



## CONTENTS

Audience	3
Organization	3
Conventions	7
Related Documentation	8
<i>Hardware Documents</i>	8
Software Documentation	8
Cisco IOS Documentation	9
Commands in Task Tables	9
Notices	9
OpenSSL/Open SSL Project	10
License Issues	10
Obtaining Documentation and Submitting a Service Request	i-12

### **Product Overview** 1-1

Layer 2 Software Features	1-1
802.1Q Tunneling, VLAN Mapping, and Layer 2 Protocol Tunneling	1-2
Cisco IOS Auto Smartport Macros	1-2
Cisco Discovery Protocol	1-3
Cisco Group Management Protocol (CGMP) server	1-3
EtherChannel Bundles	1-3
Ethernet CFM	1-3
Ethernet OAM Protocol	1-3
Flex Links and MAC Address-Table Move Update	1-4
Flexible NetFlow (Supervisor Engine 7-E and 7L-E only)	1-4
Internet Group Management Protocol (IGMP) Snooping	1-4
IPv6 Multicast BSR and BSR Scoped Zone Support	1-5
IPv6 Multicast Listen Discovery (MLD) and Multicast Listen Discovery Snooping	1-6
Jumbo Frames	1-6
Link Aggregation Control Protocol	1-7
Cisco IOS XE IP Application Services Features in Cisco IOS XE 3.1.OSG	1-7
Link Layer Discovery Protocol	1-7
Link State Tracking	1-8
Location Service	1-8
Multiple Spanning Tree	1-8
Per-VLAN Rapid Spanning Tree	1-8

- Quality of Service **1-9**
  - Cisco Modular QoS Command-Line-Interface **1-9**
  - Two-Rate Three-Color Policing **1-9**
- Resilient Ethernet Protocol **1-10**
- SmartPort Macros **1-10**
- Spanning Tree Protocol **1-10**
- Stateful Switchover **1-10**
- SVI Autostate **1-11**
- Unidirectional Link Detection **1-11**
- VLANs **1-11**
- Virtual Switching Systems **1-12**
- Virtual Switch System Client **1-12**
- Y.1731 (AIS and RDI) **1-12**
- Layer 3 Software Features **1-13**
  - Bidirectional Forwarding Detection **1-14**
  - Cisco Express Forwarding **1-14**
  - Device Sensor **1-14**
  - EIGRP Stub Routing **1-14**
  - Enhanced Object Tracking **1-15**
  - GLBP **1-15**
    - Cisco IOS XE IP Application Services Features in Cisco IOS XE 3.1.OSG **1-15**
  - HSRP **1-16**
    - Cisco IOS XE IP Application Services: HSRP Features in Cisco IOS XE 3.1.OSG **1-16**
    - SSO Aware HSRP **1-16**
- IP Routing Protocols **1-17**
  - BGP **1-17**
  - EIGRP **1-17**
  - IS-IS **1-18**
  - OSPF **1-18**
  - RIP **1-19**
- In Service Software Upgrade **1-19**
- IPv6 **1-19**
- Multicast Services **1-19**
- NSF with SSO **1-20**
- OSPF for Routed Access **1-21**
- Policy-Based Routing **1-21**
- Unicast Reverse Path Forwarding **1-22**
- Unidirectional Link Routing **1-22**
- VRF-lite **1-22**
- Virtual Router Redundancy Protocol **1-22**

Management Features	1-23
Cisco Call Home	1-24
Cisco Energy Wise	1-24
Cisco IOS IP Service Level Agreements	1-24
Cisco Media Services Proxy	1-25
Cisco Medianet AutoQoS	1-25
Cisco Medianet Flow Metadata	1-26
Cisco IOS Mediatrace and Performance Monitor	1-26
Cisco Network Assistant	1-27
Dynamic Host Control Protocol	1-28
Easy Virtual Network	1-28
Embedded CiscoView	1-29
Embedded Event Manager	1-29
Ethernet Management Port	1-29
File System Management on Supervisor Engine 7-E and Supervisor Engine 7L-E	1-29
FAT File Management System on Supervisor Engine 6-E, Supervisor Engine 6L-E, Catalyst 4948E, and Catalyst 4900M	1-30
Forced 10/100 Autonegotiation	1-30
Intelligent Power Management	1-30
MAC Address Notification	1-30
MAC Notify MIB	1-30
NetFlow-lite	1-30
Power over Ethernet	1-31
Secure Shell	1-31
Simple Network Management Protocol	1-31
Smart Install	1-31
SPAN and RSPAN	1-32
Universal Power over Ethernet	1-32
Web Content Coordination Protocol	1-32
Wireshark	1-33
XML-PI	1-33
Security Features	1-33
802.1X Identity-Based Network Security	1-34
Cisco TrustSec MACsec Encryption	1-35
Cisco TrustSec Security Architecture	1-36
Cisco TrustSec Security Groups, SGTs and SGACLs	1-36
Dynamic ARP Inspection	1-37
Dynamic Host Configuration Protocol Snooping	1-37
Flood Blocking	1-37
Hardware-Based Control Plane Policing	1-37

IP Source Guard	1-38
IP Source Guard for Static Hosts	1-38
IPv6 First Hop Security	1-38
Local Authentication, RADIUS, and TACACS+ Authentication	1-40
Network Admission Control	1-40
Network Security with ACLs	1-40
Port Security	1-41
PPPoE Intermediate Agent	1-41
Session Aware Networking	1-41
Storm Control	1-42
uRPF Strict Mode	1-42
Utilities	1-42
Layer 2 Traceroute	1-42
Time Domain Reflectometry	1-43
Debugging Features	1-43
Web-based Authentication	1-43
New and Modified IOS Software Features Supported in Cisco IOS 15.2(1)E and Cisco IOS XE 3.5.0E	1-44
<b>Command-Line Interfaces</b>	2-1
Accessing the Switch CLI	2-2
Accessing the CLI Using the EIA/TIA-232 Console Interface	2-2
Accessing the CLI Through Telnet	2-2
Performing Command-Line Processing	2-3
Performing History Substitution	2-4
About Cisco IOS Command Modes	2-4
Getting a List of Commands and Syntax	2-5
Virtual Console for Standby Supervisor Engine	2-6
ROMMON Command-Line Interface	2-7
Archiving Crashfiles Information	2-8
Displaying a Crash Dump for Supervisor Engine 6-E and 6L-E	2-8
<b>Configuring the Switch for the First Time</b>	3-1
Default Switch Configuration	3-1
Configuring DHCP-Based Autoconfiguration	3-2
About DHCP-Based Autoconfiguration	3-2
DHCP Client Request Process	3-3
Configuring the DHCP Server	3-4
Configuring the TFTP Server	3-4
Configuring the DNS Server	3-5

Configuring the Relay Device	3-5
Obtaining Configuration Files	3-6
Example Configuration	3-7
Configuring the Switch	3-8
Using Configuration Mode to Configure Your Switch	3-9
Verifying the Running Configuration Settings	3-9
Saving the Running Configuration Settings to Your Start-Up File	3-10
Reviewing the Configuration in NVRAM	3-10
Configuring a Default Gateway	3-11
Configuring a Static Route	3-11
Controlling Access to Privileged EXEC Commands	3-13
Setting or Changing a Static enable Password	3-13
Using the enable password and enable secret Commands	3-14
Setting or Changing a Privileged Password	3-14
Controlling Switch Access with TACACS+	3-15
Understanding TACACS+	3-15
TACACS+ Operation	3-17
Configuring TACACS+	3-17
Displaying the TACACS+ Configuration	3-22
Encrypting Passwords	3-22
Configuring Multiple Privilege Levels	3-23
Setting the Privilege Level for a Command	3-23
Changing the Default Privilege Level for Lines	3-23
Logging In to a Privilege Level	3-24
Exiting a Privilege Level	3-24
Displaying the Password, Access Level, and Privilege Level Configuration	3-24
Recovering a Lost Enable Password	3-25
Modifying the Supervisor Engine Startup Configuration	3-25
Understanding the Supervisor Engine Boot Configuration	3-25
Understanding the ROM Monitor	3-26
Configuring the Software Configuration Register	3-26
Modifying the Boot Field and Using the boot Command	3-27
Modifying the Boot Field	3-28
Verifying the Configuration Register Setting	3-29
Specifying the Startup System Image	3-30
Flash Memory Features	3-31
Security Precautions	3-31
Configuring Flash Memory	3-31
Controlling Environment Variables	3-31

Resetting a Switch to Factory Default Settings 3-32

**Administering the Switch 4-1**

Managing the System Time and Date 4-1

System Clock 4-2

Understanding Network Time Protocol 4-2

Configuring NTP 4-3

Default NTP Configuration 4-4

Configuring NTP Authentication 4-4

Configuring NTP Associations 4-6

Configuring NTP Broadcast Service 4-7

Configuring NTP Access Restrictions 4-8

Configuring the Source IP Address for NTP Packets 4-10

Displaying the NTP Configuration 4-11

Configuring Time and Date Manually 4-11

Setting the System Clock 4-11

Displaying the Time and Date Configuration 4-12

Configuring the Time Zone 4-12

Configuring Summer Time (Daylight Saving Time) 4-13

**Managing Software Licenses Using Permanent Right-To-Use Features 4-14**

About a PRTU License 4-15

Benefits of a PRTU License 4-15

Guidelines for the RTU License Model 4-16

Applying a PRTU License 4-16

Activating a PRTU License 4-16

Deactivating a PRTU License 4-17

Displaying Software License Information 4-17

Configuring a System Name and Prompt 4-21

Configuring a System Name 4-22

Understanding DNS 4-22

Default DNS Configuration 4-23

Setting Up DNS 4-23

Displaying the DNS Configuration 4-24

Creating a Banner 4-24

Default Banner Configuration 4-24

Configuring a Message-of-the-Day Login Banner 4-24

Configuring a Login Banner 4-27

Managing the MAC Address Table 4-28

Building the Address Table 4-28

MAC Addresses and VLANs 4-29

Default MAC Address Table Configuration	4-30
Changing the Address Aging Time	4-30
Removing Dynamic Address Entries	4-31
Configuring MAC Change Notification Traps	4-31
Configuring MAC Move Notification Traps	4-33
Configuring MAC Threshold Notification Traps	4-35
Adding and Removing Static Address Entries	4-36
Configuring Unicast MAC Address Filtering	4-37
Disabling MAC Address Learning on a VLAN	4-39
Configuring Disable MAC Address Learning	4-39
Usage Guidelines	4-40
Deployment Scenarios	4-40
Feature Compatibility	4-42
Feature Incompatibility	4-43
Partial Feature Incompatibility	4-43
Displaying Address Table Entries	4-44
Managing the ARP Table	4-44
Configuring Embedded CiscoView Support	4-44
Understanding Embedded CiscoView	4-45
Installing and Configuring Embedded CiscoView	4-45
Displaying Embedded CiscoView Information	4-48
<b>Configuring Virtual Switching Systems</b>	<b>5-1</b>
Understanding Virtual Switching Systems	5-2
VSS Overview	5-2
Key Concepts	5-3
VSS Functionality	5-5
Hardware Requirements	5-9
Understanding VSL Topology	5-11
VSS Redundancy	5-11
Overview	5-12
RPR and SSO Redundancy	5-12
Switch Roles in a VSS	5-12
Failed Switch Recovery	5-13
VSL Failure	5-14
User Actions	5-14
Multichassis EtherChannels	5-14
Overview	5-14
MEC Failure Scenarios	5-15
Packet Handling	5-16

