 56-22
restarting
phones 56-22
RFC 1483 Routing 5-18
AAL5 MUX 6-27, 6-30, 6-33, 7-5, 7-9
AAL5 SNAP 6-27, 6-30, 6-33, 7-5, 7-9
RIP route 13-5
route map 18-26
route maps 18-13, 25-29
routing

distance metric 13-4
EIGRP route 13-7
OSPF route 13-5
passive interface 13-5, 13-6, 13-7
peformance 21-1
permanent route 13-5
RIP route 13-5
routing protocol, dynamic 3-8
RSA
digital signature 97-21
encryption 97-21
rule 25-14
rule entry
guidelines 15-8
rules
extended rules 15-5
NAT, and VPN connections 25-29
standard rules 15-5
rule set 63-16
running configuration
display 63-16
save to file 63-1

S

scheduler allocate 46-16
scheduler interval 46-16
screencast
cellular WAN 9-1
CME as SRST 48-1
CUE restriction table 52-2
dialing restrictions 57-7
energywise 11-1
extension template 59-72
license management 69-1
offline or demo mode 1-15
outgoing dial plan 57-5
user profile 1-11
voice security audit 52-1
wireless support 8-1
screens
Select / Create 2-15
SDEE
messages 41-20
IDS error 41-24
IDS status 41-23
subscriptions 41-18, 41-26
SDF 41-66
in router memory 41-64
IPS supplied 41-63
loading 41-57
locations 41-17, 41-19
SDP
launching 20-1
troubleshooting 20-2
Secure Device Provisioning, see SDP 20-1
security association lifetime 36-5
security audit

voice 52-1
Security Audit wizard
Configure User Accounts for Telnet 46-29
Enable Secret and Banner 46-30
Interface Selection 46-4
Logging 46-30
Report Card 46-5
starting 46-1
Security Dashboard 41-64
deploying signatures 41-66
top threats 41-65
sequence numbers, enabling 46-11
serial interface
clock settings 5-13
subinterface 3-2
service object groups
creating 16-7
deleting 16-9
editing 16-8
understanding 16-6
working with 16-7
service object groups reference
Create Service Object Groups dialog box 16-18
Edit Service Object Groups dialog box 16-34
Service Object Groups summary page 16-17
Session Initiation Protocol (SIP) 51-1
SHA_1 25-9
shared key 97-21
shared line
creating 56-27
show commands 63-17
signatures, see IPS
silent ring
call-waiting 59-44
night service bell 59-44
single number reach (SNR) 56-3
enable 56-16
SNMP, disabling 46-15
softkey
login override 59-6
telephony 53-1, 53-2
templates
associating phones 59-71
configuring 59-62
softkey template 59-66
speed-dial
intercom 59-31
split tunneling 25-21
SRST
configuring 49-1
formats 49-1
licenses 49-1
rerouting 50-1
SSH 26-15
enabling 46-24
standard rules 15-5

numbering range 15-7
startup configuration
write from file 63-1
static address translation rule 18-17
static route
configuring 3-4
configuring in WAN wizard 5-6
default 13-4
static translation rule
redirect port 18-20, 18-23
Status Bar 1-2
subinterfaces, for Serial and ATM interfaces 3-2
syslog
configuring 46-30
in IPS 41-18, 41-26
viewing 70-10

T

TCP keep-alive message, enabling 46-11
TCP small servers, disabling 46-7
TCP synwait time 46-13
telephony
configuring 53-1
date format 53-3, 53-5
features 59-1
hook flash 53-3, 53-5
hunt groups logout 53-3, 53-6
license 53-1
phone registration source IP address 53-5
softkey 53-1, 53-2
time format 53-3, 53-5
Telnet 63-2
Telnet user accounts 46-17
Telnet user accounts, configuring 46-29
template
extension 59-72
termination, call park 59-13
terminology, definitions 1-1
text banner, configuring 46-14, 46-30
time format 53-3, 53-5
time stamps, enabling 46-11
toolbar 1-2
configuring 59-2
Tools menu 95-1
Traffic
viewing activity 70-17
traffic flow 23-3, 23-5
icons 23-6
transform set 25-11, 36-7
transform sets, multiple 25-36
translation rules 18-9
translation timeouts 18-9
trunk
analog 12-3
digital 12-9

U

UDP small servers, disabling 46-8

unauthorized use of phones (After-Hours Tollbar) 59-2

unicast RPF, enabling 46-22

unsupported interface 3-2

- configuring a firewall on 22-18
- configuring as WAN 3-6
- configuring a VPN on 25-37
- configuring NAT on 3-8, 22-20

Unsupported Rules window 15-4

user accounts, Telnet 46-17

user configuration 56-12, 56-22, 56-41

user ID 56-36

user profile 1-11

users

- display name 56-48
- password generation 56-48, 56-51
- Phone tab 56-42, 56-54
- PIN generation 56-49, 56-52

users, phones, extensions

- basic workflow 56-1

user settings

- understanding 56-21

user settings reference

- Create User dialog box
  - Mailbox tab 56-50
  - Phone/Extension tab 56-42, 56-54
  - User tab 56-47
- Edit User dialog box
  - Mailbox tab 56-50
  - Phone/Extension tab 56-42, 56-54
  - User tab 56-47
- User Settings summary page 56-36

V

VCI 5-19

voice

- mailbox 56-50

voice class codecs

- creating 57-8
- deleting 57-8
- editing 57-8
- reference 57-9
- understanding 57-8

voice class codecs reference

- Create Voice Class Codec dialog box 57-11
- Edit Voice Class Codec dialog box 57-11
- Voice Class Codecs summary page 57-10

voice gateway mode 51-1

voicemail

- Cisco Unity Express 61-14
- default mailbox settings 61-9
- features 61-1
- greeting 56-54
- mailbox defaults 61-9

voice mode 47-5

VoIP parameters
disabling 58-2
enabling 58-2
enabling or disabling 58-2
reference 58-3
understanding 58-1
VPI 5-19
VPN 25-1, 25-23
AH authentication 25-12
configuring backup peers 25-35
configuring NAT passthrough 25-37
configuring on an unsupported interface 25-37
configuring on peer router 25-33
deleting tunnel 25-28
editing existing tunnel 25-34
ESP authentication 25-11
IP Compression 25-12
IPSec rule 25-14, 36-10
mirror configuration 25-33
mirror policy 25-29
multiple devices 25-36
multiple sites or tunnels 25-30
peers 36-6, 36-7
pre-shared key 25-7
protected traffic 25-7, 25-13, 36-9
remote IPSec peer 25-6
transform set 25-11, 36-7
transport mode 25-12
tunnel mode 25-12
viewing activity 25-34, 70-25
VPN concentrator
permitting traffic through a firewall to 22-21
vty lines
configuring an access class 46-23

W

WAN
cellular 9-1
WAN connections
deleting 6-57
WAN interface
unsupported 3-6
WCCP 64-3
Web Cache Communication Protocol 64-3
wireless support 8-1

X

Xauth logon 26-15