Traffic on the VSL	5-16
Layer 2 Protocols	5-17
Layer 3 Protocols	5-18
System Monitoring	5-20
Environmental Monitoring	5-20
File System Access	5-20
Diagnostics	5-21
Network Management	5-21
Dual-Active Detection	5-23
Dual-Active Detection Using Enhanced PAGP	5-23
Dual-Active Detection Using Fast-Hello	5-24
Recovery Actions	5-24
Configuring a Recovery IP Address	5-25
VSS Initialization	5-26
Virtual Switch Link Protocol	5-26
SSO Dependencies	5-27
Initialization Procedure	5-27
VSS Configuration Guidelines and Restrictions	5-28
General VSS Restrictions and Guidelines	5-28
Multichassis EtherChannel Restrictions and Guidelines	5-30
Dual-Active Detection Restrictions and Guidelines	5-30
Configuring a VSS	5-30
Converting to a VSS	5-30
Backing Up the Standalone Configuration	5-32
Configuring SSO and NSF	5-32
Assigning Virtual Switch Domain and Switch Numbers	5-32
Configuring VSL Port Channel and Ports	5-33
Converting the Switch to Virtual Switch Mode	5-34
(Optional) Configuring VSS Standby Switch Modules	5-35
Displaying VSS Information	5-36
Converting a VSS to Standalone Switch	5-37
Copying the VSS Configuration to a Backup File	5-38
Converting the VSS Active Switch to Standalone	5-38
Converting the VSS Standby Switch to Standalone	5-38
Configuring VSS Parameters	5-39
Configuring VSL Switch Priority	5-39
Configuring a VSL	5-41
Adding and Deleting a VSL Port After the Bootup	5-41
Displaying VSL Information	5-42
Configuring VSL QoS	5-43



Configuring the Router MAC Address	5-44
Configuring Multichassis EtherChannels	5-45
Configuring Dual-Active Detection	5-49
Configuring Enhanced PAgP Dual-Active Detection	5-49
Configuring Fast-Hello Dual-Active Detection	5-50
Displaying Dual-Active Detection	5-51
In-Service Software Upgrade (ISSU) on a VSS	5-53
VSS ISSU Concept	5-53
Traffic and Network Protocol Disruption During ISSU in a VSS	5-55
Related Documents	5-55
Prerequisites to Performing ISSU	5-55
About Performing ISSU	5-56
Performing an ISSU Upgrade: Two Methods	5-56
Guidelines for Performing ISSU	5-59
Compatibility Matrix	5-59
Compatibility Verification Using Cisco Feature Navigator	5-60
How to Perform the ISSU Process	5-61
Verifying the ISSU Software Installation	5-61
Verifying Redundancy Mode Before Beginning the ISSU Process	5-62
Verifying the ISSU State Before Beginning the ISSU Process	5-63
ISSU using the Four-command Sequence: Step 1 (loadversion)	5-65
ISSU using the Four-command Sequence: Step 2 (runversion)	5-66
ISSU using the Four Command Sequence: Step 3 (acceptversion)	5-68
ISSU using the Four Command Sequence: Step 4 (commitversion)	5-69
Using changeversion to Automate an ISSU Upgrade	5-70
Aborting a Software Upgrade During ISSU	5-76
Configuring the Rollback Timer to Safeguard Against Upgrade Issues	5-77
The ISSU Compatibility Matrix	5-79
License Upgrade on a VSS	5-81
<b>Configuring the Cisco IOS In-Service Software Upgrade Process</b>	<b>6-1</b>
Prerequisites to Performing ISSU	6-2
About ISSU	6-3
Stateful Switchover Overview	6-3
NSF Overview	6-5
ISSU Process Overview	6-6
Performing an ISSU Upgrade: 2 Methods	6-11
Changeversion Process	6-12
Changeversion: Quick Option	6-12
Scheduled Changeversion: "in" and "at" Options	6-12

- Changeversion Deployment Scenario 6-13
- Aborting an In-Progress Changeversion Procedure 6-13
- Guidelines for Performing ISSU 6-13
- Versioning Capability in Cisco IOS Software to Support ISSU 6-13
  - Compatibility Matrix 6-14
  - SNMP Support for ISSU 6-15
  - Compatibility Verification Using Cisco Feature Navigator 6-15
- Performing the ISSU Process 6-15
  - Upgrading ISSU to Cisco IOS XE 3.4.0SG/15.1(2)SG from a Prior Release 6-16
  - Downgrading ISSU from Cisco IOS XE 3.4.0SG/15.1(2)SG to a Prior Release 6-17
  - Verifying the ISSU Software Installation 6-18
  - Verifying Redundancy Mode Before Beginning the ISSU Process 6-19
  - Verifying the ISSU State Before Beginning the ISSU Process 6-20
  - Loading New Cisco IOS Software on the Standby Supervisor Engine 6-21
  - Switching to the Standby Supervisor Engine 6-24
  - Stopping the ISSU Rollback Timer (Optional) 6-26
  - Loading New Cisco IOS Software on the New Standby Supervisor Engine 6-27
  - Using changeversion to Automate an ISSU Upgrade 6-29
  - Aborting a Software Upgrade During ISSU 6-34
  - Configuring the Rollback Timer to Safeguard Against Upgrade Issues 6-35
  - Displaying ISSU Compatibility Matrix Information 6-36
  - Displaying ISSU Compatibility Matrix Information 6-40
- Related Documents 6-42

**Configuring the Cisco IOS XE In Service Software Upgrade Process 7-1**

- Related Documents 7-2
- Prerequisites to Performing ISSU 7-2
- About Performing ISSU 7-3
  - Stateful Switchover 7-3
  - NSF 7-5
  - ISSU Process 7-6
  - Performing an ISSU Upgrade: 2 Methods 7-11
  - Changeversion Process 7-12
    - Changeversion: Quick Option (LV to INIT) 7-12
    - Scheduled Changeversion: “in” and “at” Options 7-12
    - Changeversion Deployment Scenario 7-13
    - Aborting an In-Progress Changeversion Procedure 7-13
- Guidelines for Performing ISSU 7-13
  - Compatibility Matrix 7-13
  - SNMP Support for ISSU 7-14

Compatibility Verification Using Cisco Feature Navigator	7-14
How to Perform the ISSU Process	7-15
Upgrading ISSU to Cisco IOS XE 3.4.0SG/15.1(2)SG from a Prior Release	7-15
Downgrading ISSU from Cisco IOS XE 3.4.0SG/15.1(2)SG to a Prior Release	7-17
Verifying the ISSU Software Installation	7-18
Verifying Redundancy Mode Before Beginning the ISSU Process	7-18
Verifying the ISSU State Before Beginning the ISSU Process	7-20
Loading New Cisco IOS XE Software on the Standby Supervisor Engine	7-20
Switching to the Standby Supervisor Engine	7-23
Stopping the ISSU Rollback Timer (Optional)	7-25
Loading New Cisco IOS XE Software on the New Standby Supervisor Engine	7-26
Using changeversion to Automate an ISSU Upgrade	7-28
Aborting a Software Upgrade During ISSU	7-33
Configuring the Rollback Timer to Safeguard Against Upgrade Issues	7-35
Displaying ISSU Compatibility Matrix Information	7-36
Cisco High Availability Features in Cisco IOS XE 3.1.0SG	7-38

## Configuring Interfaces 8-1

About Interface Configuration	8-2
Using the interface Command	8-2
Configuring a Range of Interfaces	8-4
Using the Ethernet Management Port	8-6
Understanding the Ethernet Management Port	8-6
Fa1 Interface and mgmtVrf	8-7
SSO Model	8-9
ISSU Model	8-10
Supported Features on the Ethernet Management Port	8-10
Configuring the Ethernet Management Port	8-10
Defining and Using Interface-Range Macros	8-11
Deploying SFP+ in X2 Ports	8-12
Deploying 10-Gigabit Ethernet and Gigabit Ethernet SFP Ports on Supervisor Engine V-10GE	8-12
Deploying 10-Gigabit Ethernet or Gigabit Ethernet Ports	8-13
Port Numbering TwinGig Convertors	8-13
Limitations on Using a TwinGig Convertor	8-14
Selecting X2/TwinGig Convertor Mode	8-14
Invoking Shared-Backplane Uplink Mode on Supervisor Engine 6-E and Supervisor Engine 6L-E	8-16
Limitation and Restrictions on Supervisor Engine 7-E and Supervisor Engine 7L-E	8-16
Selecting Uplink Mode on a Supervisor Engine 6-E	8-16

- Support for WS-X46490-CSFP-E on a 10-slot Chassis 8-17
- Selecting the Uplink Port on a Supervisor Engine 7L-E 8-18
  - Single Supervisor Mode 8-18
  - Redundant Supervisor Mode 8-19
- Digital Optical Monitoring Transceiver Support 8-19
- Configuring Optional Interface Features 8-20
  - Configuring Ethernet Interface Speed and Duplex Mode 8-20
    - Speed and Duplex Mode Configuration Guidelines 8-20
    - Setting the Interface Speed 8-21
    - Setting the Interface Duplex Mode 8-22
    - Displaying the Interface Speed and Duplex Mode Configuration 8-22
    - Adding a Description for an Interface 8-23
  - Configuring Flow Control 8-23
  - Configuring Jumbo Frame Support 8-26
    - Ports and Modules That Support Jumbo Frames 8-26
    - Jumbo Frame Support 8-26
    - Configuring MTU Sizes 8-28
  - Interacting with Baby Giants 8-29
  - Configuring the Port Debounce Timer 8-29
  - Configuring Auto-MDIX on a Port 8-30
    - Displaying the Interface Auto-MDIX Configuration 8-32
- Understanding Online Insertion and Removal 8-33
- Online Insertion and Removal on a WS-4500X-32 8-33
  - Shutting down a Module 8-34
  - Booting a Module After if it has been Stopped 8-34
  - Common Scenarios 8-35
- Monitoring and Maintaining the Interface 8-35
  - Monitoring Interface and Controller Status 8-36
  - Clearing and Resetting the Interface 8-36
  - Shutting Down and Restarting an Interface 8-37
  - Configuring Interface Link Status and Trunk Status Events 8-37
    - Configuring Link Status Event Notification for an Interface 8-38
    - Global Settings 8-38
    - Configuring a Switch Global Link Status Logging Event 8-38
    - Examples 8-38
  - Resetting the Interface to the Default Configuration 8-40

**Checking Port Status and Connectivity 9-1**

- Checking Module Status 9-1

Checking Interfaces Status	9-2
Displaying MAC Addresses	9-3
Checking Cable Status Using Time Domain Reflectometer	9-3
Overview	9-3
Running the TDR Test	9-4
TDR Guidelines	9-5
Using Telnet	9-5
Changing the Logout Timer	9-6
Monitoring User Sessions	9-6
Using Ping	9-7
Understanding How Ping Works	9-7
Running Ping	9-8
Using IP Traceroute	9-8
Understanding How IP Traceroute Works	9-8
Running IP Traceroute	9-9
Using Layer 2 Traceroute	9-9
Layer 2 Traceroute Usage Guidelines	9-10
Running Layer 2 Traceroute	9-11
Configuring ICMP	9-12
Enabling ICMP Protocol Unreachable Messages	9-12
Enabling ICMP Redirect Messages	9-12
Enabling ICMP Mask Reply Messages	9-13
<b>Configuring Supervisor Engine Redundancy Using RPR and SSO on Supervisor Engine 6-E and Supervisor Engine 6L-E</b>	<b>10-1</b>
About Supervisor Engine Redundancy	10-2
Overview	10-2
RPR Operation	10-2
SSO Operation	10-3
About Supervisor Engine Redundancy Synchronization	10-4
RPR Supervisor Engine Configuration Synchronization	10-5
SSO Supervisor Engine Configuration Synchronization	10-5
Supervisor Engine Redundancy Guidelines and Restrictions	10-5
Configuring Supervisor Engine Redundancy	10-7
Configuring Redundancy	10-8
Virtual Console for Standby Supervisor Engine	10-10
Synchronizing the Supervisor Engine Configurations	10-11
Performing a Manual Switchover	10-12
Performing a Software Upgrade	10-13

Manipulating Bootflash on the Redundant Supervisor Engine 10-14

**Configuring Supervisor Engine Redundancy Using RPR and SSO on Supervisor Engine 7-E and Supervisor Engine 7L-E 11-1**

About Supervisor Engine Redundancy 11-2

Overview 11-2

RPR Operation 11-3

SSO Operation 11-3

About Supervisor Engine Redundancy Synchronization 11-5

RPR Supervisor Engine Configuration Synchronization 11-5

SSO Supervisor Engine Configuration Synchronization 11-5

Supervisor Engine Redundancy Guidelines and Restrictions 11-5

Configuring Supervisor Engine Redundancy 11-7

Configuring Redundancy 11-7

Virtual Console for Standby Supervisor Engine 11-9

Synchronizing the Supervisor Engine Configurations 11-10

Performing a Manual Switchover 11-12

Performing a Software Upgrade 11-12

Manipulating Bootflash on the Standby Supervisor Engine 11-14

**Configuring Cisco NSF with SSO Supervisor Engine Redundancy 12-1**

About NSF with SSO Supervisor Engine Redundancy 12-1

About Cisco IOS NSF-Aware and NSF-Capable Support 12-2

NSF with SSO Supervisor Engine Redundancy Overview 12-3

SSO Operation 12-4

NSF Operation 12-4

Cisco Express Forwarding 12-5

Routing Protocols 12-5

BGP Operation 12-5

OSPF Operation 12-6

IS-IS Operation 12-7

EIGRP Operation 12-8

NSF Guidelines and Restrictions 12-9

Configuring NSF with SSO Supervisor Engine Redundancy 12-9

Configuring SSO 12-10

Configuring CEF NSF 12-10

Verifying CEF NSF 12-11

Configuring BGP NSF 12-11

Verifying BGP NSF 12-11

Configuring OSPF NSF 12-12

Verifying OSPF NSF	12-13
Configuring IS-IS NSF	12-13
Verifying IS-IS NSF	12-14
Configuring EIGRP NSF	12-16
Verifying EIGRP NSF	12-16
Cisco High Availability Features in Cisco IOS XE 3.1.OSG	12-17
<b>Environmental Monitoring and Power Management</b>	<b>13-1</b>
About Environmental Monitoring	13-1
Using CLI Commands to Monitor your Environment	13-2
Displaying Environment Conditions	13-2
Displaying On Board Failure Logging (OBFL) information for 9000W AC	13-4
Emergency Actions	13-5
System Alarms	13-6
Power Management	13-7
Power Management for the Catalyst 4500 Series Switches	13-7
Supported Power Supplies	13-8
Power Management Modes for the Catalyst 4500 Switch	13-9
Selecting a Power Management Mode	13-10
Power Management Limitations in Catalyst 4500 Series Switches	13-10
Available Power for Catalyst 4500 Series Switches Power Supplies	13-14
Special Considerations for the 4200 W AC and 6000 W AC Power Supplies	13-15
Combined Mode Power Resiliency	13-19
Special Considerations for the 1400 W DC Power Supply	13-21
Special Considerations for the 1400 W DC SP Triple Input Power Supply	13-22
Powering Down a Module	13-22
Power Management for the Catalyst 4948 Switches	13-23
Power Management Modes for the Catalyst 4948 Switch	13-23
IEEE 802.3az Energy Efficient Ethernet	13-23
Determining EEE Capability	13-24
Enabling EEE	13-24
Determining EEE Status	13-24
<b>Configuring Power over Ethernet</b>	<b>14-1</b>
About Power over Ethernet	14-1
Hardware Requirements	14-2
Power Management Modes	14-2
Intelligent Power Management	14-4
Configuring Power Consumption for Powered Devices on an Interface	14-5
Displaying the Operational Status for an Interface	14-6

- Displaying all PoE Detection and Removal Events 14-7
- Displaying the PoE Consumed by a Module 14-8
- PoE Policing and Monitoring 14-12
  - PoE Policing Modes 14-12
  - Configuring Power Policing on an Interface 14-13
  - Displaying Power Policing on an Interface 14-14
  - Configuring Errdisable Recovery 14-14
- Enhanced Power PoE Support on the E-Series Chassis 14-15
  - Configuring Universal PoE 14-16

**Configuring the Catalyst 4500 Series Switch with Cisco Network Assistant 15-1**

- About Network Assistant 15-2
  - Community Overview 15-2
  - Clustering Overview 15-2
- Network Assistant-Related Parameters and Their Defaults 15-3
- Network Assistant CLI Commands 15-3
- Configuring Your Switch for Network Assistant 15-4
  - (Minimum) Required Configuration 15-4
  - (Additional) Configuration Required to Use Community 15-5
  - (Additional) Configuration Required to Use Clustering 15-5
- Managing a Network Using Community 15-6
  - Candidate and Member Requirements 15-7
  - Automatic Discovery of Candidates and Members 15-7
  - Community Names 15-8
  - Hostnames 15-8
  - Passwords 15-8
  - Communication Protocols 15-8
  - Access Modes in Network Assistant 15-9
  - Community Information 15-9
  - Adding Devices 15-9
- Converting a Cluster into a Community 15-10
- Managing a Network Using Cluster 15-11
  - Understanding Switch Clusters 15-11
    - Cluster Command Switch Requirements 15-11
    - Network Assistant and VTY 15-12
    - Candidate Switch and Cluster Member Switch Requirements 15-12
  - Using the CLI to Manage Switch Clusters 15-13
- Configuring Network Assistant in Community or Cluster Mode 15-13
  - Configuring Network Assistant on a Networked Switch in Community Mode 15-13



Configuring Network Assistant in a Networked Switch in Cluster Mode 15-17

## **Configuring VLANs, VTP, and VMPS 16-1**

### **VLANs 16-1**

About VLANs 16-1

VLAN Configuration Guidelines and Restrictions 16-3

VLAN Ranges 16-3

Configurable Normal-Range VLAN Parameters 16-4

VLAN Default Configuration 16-4

Configuring VLANs 16-5

Configuring VLANs in Global Configuration Mode 16-6

Assigning a Layer 2 LAN Interface to a VLAN 16-7

### **VLAN Trunking Protocol 16-7**

About VTP 16-8

Understanding the VTP Domain 16-8

Understanding VTP Modes 16-9

Understanding VTP Advertisements 16-9

Understanding VTP Versions 16-9

Understanding VTP Pruning 16-11

VTP Configuration Guidelines and Restrictions 16-12

VTP Default Configuration 16-13

Configuring VTP 16-14

Configuring VTP Global Parameters 16-14

Configuring the VTP Mode 16-16

Starting a Takeover 16-19

Displaying VTP Statistics 16-19

Displaying VTP Devices in a Domain 16-20

### **VLAN Membership Policy Server 16-20**

About VMPS 16-20

Understanding the VMPS Server 16-21

Security Modes for VMPS Server 16-21

Fallback VLAN 16-22

Illegal VMPS Client Requests 16-23

Overview of VMPS Clients 16-23

Understanding Dynamic VLAN Membership 16-23

Default VMPS Client Configuration 16-24

Configuring a Switch as a VMPS Client 16-24

Administering and Monitoring the VMPS 16-27

Troubleshooting Dynamic Port VLAN Membership 16-28

Dynamic Port VLAN Membership Configuration Example 16-29

VMPS Database Configuration File Example 16-32

**Configuring IP Unnumbered Interface 17-1**

- About IP Unnumbered Interface Support 17-1
  - IP Unnumbered Interface Support with DHCP Server and Relay Agent 17-2
  - DHCP Option 82 17-2
  - IP Unnumbered Interface with Connected Host Polling 17-3
- IP Unnumbered Configuration Guidelines and Restrictions 17-3
- Configuring IP Unnumbered Interface Support with DHCP Server 17-4
  - Configuring IP Unnumbered Interface Support on LAN and VLAN Interfaces 17-4
  - Configuring IP Unnumbered Interface Support on a Range of Ethernet VLANs 17-5
- Configuring IP Unnumbered Interface Support with Connected Host Polling 17-6
- Displaying IP Unnumbered Interface Settings 17-7
- Troubleshooting IP Unnumbered Interface 17-8
- Related Documents 17-8

**Configuring Layer 2 Ethernet Interfaces 18-1**

- About Layer 2 Ethernet Switching 18-1
  - Layer 2 Ethernet Switching 18-2
    - Switching Frames Between Segments 18-2
    - Building the MAC Address Table 18-2
  - VLAN Trunks 18-3
  - Layer 2 Interface Modes 18-3
- Default Layer 2 Ethernet Interface Configuration 18-4
- Layer 2 Interface Configuration Guidelines and Restrictions 18-4
- Configuring Ethernet Interfaces for Layer 2 Switching 18-5
  - Configuring an Ethernet Interface as a Layer 2 Trunk 18-5
  - Configuring an Interface as a Layer 2 Access Port 18-7
  - Clearing Layer 2 Configuration 18-8

**Configuring SmartPort Macros 19-1**

- About SmartPort Macros and Static SmartPort 19-1
- Configuring SmartPort Macros 19-2
  - Passing Parameters Through the Macro 19-3
    - Macro Parameter Help 19-3
  - Default SmartPort Macro Configuration 19-4
    - cisco-global 19-4
    - cisco-desktop 19-4
    - cisco-phone 19-5

cisco-router	19-5
cisco-switch	19-5
SmartPort Macro Configuration Guidelines	19-6
Creating SmartPort Macros	19-8
Applying SmartPort Macros	19-8
cisco-global	19-10
cisco-desktop	19-10
cisco-phone	19-11
cisco-switch	19-11
cisco-router	19-12
Displaying SmartPort Macros	19-13
Configuring Static SmartPort Macros	19-13
Default Static SmartPort Configuration	19-13
Static SmartPort Configuration Guidelines	19-14
Applying Static SmartPort Macros	19-14
<b>Configuring Cisco IOS Auto Smartport Macros</b>	<b>20-1</b>
About Auto Smartport Macros	20-1
Device Classifier	20-2
Device Visibility Mode	20-3
Configuring Auto Smartport Macros	20-3
Enabling Auto Smartport Macros	20-3
Auto Smartport Default Configuration	20-4
Auto Smartport Configuration Guidelines	20-5
Configuring Auto Smartport Built-in Macro Parameters	20-6
Configuring User-Defined Event Triggers	20-8
802.1X-Based Event Trigger	20-8
MAC Address-Based Event Trigger	20-9
Configuring Mapping Between User-Defined Triggers and Built-in Macros	20-9
Configuring Auto Smartport User-Defined Macros	20-10
Displaying Auto Smartport	20-13
<b>Configuring STP and MST</b>	<b>21-1</b>
About STP	21-1
Understanding the Bridge ID	21-2
Bridge Priority Value	21-2
Extended System ID	21-3
STP MAC Address Allocation	21-3
Bridge Protocol Data Units	21-3
Election of the Root Bridge	21-4

- STP Timers 21-4
- Creating the STP Topology 21-5
- STP Port States 21-5
- MAC Address Allocation 21-6
- STP and IEEE 802.1Q Trunks 21-6
- Per-VLAN Rapid Spanning Tree 21-6
- Default STP Configuration 21-7
- Configuring STP 21-7
  - Enabling STP 21-8
  - Enabling the Extended System ID 21-9
  - Configuring the Root Bridge 21-9
  - Configuring a Secondary Root Switch 21-12
  - Configuring STP Port Priority 21-13
  - Configuring STP Port Cost 21-15
  - Configuring the Bridge Priority of a VLAN 21-17
  - Configuring the Hello Time 21-17
  - Configuring the Maximum Aging Time for a VLAN 21-18
  - Configuring the Forward-Delay Time for a VLAN 21-19
  - Disabling Spanning Tree Protocol 21-20
  - Enabling Per-VLAN Rapid Spanning Tree 21-20
    - Specifying the Link Type 21-21
    - Restarting Protocol Migration 21-21
- About MST 21-22
  - IEEE 802.1s MST 21-22
  - IEEE 802.1w RSTP 21-23
    - RSTP Port Roles 21-24
    - RSTP Port States 21-24
  - MST-to-SST Interoperability 21-24
  - Common Spanning Tree 21-25
  - MST Instances 21-26
  - MST Configuration Parameters 21-26
  - MST Regions 21-26
    - MST Region Overview 21-26
    - Boundary Ports 21-27
    - IST Master 21-27
    - Edge Ports 21-27
    - Link Type 21-28
  - Message Age and Hop Count 21-28
  - MST-to-PVST+ Interoperability 21-28

MST Configuration Restrictions and Guidelines 21-29

Configuring MST 21-29

Enabling MST 21-29

Configuring MST Instance Parameters 21-31

Configuring MST Instance Port Parameters 21-32

Restarting Protocol Migration 21-33

Displaying MST Configurations 21-33

**Configuring Flex Links and MAC Address-Table Move Update 22-1**

About Flex Links 22-1

Flex Links 22-2

VLAN Flex Links Load Balancing and Support 22-2

Flex Links Failover Actions 22-3

MAC Address-Table Move Update 22-4

Configuring Flex Links 22-5

Default Configuration 22-5

Configuration Guidelines 22-6

Configuring Flex Links 22-6

Configuring VLAN Load Balancing on Flex Links 22-8

Configuring MAC Address-Table Move Update 22-10

Default Configuration 22-10

Configuration Guidelines 22-10

Configuring the MAC Address-Table Move Update Feature 22-10

Configuring a Switch to Send MAC Address-Table Move Updates 22-10

Configuring a Switch to Receive MAC Address-Table Move Updates 22-12

Monitoring Flex Links and the MAC Address-Table Move Update 22-12

22-12

**Configuring Resilient Ethernet Protocol 23-1**

About REP 23-1

Link Integrity 23-4

Fast Convergence 23-4

VLAN Load Balancing 23-4

Spanning Tree Interaction 23-6

REP Ports 23-6

Configuring REP 23-7

Default REP Configuration 23-7

REP Configuration Guidelines 23-7

Configuring the REP Administrative VLAN 23-8

Configuring REP Interfaces 23-9

Setting Manual Preemption for VLAN Load Balancing	23-13
Configuring SNMP Traps for REP	23-14
Monitoring REP	23-14
<b>Configuring Optional STP Features</b>	<b>24-1</b>
About Root Guard	24-2
Enabling Root Guard	24-2
About Loop Guard	24-3
Enabling Loop Guard	24-4
About EtherChannel Guard	24-6
Enabling EtherChannel Guard (Optional)	24-6
About PortFast	24-6
Enabling PortFast	24-7
About BPDU Guard	24-8
Enabling BPDU Guard	24-8
About PortFast BPDU Filtering	24-9
Enabling PortFast BPDU Filtering	24-9
About UplinkFast	24-11
Enabling UplinkFast	24-12
About BackboneFast	24-13
Enabling BackboneFast	24-15
<b>Configuring EtherChannel and Link State Tracking</b>	<b>25-1</b>
About EtherChannel	25-2
Port Channel Interfaces	25-2
Configuring EtherChannels	25-3
EtherChannel Configuration Overview	25-3
Manual EtherChannel Configuration	25-3
PAgP EtherChannel Configuration	25-4
IEEE 802.3ad LACP EtherChannel Configuration	25-4
Load Balancing	25-5
EtherChannel Configuration Guidelines and Restrictions	25-5
Configuring EtherChannel	25-6
Configuring Layer 3 EtherChannels	25-7
Creating Port Channel Logical Interfaces	25-7
Configuring Physical Interfaces as Layer 3 EtherChannels	25-7
Configuring Layer 2 EtherChannels	25-10
Configuring LACP Standalone or Independent Mode	25-12

Configuring the LACP System Priority and System ID	25-13
Configuring EtherChannel Load Balancing	25-14
Removing an Interface from an EtherChannel	25-15
Removing an EtherChannel	25-15
Displaying EtherChannel to a Virtual Switch System	25-16
Understanding VSS Client	25-16
Virtual Switch System	25-16
Dual-Active Scenarios	25-16
Dual-Active Detection Using Enhanced PAGP	25-16
Displaying EtherChannel Links to VSS	25-18
Understanding Link-State Tracking	25-18
Configuring Link-State Tracking	25-21
Default Link-State Tracking Configuration	25-21
Link-State Tracking Configuration Guidelines	25-21
Configuring Link-State Tracking	25-21
Displaying Link-State Tracking Status	25-22

## **Configuring IGMP Snooping and Filtering, and MVR** 26-1

About IGMP Snooping	26-2
Immediate-Leave Processing	26-3
IGMP Configurable-Leave Timer	26-4
IGMP Snooping Querier	26-4
Explicit Host Tracking	26-4
Configuring IGMP Snooping	26-5
Default IGMP Snooping Configuration	26-5
Enabling IGMP Snooping Globally	26-6
Enabling IGMP Snooping on a VLAN	26-6
Configuring Learning Methods	26-7
Configuring PIM/DVMRP Learning	26-7
Configuring CGMP Learning	26-7
Configuring a Static Connection to a Multicast Router	26-8
Enabling IGMP Immediate-Leave Processing	26-8
Configuring the IGMP Leave Timer	26-9
Configuring IGMP Snooping Querier	26-10
Configuring Explicit Host Tracking	26-11
Configuring a Host Statically	26-11
Suppressing Multicast Flooding	26-12
IGMP Snooping Interface Configuration	26-12
IGMP Snooping Switch Configuration	26-13

Displaying IGMP Snooping Information	26-14
Displaying Querier Information	26-15
Displaying IGMP Host Membership Information	26-15
Displaying Group Information	26-16
Displaying Multicast Router Interfaces	26-17
Displaying MAC Address Multicast Entries	26-18
Displaying IGMP Snooping Information on a VLAN Interface	26-18
Displaying IGMP Snooping Querier Information	26-19
Understanding Multicast VLAN Registration	26-20
Using MVR in a Multicast Television Application	26-21
Configuring MVR	26-23
Default MVR Configuration	26-23
MVR Configuration Guidelines and Limitations	26-23
Configuring MVR Global Parameters	26-24
Configuring MVR on Access Ports	26-26
Configuring MVR on a Trunk Port	26-27
Displaying MVR Information	26-29
Configuring IGMP Filtering	26-30
Default IGMP Filtering Configuration	26-30
Configuring IGMP Profiles	26-31
Applying IGMP Profiles	26-32
Setting the Maximum Number of IGMP Groups	26-33
Displaying IGMP Filtering Configuration	26-34
<b>Configuring IPv6 Multicast Listener Discovery Snooping</b>	<b>27-1</b>
About MLD Snooping	27-1
MLD Messages	27-2
MLD Queries	27-3
Multicast Client Aging	27-3
Multicast Router Discovery	27-3
MLD Reports	27-4
MLD Done Messages and Immediate-Leave	27-4
Topology Change Notification Processing	27-4
Configuring IPv6 MLD Snooping	27-5
Default MLD Snooping Configuration	27-5
MLD Snooping Configuration Guidelines	27-6
Enabling or Disabling MLD Snooping	27-6
Configuring a Static Multicast Group	27-7
Configuring a Multicast Router Port	27-7



Enabling MLD Immediate Leave	27-8
Configuring MLD Snooping Queries	27-9
Disabling MLD Listener Message Suppression	27-10
Displaying MLD Snooping Information	27-10
<b>Configuring 802.1Q Tunneling, VLAN Mapping, and Layer 2 Protocol Tunneling</b>	<b>28-1</b>
About 802.1Q Tunneling	28-2
Configuring 802.1Q Tunneling	28-3
802.1Q Tunneling Configuration Guidelines	28-3
Native VLANs	28-4
System MTU	28-5
802.1Q Tunneling and Other Features	28-5
Configuring an 802.1Q Tunneling Port	28-6
About VLAN Mapping	28-7
Deployment Example	28-7
Mapping Customer VLANs to Service-Provider VLANs	28-9
Configuring VLAN Mapping	28-9
Default VLAN Mapping Configuration	28-9
VLAN Mapping Configuration Guidelines	28-10
Configuring VLAN Mapping	28-11
One-to-One Mapping	28-11
Traditional Q-in-Q on a Trunk Port	28-12
Selective Q-in-Q on a Trunk Port	28-12
About Layer 2 Protocol Tunneling	28-13
Configuring Layer 2 Protocol Tunneling	28-15
Default Layer 2 Protocol Tunneling Configuration	28-16
Layer 2 Protocol Tunneling Configuration Guidelines	28-16
Configuring Layer 2 Tunneling	28-17
Monitoring and Maintaining Tunneling Status	28-18
<b>Configuring CDP</b>	<b>29-1</b>
About CDP	29-1
Configuring CDP	29-2
Enabling CDP Globally	29-2
Displaying the CDP Global Configuration	29-2
Enabling CDP on an Interface	29-3
Displaying the CDP Interface Configuration	29-3
Monitoring and Maintaining CDP	29-3

<b>Configuring LLDP, LLDP-MED, and Location Service</b>	<b>30-1</b>
About LLDP, LLDP-MED, and Location Service	30-1
LLDP	30-1
LLDP-MED	30-2
Location Service	30-3
Configuring LLDP and LLDP-MED, and Location Service	30-4
Default LLDP Configuration	30-5
Configuring LLDP Characteristics	30-5
Disabling and Enabling LLDP Globally	30-6
Disabling and Enabling LLDP on an Interface	30-7
Configuring LLDP-MED TLVs	30-9
Configuring Network-Policy Profile	30-10
Configuring LLDP Power Negotiation	30-11
Configuring Location TLV and Location Service	30-12
Monitoring and Maintaining LLDP, LLDP-MED, and Location Service	30-14
Cisco IOS Carries Ethernet Features in Cisco IOS XE 3.1.OSG	30-15
<b>Configuring UDLD</b>	<b>31-1</b>
About UDLD	31-1
UDLD Topology	31-2
Fast UDLD Topology	31-2
Operation Modes	31-3
Default States for UDLD	31-3
Default UDLD Configuration	31-4
Configuring UDLD on the Switch	31-4
Fast UDLD Guidelines and Restrictions	31-4
Enabling UDLD Globally	31-5
Enabling UDLD on Individual Interfaces	31-6
Disabling UDLD on Individual Interfaces	31-7
Disabling UDLD on a Fiber-Optic Interface	31-7
Configuring a UDLD Probe Message Interval Globally	31-8
Configuring a Fast UDLD Probe Message Interval per Interface	31-8
Resetting Disabled LAN Interfaces	31-8
Displaying UDLD Link Status	31-9
<b>Configuring Unidirectional Ethernet</b>	<b>32-1</b>
About Unidirectional Ethernet	32-1
Configuring Unidirectional Ethernet	32-2

<b>Configuring Layer 3 Interfaces</b>	<b>33-1</b>
About Layer 3 Interfaces	33-1
Logical Layer 3 VLAN Interfaces	33-2
Physical Layer 3 Interfaces	33-2
Understanding SVI Autostate Exclude	33-3
Understanding Layer 3 Interface Counters	33-3
Configuration Guidelines	33-5
Configuring Logical Layer 3 VLAN Interfaces	33-6
Configuring VLANs as Layer 3 Interfaces	33-7
Configuring SVI Autostate Exclude	33-7
Configuring IP MTU Sizes	33-9
Configuring Layer 3 Interface Counters	33-10
Configuring Physical Layer 3 Interfaces	33-12
Configuring EIGRP Stub Routing	33-13
About EIGRP Stub Routing	33-13
Configuring EIGRP Stub Routing	33-14
Dual-Homed Remote Topology	33-15
EIGRP Stub Routing Configuration Tasks	33-18
Monitoring and Maintaining EIGRP	33-19
EIGRP Configuration Examples	33-19
Route Summarization Example	33-19
Route Authentication Example	33-20
Stub Routing Example	33-20
<b>Configuring Cisco Express Forwarding</b>	<b>34-1</b>
About CEF	34-1
CEF Features	34-1
Forwarding Information Base	34-2
Adjacency Tables	34-2
Adjacency Discovery	34-2
Adjacency Resolution	34-2
Adjacency Types That Require Special Handling	34-3
Unresolved Adjacency	34-3
Catalyst 4500 Series Switch Implementation of CEF	34-3
Hardware and Software Switching	34-4
Hardware Switching	34-5
Software Switching	34-5
Load Balancing	34-6
Software Interfaces	34-6

CEF Configuration Restrictions	34-6
Configuring CEF	34-6
Enabling CEF	34-6
Configuring Load Balancing for CEF	34-7
Configuring Per-Destination Load Balancing	34-7
Configuring Load Sharing Hash Function	34-7
Viewing CEF Information	34-8
Monitoring and Maintaining CEF	34-8
Displaying IP Statistics	34-8
<b>Configuring Unicast Reverse Path Forwarding</b>	<b>35-1</b>
About Unicast Reverse Path Forwarding	35-1
How Unicast RPF Works	35-2
Implementing Unicast RPF	35-4
Security Policy and Unicast RPF	35-5
Where to Use Unicast RPF	35-5
Routing Table Requirements	35-7
Where Not to Use Unicast RPF	35-7
Unicast RPF with BOOTP and DHCP	35-8
Restrictions	35-8
Limitation	35-8
Related Features and Technologies	35-8
Prerequisites to Configuring Unicast RPF	35-9
Unicast RPF Configuration Tasks	35-9
Configuring Unicast RPF	35-9
Verifying Unicast RPF	35-10
Monitoring and Maintaining Unicast RPF	35-11
Unicast RPF Configuration Example: Inbound and Outbound Filters	35-12
<b>Configuring IP Multicast</b>	<b>36-1</b>
About IP Multicast	36-1
IP Multicast Protocols	36-2
Internet Group Management Protocol	36-3
Protocol-Independent Multicast	36-3
Rendezvous Point (RP)	36-4
IGMP Snooping	36-4
IP Multicast Implementation on the Catalyst 4500 Series Switch	36-4
Restrictions on IP Multicast	36-5
CEF, MFIB, and Layer 2 Forwarding	36-6
IP Multicast Tables	36-7

Hardware and Software Forwarding	36-9
Non-Reverse Path Forwarding Traffic	36-10
Multicast Fast Drop	36-11
Multicast Forwarding Information Base	36-12
S/M, 224/4	36-13
Multicast HA	36-13
Configuring IP Multicast Routing	36-13
Default Configuration in IP Multicast Routing	36-13
Enabling IP Multicast Routing	36-14
Enabling PIM on an Interface	36-14
Enabling Dense Mode	36-15
Enabling Sparse Mode	36-15
Enabling Sparse-Dense Mode	36-15
Enabling Bidirectional Mode	36-16
Enabling PIM-SSM Mapping	36-17
Configuring a Rendezvous Point	36-17
Configuring Auto-RP	36-17
Configuring a Single Static RP	36-20
Load Splitting of IP Multicast Traffic	36-22
Monitoring and Maintaining IP Multicast Routing	36-23
Displaying System and Network Statistics	36-23
Displaying the Multicast Routing Table	36-24
Displaying IP MFIB	36-26
Displaying Bidirectional PIM Information	36-27
Displaying PIM Statistics	36-27
Clearing Tables and Databases	36-28
Configuration Examples	36-28
PIM Dense Mode Example	36-28
PIM Sparse Mode Example	36-29
Bidirectional PIM Mode Example	36-29
Sparse Mode with a Single Static RP Example	36-29
Sparse Mode with Auto-RP: Example	36-30
<b>Configuring ANCP Client</b>	<b>37-1</b>
About ANCP Client	37-1
Enabling and Configuring ANCP Client	37-2
Identifying a Port with the ANCP Protocol	37-2
Example 1	37-3
Example 2	37-4
Identifying a Port with DHCP Option 82	37-4

ANCP Guidelines and Restrictions 37-5

**Configuring Bidirection Forwarding Detection 38-1**

Finding Feature Information 38-1

Contents 38-1

Prerequisites for Bidirectional Forwarding Detection 38-2

Restrictions for Bidirectional Forwarding Detection 38-2

Information About Bidirectional Forwarding Detection 38-3

BFD Operation 38-3

Neighbor Relationships 38-3

BFD Detection of Failures 38-4

BFD Version Interoperability 38-5

BFD Session Limits 38-5

BFD Support for Nonbroadcast Media Interfaces 38-5

BFD Support for Nonstop Forwarding with Stateful Switchover 38-5

BFD Support for Stateful Switchover 38-6

BFD Support for Static Routing 38-6

Benefits of Using BFD for Failure Detection 38-7

Hardware Support for BFD 38-7

How to Configure Bidirectional Forwarding Detection 38-8

Configuring BFD Session Parameters on the Interface 38-8

Configuring BFD Support for Dynamic Routing Protocols 38-9

Configuring BFD Support for BGP 38-9

Configuring BFD Support for EIGRP 38-10

Configuring BFD Support for OSPF 38-11

Configuring BFD Support for Static Routing 38-13

Configuring BFD Echo Mode 38-15

Prerequisites 38-15

Restrictions 38-15

Configuring the BFD Slow Timer 38-16

Disabling BFD Echo Mode Without Asymmetry 38-16

Monitoring and Troubleshooting BFD 38-17

Configuration Examples for Bidirectional Forwarding Detection 38-17

Example: Configuring BFD in an EIGRP Network with Echo Mode Enabled by Default 38-17

Example: Configuring BFD in an OSPF Network 38-22

Example: Configuring BFD Hardware-Offload support in a BGP Network Network 38-25

Example: Configuring BFD Support for Static Routing 38-27

Additional References 38-28

Related Documents 38-28

Standards	38-28
MIBs	38-29
RFCs	38-29
Technical Assistance	38-29
<b>Configuring Policy-Based Routing</b>	<b>39-1</b>
About Policy-Based Routing	39-1
About PBR	39-2
Understanding Route-Maps	39-2
Using Policy-Based Routing	39-5
Policy-Based Routing Configuration Tasks	39-6
Enabling IPv4 PBR	39-6
Enabling IPv6 PBR	39-9
Enabling Local PBR	39-11
IPv4	39-11
IPv6	39-11
Examples of the show Command	39-11
Unsupported Commands	39-12
Policy-Based Routing Configuration Examples	39-12
Equal Access	39-12
Differing Next Hops	39-13
Deny ACE	39-13
<b>Configuring VRF-lite</b>	<b>40-1</b>
About VRF-lite	40-2
VRF-lite Configuration Guidelines	40-3
Configuring VRF-lite for IPv4	40-5
Configuring VRFs	40-5
Configuring VRF-Aware Services	40-6
Configuring the User Interface for ARP	40-6
Configuring Per-VRF for TACACS+ Servers	40-6
Configuring Multicast VRFs	40-7
Configuring a VPN Routing Session	40-8
Configuring BGP PE to CE Routing Sessions	40-9
VRF-lite Configuration Example	40-10
Configuring Switch S8	40-11
Configuring Switch S20	40-12
Configuring Switch S11	40-12
Configuring the PE Switch S3	40-13
Displaying VRF-lite Status	40-14

- Configuring VRF-lite for IPv6 40-15
  - Configuring VRF-Aware Services 40-15
    - Configuring the User Interface for ARP 40-15
    - Configuring the User Interface for PING 40-15
    - Configuring the User Interface for uRPF 40-16
    - Configuring the User Interface for Traceroute 40-16
    - Configuring the User Interface for FTP and TFTP 40-16
    - Configuring the User Interface for Telnet and SSH 40-17
    - Configuring the User Interface for NTP 40-17
  - VRF-lite Configuration Example 40-17
  - Displaying VRF-lite Status 40-21
  - Configuring IPv6 VRF-lite 40-22
    - Configure VRFs 40-23
    - Associate Interfaces to the Defined VRFs 40-24
    - Populate VRF with Routes via Routing Protocols 40-24
    - Static Route 40-24
    - Routing Protocols 40-25
- VPN Co-existence Between IPv4 and IPv6 40-28
- Migrating from the Old to New CLI Scheme 40-28

**Configuring Quality of Service 41-1**

- Overview of QoS 41-1
  - Prioritization 41-2
  - QoS Terminology 41-3
  - Basic QoS Model 41-5
  - Classification 41-6
    - Classification Based on QoS ACLs 41-6
    - Classification Based on Class Maps and Policy Maps 41-7
  - Policing and Marking 41-8
  - Queueing and Scheduling 41-8
    - Active Queue Management 41-9
    - Sharing Link Bandwidth Among Transmit Queues 41-9
    - Strict Priority / Low Latency Queueing 41-9
    - Traffic Shaping 41-9
  - Packet Modification 41-9
  - Per Port Per VLAN QoS 41-10
  - Flow-based QoS 41-10
  - Using Metadata in QoS Policy 41-11
  - Configuring System Queue Limit 41-12
- Configuring VSS QoS 41-13



MQoS-based QoS Configuration	41-13	
Platform-supported Classification Criteria and QoS Features		41-14
Platform Hardware Capabilities	41-15	
Prerequisites for Applying a QoS Service Policy	41-15	
Restrictions for Applying a QoS Service Policy	41-15	
Classification	41-16	
Classification Statistics	41-16	
Configuring a Policy Map	41-16	
Attaching a Policy Map to an Interface	41-17	
Policing	41-17	
How to Implement Policing	41-18	
Platform Restrictions	41-18	
Marking Network Traffic	41-18	
Contents	41-18	
Information About Marking Network Traffic	41-19	
Marking Action Drivers	41-21	
Traffic Marking Procedure Flowchart	41-21	
Restrictions for Marking Network Traffic	41-22	
Multi-attribute Marking Support	41-22	
Hardware Capabilities for Marking	41-23	
Configuring the Policy Map Marking Action	41-23	
Marking Statistics	41-24	
Shaping, Sharing (Bandwidth), Priority Queuing, Queue-limiting and DBL		41-25
Shaping	41-25	
Sharing(bandwidth)	41-27	
Priority queuing	41-30	
Queue-limiting	41-31	
Active Queue Management (AQM) via Dynamic Buffer Limiting (DBL)		41-34
Transmit Queue Statistics	41-35	
Enabling Per-Port Per-VLAN QoS	41-36	
Policy Associations	41-39	
Software QoS	41-40	
Applying Flow-based QoS Policy	41-41	
Examples	41-42	
Configuration Guidelines	41-44	
Configuring CoS Mutation	41-45	
Configuring System Queue Limit	41-46	
Configuring QoS on a Standalone Supervisor Engine 6-E/6L-E or Supervisor Engine 7-E/7L-E		41-47
MQoS-based QoS Configuration	41-48	
Platform-supported Classification Criteria and QoS Features	41-48	

Platform Hardware Capabilities	41-49
Prerequisites for Applying a QoS Service Policy	41-49
Restrictions for Applying a QoS Service Policy	41-50
Classification	41-50
Classification Statistics	41-50
Configuring a Policy Map	41-50
Attaching a Policy Map to an Interface	41-51
Policing	41-51
How to Implement Policing	41-52
Platform Restrictions	41-52
Marking Network Traffic	41-52
Contents	41-53
Information About Marking Network Traffic	41-53
Marking Action Drivers	41-55
Traffic Marking Procedure Flowchart	41-55
Restrictions for Marking Network Traffic	41-56
Multi-attribute Marking Support	41-56
Hardware Capabilities for Marking	41-57
Configuring the Policy Map Marking Action	41-57
Marking Statistics	41-59
Shaping, Sharing (Bandwidth), Priority Queuing, Queue-limiting and DBL	41-59
Shaping	41-59
Sharing(bandwidth)	41-61
Priority queuing	41-64
Queue-limiting	41-65
Active Queue Management (AQM) via Dynamic Buffer Limiting (DBL)	41-68
Transmit Queue Statistics	41-69
Enabling Per-Port Per-VLAN QoS	41-70
Policy Associations	41-73
Software QoS	41-74
Applying Flow-based QoS Policy	41-75
Examples	41-76
Configuration Guidelines	41-78
Configuring CoS Mutation	41-79
Configuring System Queue Limit	41-80
Configuring VSS Auto-QoS	41-81
Configuring Auto-QoS on a Standalone Supervisor Engine 6-E/6L-E or Supervisor Engine 7-E/7L-E	41-86
<b>Configuring Voice Interfaces</b>	<b>42-1</b>
About Voice Interfaces	42-1

Cisco IP Phone Voice Traffic	42-2
Cisco IP Phone Data Traffic	42-2
Configuring a Port to Connect to a Cisco 7960 IP Phone	42-3
Configuring Voice Ports for Voice and Data Traffic	42-3
Overriding the CoS Priority of Incoming Frames	42-5
Configuring Power	42-5
<b>Configuring Private VLANs</b>	<b>43-1</b>
About Private VLANs	43-1
Purpose of a PVLAN	43-2
PVLAN Terminology	43-3
PVLANS across Multiple Switches	43-5
Standard Trunk Ports	43-5
Isolated PVLAN Trunk Ports	43-6
Promiscuous PVLAN Trunk Ports	43-7
PVLAN Modes Over Gigabit Etherchannel	43-8
Private-VLAN Interaction with Other Features	43-8
PVLANS and VLAN ACL/QoS	43-8
PVLANS and Unicast, Broadcast, and Multicast Traffic	43-9
PVLANS and SVIs	43-10
Per-Virtual Port Error-Disable on PVLANS	43-10
PVLAN Commands	43-10
Configuring PVLANS	43-11
Basic PVLAN Configuration Procedure	43-12
Default Private-VLAN Configuration	43-12
PVLAN Configuration Guidelines and Restrictions	43-12
Configuring a VLAN as a PVLAN	43-15
Associating a Secondary VLAN with a Primary VLAN	43-16
Configuring a Layer 2 Interface as a PVLAN Promiscuous Port	43-17
Configuring a Layer 2 Interface as a PVLAN Host Port	43-18
Configuring a Layer 2 Interface as an Isolated PVLAN Trunk Port	43-19
Configuring a Layer 2 Interface as a Promiscuous PVLAN Trunk Port	43-21
Permitting Routing of Secondary VLAN Ingress Traffic	43-23
Configuring PVLAN over EtherChannel	43-24
Configuring a Layer 2 EtherChannel	43-24
Configuring a Layer 2 Etherchannel as a PVLAN Promiscuous Port	43-24
Configuring a Layer 2 EtherChannel as a PVLAN Host Port	43-26
Configuring a Layer 2 EtherChannel as an Isolated PVLAN Trunk Port	43-27
Configuring a Layer 2 Etherchannel as a Promiscuous PVLAN Trunk Port	43-28

<b>Configuring MACsec Encryption</b>	<b>44-1</b>
Understanding Media Access Control Security and MACsec Key Agreement	44-2
MKA Policies	44-2
Virtual Ports	44-3
MACsec	44-3
MACsec, MKA, and 802.1X Host Modes	44-3
Single-Host Mode	44-4
Multiple-Host Mode	44-4
MKA Statistics	44-4
Configuring MACsec and MACsec Key Agreement	44-6
Default MACsec MACsec Key Agreement Configuration	44-6
Configuring an MKA Policy	44-6
Configuring MACsec on an Interface	44-7
Understanding Cisco TrustSec MACsec	44-8
Configuring Cisco TrustSec MACsec	44-10
Configuring Cisco TrustSec Credentials on the Switch	44-10
Configuring Cisco TrustSec Switch-to-Switch Link Security in 802.1X Mode	44-11
Configuring Cisco TrustSec Switch-to-Switch Link Security in Manual Mode	44-12
Cisco TrustSec Switch-to-Switch Link Security Configuration Example	44-14
<b>Configuring 802.1X Port-Based Authentication</b>	<b>45-1</b>
About 802.1X Port-Based Authentication	45-1
Device Roles	45-2
802.1X and Network Access Control	45-3
Authentication Initiation and Message Exchange	45-4
Ports in Authorized and Unauthorized States	45-5
802.1X Host Mode	45-6
Single-Host Mode	45-7
Multiple-Hosts Mode	45-7
Multidomain Authentication Mode	45-7
Multiauthentication Mode	45-8
Pre-authentication Open Access	45-8
802.1X Violation Mode	45-8
Using MAC Move	45-9
Using MAC Replace	45-9
Using 802.1X with VLAN Assignment	45-10
Using 802.1X for Guest VLANs	45-11
Usage Guidelines for Using 802.1X Authentication with Guest VLANs	45-11

- Usage Guidelines for Using 802.1X Authentication with Guest VLANs on Windows-XP Hosts **45-12**
- Using 802.1X with MAC Authentication Bypass **45-12**
  - Feature Interaction **45-13**
- Using 802.1X with Web-Based Authentication **45-14**
- Using 802.1X with Inaccessible Authentication Bypass **45-14**
- Using 802.1X with Unidirectional Controlled Port **45-15**
  - Unidirectional State **45-16**
  - Bidirectional State **45-16**
- Using 802.1X with VLAN User Distribution **45-16**
  - Deployment Example **45-17**
- Using 802.1X with Authentication Failed VLAN Assignment **45-17**
  - Usage Guidelines for Using Authentication Failed VLAN Assignment **45-18**
- Using 802.1X with Port Security **45-19**
- Using 802.1X Authentication with ACL Assignments and Redirect URLs **45-20**
  - Cisco Secure ACS and AV Pairs for URL-Redirect **45-20**
  - ACLs **45-21**
- Using 802.1X with RADIUS-Provided Session Timeouts **45-21**
- Using 802.1X with Voice VLAN Ports **45-22**
- Using Voice Aware 802.1x Security **45-22**
- Using Multiple Domain Authentication and Multiple Authentication **45-23**
- 802.1X Supplicant and Authenticator Switches with Network Edge Access Topology **45-24**
  - Deployment **45-24**
- How 802.1X Fails on a Port **45-25**
- Supported Topologies **45-26**
- Configuring 802.1X Port-Based Authentication **45-26**
  - Default 802.1X Configuration **45-27**
  - 802.1X Configuration Guidelines **45-29**
  - Enabling 802.1X Authentication **45-29**
  - Configuring Switch-to-RADIUS-Server Communication **45-32**
  - Configuring Multiple Domain Authentication and Multiple Authorization **45-34**
  - Configuring 802.1X Authentication with ACL Assignments and Redirect URLs **45-38**
    - Downloadable ACL **45-38**
    - URL-Redirect **45-41**
    - Configuring a Downloadable Policy **45-44**
  - Configuring 802.1X Authentication with Per-User ACL and Filter-ID ACL **45-45**
    - Per-User ACL and Filter-ID ACL **45-45**
    - Configuring a Per-User ACL and Filter-ID ACL **45-52**
  - Configuring RADIUS-Provided Session Timeouts **45-53**
  - Configuring MAC Move **45-55**

- Configuring MAC Replace **45-55**
- Configuring Violation Action **45-56**
- Configuring 802.1X with Guest VLANs **45-57**
- Configuring 802.1X with MAC Authentication Bypass **45-60**
- Configuring 802.1X with Inaccessible Authentication Bypass **45-62**
- Configuring 802.1X with Unidirectional Controlled Port **45-66**
- Configuring 802.1X with VLAN User Distribution **45-68**
  - Configuring the Switch **45-68**
  - ACS Configuration **45-69**
- Configuring 802.1X with Authentication Failed **45-70**
- Configuring 802.1X with Voice VLAN **45-72**
- Configuring Voice Aware 802.1x Security **45-73**
- Configuring 802.1X with VLAN Assignment **45-75**
  - Cisco ACS Configuration for VLAN Assignment **45-76**
- Enabling Fallback Authentication **45-77**
- Enabling Periodic Reauthentication **45-81**
- Enabling Multiple Hosts **45-83**
- Changing the Quiet Period **45-84**
- Changing the Switch-to-Client Retransmission Time **45-85**
- Setting the Switch-to-Client Frame-Retransmission Number **45-86**
- Configuring an Authenticator and a Supplicant Switch with NEAT **45-88**
  - Configuring Switch as an Authenticator **45-88**
  - Cisco AV Pair Configuration **45-89**
  - Configuring Switch as a Supplicant **45-92**
  - Configuring NEAT with ASP **45-93**
  - Configuration Guidelines **45-93**
- Manually Reauthenticating a Client Connected to a Port **45-94**
- Initializing the 802.1X Authentication State **45-94**
- Removing 802.1X Client Information **45-95**
- Resetting the 802.1X Configuration to the Default Values **45-95**
- Controlling Switch Access with RADIUS **45-95**
  - Understanding RADIUS **45-96**
  - RADIUS Operation **45-97**
  - RADIUS Change of Authorization **45-97**
    - Overview **45-98**
    - Change-of-Authorization Requests **45-98**
    - CoA Request Response Code **45-99**
    - CoA Request Commands **45-100**
- Configuring RADIUS **45-103**
  - Default RADIUS Configuration **45-103**

Identifying the RADIUS Server Host	45-103
Configuring RADIUS Login Authentication	45-106
Defining AAA Server Groups	45-108
Configuring RADIUS Authorization for User Privileged Access and Network Services	45-110
Starting RADIUS Accounting	45-111
Configuring Settings for All RADIUS Servers	45-112
Configuring the Switch to Use Vendor-Specific RADIUS Attributes	45-112
Configuring the Switch for Vendor-Proprietary RADIUS Server Communication	45-114
Configuring CoA on the Switch	45-115
Monitoring and Troubleshooting CoA Functionality	45-116
Configuring RADIUS Server Load Balancing	45-116
Displaying the RADIUS Configuration	45-116
Configuring Device Sensor	45-116
About Device Sensor	45-117
MSP-IOS Sensor Device Classifier Interaction	45-118
Configuring Device Sensor	45-118
Enabling MSP	45-119
Enabling Accounting Augmentation	45-119
Creating a Cisco Discovery Protocol Filter	45-120
Creating an LLDP Filter	45-120
Creating a DHCP Filter	45-121
Applying a Protocol Filter to the Device Sensor Output	45-121
Tracking TLV Changes	45-122
Verifying the Device Sensor Configuration	45-123
Troubleshooting Commands	45-124
Restrictions for Device Sensor	45-124
Configuration Examples for the Device Sensor Feature	45-124
Displaying 802.1X Statistics and Status	45-125
Displaying Authentication Details	45-125
Determining the Authentication Methods Registered with the Auth Manager	45-125
Displaying the Auth Manager Summary for an Interface	45-126
Displaying the Summary of All Auth Manager Sessions on the Switch	45-126
Displaying a Summary of All Auth Manager Sessions on the Switch Authorized for a Specified Authentication Method	45-126
Verifying the Auth Manager Session for an Interface	45-126
Displaying MAB Details	45-128
EPM Logging	45-129
Cisco IOS Security Features	45-130

**Configuring the PPPoE Intermediate Agent 46-1**

Related Documents 46-2

RFCs 46-2

About PPPoE Intermediate Agent 46-2

Enabling PPPoE IA on a Switch 46-2

Configuring the Access Node Identifier for PPPoE IA on a Switch 46-2

Configuring the Identifier String, Option, and Delimiter for PPPoE IA on an Switch 46-3

Configuring the Generic Error Message for PPPoE IA on an Switch 46-3

Enabling PPPoE IA on an Interface 46-4

Configuring the PPPoE IA Trust Setting on an Interface 46-4

Configuring PPPoE IA Rate Limiting Setting on an Interface 46-4

Configuring PPPoE IA Vendor-tag Stripping on an Interface 46-5

Configuring PPPoE IA Circuit-ID and Remote-ID on an Interface 46-5

Enabling PPPoE IA for a Specific VLAN on an Interface 46-5

Configuring PPPoE IA Circuit-ID and Remote-ID for a VLAN on an Interface 46-6

Displaying Configuration Parameters 46-6

Clearing Packet Counters 46-8

Debugging PPPoE Intermediate Agent 46-8

Troubleshooting Tips 46-9

**Configuring Web-Based Authentication 47-1**

About Web-Based Authentication 47-1

Device Roles 47-2

Host Detection 47-2

Session Creation 47-3

Authentication Process 47-3

Customization of the Authentication Proxy Web Pages 47-4

Web-Based Authentication Interactions with Other Features 47-4

Port Security 47-4

LAN Port IP 47-5

Gateway IP 47-5

ACLs 47-5

Context-Based Access Control 47-5

802.1X Authentication 47-5

EtherChannel 47-5

Switchover 47-5

Configuring Web-Based Authentication 47-6

Default Web-Based Authentication Configuration 47-6

Web-Based Authentication Configuration Guidelines and Restrictions 47-6



Web-Based Authentication Configuration Task List	47-7
Configuring the Authentication Rule and Interfaces	47-7
Configuring AAA Authentication	47-9
Configuring Switch-to-RADIUS-Server Communication	47-9
Configuring the HTTP Server	47-11
Customizing the Authentication Proxy Web Pages	47-11
Specifying a Redirection URL for Successful Login	47-12
Configuring the Web-Based Authentication Parameters	47-13
Removing Web-Based Authentication Cache Entries	47-14
Displaying Web-Based Authentication Status	47-14
<b>Configuring Port Security</b>	<b>48-1</b>
Port Security Commands	48-2
About Port Security	48-3
Secure MAC Addresses	48-4
Maximum Number of Secure MAC Addresses	48-4
Aging Secure MAC Addresses	48-5
Sticky Addresses on a Port	48-5
Violation Actions	48-6
Invalid Packet Handling	48-7
Configuring Port Security on Access Ports	48-7
Configuring Port Security on Access Ports	48-7
Examples of Port Security on Access Ports	48-10
Example 1: Setting Maximum Number of Secure Addresses	48-11
Example 2: Setting a Violation Mode	48-11
Example 3: Setting the Aging Timer	48-11
Example 4: Setting the Aging Timer Type	48-12
Example 5: Configuring a Secure MAC Address	48-12
Example 6: Configuring Sticky Port Security	48-13
Example 7: Setting a Rate Limit for Bad Packets	48-13
Example 8: Clearing Dynamic Secure MAC Addresses	48-14
Configuring Port Security on PVLAN Ports	48-14
Configuring Port Security on an Isolated Private VLAN Host Port	48-14
Example of Port Security on an Isolated Private VLAN Host Port	48-16
Configuring Port Security on a Private VLAN Promiscuous Port	48-16
Example of Port Security on a Private VLAN Promiscuous Port	48-17
Configuring Port Security on Trunk Ports	48-17
Configuring Trunk Port Security	48-17
Examples of Trunk Port Security	48-19

Example 1: Configuring a Maximum Limit of Secure MAC Addresses for All VLANs	48-19
Example 2: Configuring a Maximum Limit of Secure MAC Addresses for Specific VLANs	48-20
Example 3: Configuring Secure MAC Addresses in a VLAN Range	48-20
Trunk Port Security Configuration Guidelines and Restrictions	48-21
Port Mode Changes	48-22
Configuring Port Security on Voice Ports	48-22
Configuring Port Security on Voice Ports	48-23
Examples of Voice Port Security	48-25
Example 1: Configuring Maximum MAC Addresses for Voice and Data VLANs	48-25
Example 2: Configuring Sticky MAC Addresses for Voice and Data VLANs	48-26
Voice Port Security Configuration Guidelines and Restrictions	48-27
Displaying Port Security Settings	48-27
Examples of Security Settings	48-28
Example 1: Displaying Security Settings for the Entire Switch	48-28
Example 2: Displaying Security Settings for an Interface	48-29
Example 3: Displaying All Secure Addresses for the Entire Switch	48-29
Example 4: Displaying a Maximum Number of MAC Addresses on an Interface	48-30
Example 5: Displaying Security Settings on an Interface for a VLAN Range	48-30
Example 6: Displaying Secured MAC Addresses and Aging Information on an Interface	48-30
Example 7: Displaying Secured MAC Addresses for a VLAN Range on an Interface	48-31
Configuring Port Security with Other Features/Environments	48-31
DHCP and IP Source Guard	48-31
802.1X Authentication	48-32
Configuring Port Security in a Wireless Environment	48-32
Port Security Configuration Guidelines and Restrictions	48-33
<b>Configuring Control Plane Policing and Layer 2 Control Packet QoS</b>	<b>49-1</b>
Configuring Control Plane Policing	49-2
About Control Plane Policing	49-2
General Guidelines for Control Plane Policing	49-3
Default Configuration	49-4
Configuring CoPP for Control Plane Traffic	49-4
Configuring CoPP for Data Plane and Management Plane Traffic	49-5
Control Plane Policing Configuration Guidelines and Restrictions	49-8
All supervisor engines	49-8
Do not apply to Catalyst 4900M, Catalyst 4948E, Supervisor Engine 6-E, and Supervisor Engine 6L-E	49-8
Monitoring CoPP	49-9
Configuring Layer 2 Control Packet QoS	49-11
Understanding Layer 2 Control Packet QoS	49-11

Default Configuration	49-11
Enabling Layer 2 Control Packet QoS	49-12
Disabling Layer 2 Control Packet QoS	49-13
Layer 2 Control Packet QoS Configuration Examples	49-14
Layer 2 Control Packet QoS Guidelines and Restrictions	49-16
Policing IPv6 Control Traffic	49-16
<b>Configuring Dynamic ARP Inspection</b>	<b>50-1</b>
About Dynamic ARP Inspection	50-1
ARP Cache Poisoning	50-2
Purpose of Dynamic ARP Inspection	50-2
Interface Trust State, Security Coverage and Network Configuration	50-3
Relative Priority of Static Bindings and DHCP Snooping Entries	50-4
Logging of Dropped Packets	50-4
Rate Limiting of ARP Packets	50-4
Port Channels Function	50-5
Configuring Dynamic ARP Inspection	50-5
Configuring Dynamic ARP Inspection in DHCP Environments	50-5
DAI Configuration Example	50-7
Switch A	50-7
Switch B	50-9
Configuring ARP ACLs for Non-DHCP Environments	50-11
Configuring the Log Buffer	50-14
Limiting the Rate of Incoming ARP Packets	50-16
Performing Validation Checks	50-19
<b>Configuring DHCP Snooping, IP Source Guard, and IPSG for Static Hosts</b>	<b>51-1</b>
About DHCP Snooping	51-1
Trusted and Untrusted Sources	51-2
About the DHCP Snooping Database Agent	51-2
Option 82 Data Insertion	51-4
Configuring DHCP Snooping	51-6
Default Configuration for DHCP Snooping	51-7
Enabling DHCP Snooping	51-7
Enabling DHCP Snooping on the Aggregation Switch	51-9
Enabling DHCP Snooping and Option 82	51-10
Enabling DHCP Snooping on Private VLAN	51-12
Configuring DHCP Snooping on Private VLAN	51-12
Configuring DHCP Snooping with an Ethernet Channel Group	51-12
Enabling the DHCP Snooping Database Agent	51-13

Limiting the Rate of Incoming DHCP Packets	51-13
Configuration Examples for the Database Agent	51-15
Example 1: Enabling the Database Agent	51-15
Example 2: Reading Binding Entries from a TFTP File	51-17
Example 3: Adding Information to the DHCP Snooping Database	51-18
Displaying DHCP Snooping Information	51-18
Displaying a Binding Table	51-19
Displaying the DHCP Snooping Configuration	51-19
About IP Source Guard	51-19
Configuring IP Source Guard	51-20
Configuring IP Source Guard on Private VLANs	51-22
Displaying IP Source Guard Information	51-22
Displaying IP Source Binding Information	51-23
Configuring IP Source Guard for Static Hosts	51-24
About IP Source Guard for Static Hosts	51-24
Configuring IPSG for Static Hosts on a Layer 2 Access Port	51-25
Configuring IPSG for Static Hosts on a PVLAN Host Port	51-28
<b>Configuring Network Security with ACLs</b>	<b>52-1</b>
About ACLs	52-2
Overview	52-2
Supported Features That Use ACLs	52-3
Router ACLs	52-3
Port ACLs	52-4
Dynamic ACLs	52-5
VLAN Maps	52-5
Hardware and Software ACL Support	52-6
Troubleshooting High CPU Due to ACLs	52-6
Selecting Mode of Capturing Control Packets	52-7
Guidelines and Restrictions	52-8
Selecting Control Packet Capture	52-8
TCAM Programming and ACLs	52-10
Layer 4 Operators in ACLs	52-10
Restrictions for Layer 4 Operations	52-10
Configuration Guidelines for Layer 4 Operations	52-11
How ACL Processing Impacts CPU	52-12
Configuring Unicast MAC Address Filtering	52-13
Configuring Named MAC Extended ACLs	52-14

Configuring EtherType Matching	52-15
Configuring Named IPv6 ACLs	52-16
Applying IPv6 ACLs to Layer 2 and 3 Interface	52-17
Configuring VLAN Maps	52-17
VLAN Map Configuration Guidelines	52-18
Creating and Deleting VLAN Maps	52-19
Examples of ACLs and VLAN Maps	52-19
Applying a VLAN Map to a VLAN	52-21
Using VLAN Maps in Your Network	52-22
Denying Access to a Server on Another VLAN	52-23
Displaying VLAN Access Map Information	52-24
Using VLAN Maps with Router ACLs	52-25
Guidelines for Using Router ACLs and VLAN Maps on the Same VLAN	52-25
Examples of Router ACLs and VLAN Maps Applied to VLANs	52-25
ACLs and Switched Packets	52-25
ACLs and Routed Packets	52-26
Configuring PACLs	52-27
Creating a PACL	52-27
PACL Configuration Guidelines	52-28
Removing the Requirement for a Port ACL	52-28
Configuration Restrictions	52-29
Debugging Considerations	52-29
Webauth Fallback	52-29
Configuring IPv4, IPv6, and MAC ACLs on a Layer 2 Interface	52-29
Using PACL with Access-Group Mode	52-30
Configuring Access-group Mode on Layer 2 Interface	52-31
Applying ACLs to a Layer 2 Interface	52-31
Displaying an ACL Configuration on a Layer 2 Interface	52-32
Using PACL with VLAN Maps and Router ACLs	52-32
Configuring RA Guard	52-35
Introduction	52-35
Deployment	52-36
Configuring RA Guard	52-36
Examples	52-37
Usage Guidelines	52-38
<b>Support for IPv6</b>	<b>53-1</b>
Finding Feature Information	53-1
About IPv6	53-1

IPv6 Addressing and Basic Connectivity	53-2
DHCP	53-3
Security	53-3
QoS	53-3
Management	53-4
Multicast	53-4
Static Routes	53-5
First-Hop Redundancy Protocols	53-5
Unicast Routing	53-5
RIP	53-5
OSPF	53-6
EIGRP	53-6
IS-IS	53-6
Multiprotocol BGP	53-6
Tunneling	53-7
IPv6 Default States	53-7
<b>Port Unicast and Multicast Flood Blocking</b>	<b>54-1</b>
About Flood Blocking	54-1
Configuring Port Blocking	54-1
Blocking Flooded Traffic on an Interface	54-2
Resuming Normal Forwarding on a Port	54-3
<b>Configuring Storm Control</b>	<b>55-1</b>
About Storm Control	55-1
Hardware-Based Storm Control Implementation	55-2
Software-Based Storm Control Implementation	55-2
Enabling Broadcast Storm Control	55-3
Enabling Multicast Storm Control	55-4
Disabling Broadcast Storm Control	55-5
Disabling Multicast Storm Control	55-5
Displaying Storm Control	55-6
<b>Configuring SPAN and RSPAN</b>	<b>56-1</b>
About SPAN and RSPAN	56-1
SPAN and RSPAN Concepts and Terminology	56-3
SPAN Session	56-3
Traffic Types	56-3
Source Port	56-4
Destination Port	56-5

VLAN-Based SPAN	56-5
SPAN Traffic	56-6
SPAN and RSPAN Session Limits	56-6
Default SPAN and RSPAN Configuration	56-6
Configuring SPAN	56-7
SPAN Configuration Guidelines and Restrictions	56-7
Configuring SPAN Sources	56-8
Configuring SPAN Destinations	56-9
Monitoring Source VLANs on a Trunk Interface	56-9
Configuration Scenario	56-10
Verifying a SPAN Configuration	56-10
CPU Port Sniffing	56-10
Encapsulation Configuration	56-12
Ingress Packets	56-12
Access List Filtering	56-13
ACL Configuration Guidelines	56-13
Configuring Access List Filtering	56-14
Packet Type Filtering	56-14
Configuration Example	56-15
Configuring RSPAN	56-16
RSPAN Configuration Guidelines	56-16
Creating an RSPAN Session	56-17
Creating an RSPAN Destination Session	56-18
Creating an RSPAN Destination Session and Enabling Ingress Traffic	56-19
Removing Ports from an RSPAN Session	56-20
Specifying VLANs to Monitor	56-21
Specifying VLANs to Filter	56-23
Displaying SPAN and RSPAN Status	56-24
<b>Configuring Wireshark</b>	<b>57-1</b>
Finding Feature Information	57-1
Prerequisites for Wireshark	57-2
Guidelines for Wireshark	57-2
Restrictions for Wireshark	57-4
Information about Wireshark	57-5
Capture Points	57-6
Attachment Points	57-6
Filters	57-6

- Core System Filter **57-6**
- Capture Filter **57-7**
- Display Filter **57-7**
- Input and Output Classification **57-7**
- Actions **57-8**
- Storing Captured Packets to Buffer in Memory **57-8**
  - Storing Captured Packets to a .pcap File **57-8**
- Decoding and Displaying Packets **57-9**
  - Displaying Live Traffic **57-9**
  - Displaying from the .pcap File **57-9**
  - Storing and Displaying Packets **57-9**
- Activating and Deactivating Wireshark Capture Points **57-9**
- Wireshark Features used in Switches **57-10**
- Wireshark on VSS **57-11**
- How to Configure Wireshark **57-11**
  - Default Wireshark Configuration **57-11**
  - Defining, Modifying, or Deleting a Capture Point **57-12**
    - Examples **57-13**
  - Activating and Deactivating a Capture Point **57-13**
  - Configuring Wireshark on VSS **57-14**
- Monitoring Wireshark **57-14**
- Configuration Examples for Wireshark **57-14**
  - Example: Displaying a Brief Output from a .pcap File **57-14**
  - Example: Displaying Detailed Output from a .pcap File **57-15**
  - Example: Displaying a Hexadecimal Dump Output from a .pcap File **57-17**
  - Example: Displaying Packets from a .pcap File with a Display Filter **57-18**
- Usage Examples for Wireshark **57-18**
  - Example: Simple Capture and Display **57-18**
  - Example: Simple Capture and Store **57-19**
  - Example: Using Buffer Capture **57-20**
  - Example: Capture Sessions **57-24**
  - Example: Capture and Store in Lock-step Mode **57-28**
  - Example: Simple Capture and Store in Lock-step with High-speed Mode **57-29**
  - Example: Simple Capture and Store of Packets in Egress Direction **57-30**
- VSS Specific Examples **57-31**
  - Example: Capturing and Storing in a file (Attachment Point in VSS Active Switch) **57-31**
  - Example: Capturing and Storing in a File with Display (Attachment Point in VSS Active Switch) **57-32**
  - Example: Capturing and Storing in a File (Attachment point in VSS Standby Switch) **57-32**



Example: Capturing and Storing in a File with Display (Attachment Point in VSS Standby Switch) **57-33**

Example: Circular Buffer Usage (Attachment Point in VSS Standby Switch) **57-35**

## **Configuring Enhanced Object Tracking 58-1**

Understanding Enhanced Object Tracking **58-1**

Configuring Enhanced Object Tracking Features **58-2**

Default Configuration **58-2**

Tracking Interface Line-Protocol or IP Routing State **58-2**

Configuring a Tracked List **58-3**

Configuring a Tracked List with a Boolean Expression **58-4**

Configuring a Tracked List with a Weight Threshold **58-5**

Configuring a Tracked List with a Percentage Threshold **58-6**

Configuring HSRP Object Tracking **58-7**

Configuring Other Tracking Characteristics **58-8**

Configuring IP SLAs Object Tracking **58-8**

Configuring Static Routing Support **58-10**

Configuring a Primary Interface **58-10**

Configuring a Cisco IP SLAs Monitoring Agent and Track Object **58-11**

Configuring a Routing Policy and Default Route **58-11**

Monitoring Enhanced Object Tracking **58-12**

## **Configuring System Message Logging 59-1**

About System Message Logging **59-1**

Configuring System Message Logging **59-2**

System Log Message Format **59-2**

Default System Message Logging Configuration **59-3**

Disabling Message Logging **59-4**

Setting the Message Display Destination Device **59-5**

Synchronizing Log Messages **59-6**

Enabling and Disabling Timestamps on Log Messages **59-7**

Enabling and Disabling Sequence Numbers in Log Messages (Optional) **59-7**

Defining the Message Severity Level (Optional) **59-8**

Limiting Syslog Messages Sent to the History Table and to SNMP (Optional) **59-9**

Configuring UNIX Syslog Servers **59-10**

Logging Messages to a UNIX Syslog Daemon **59-10**

Configuring the UNIX System Logging Facility **59-11**

Displaying the Logging Configuration **59-12**

<b>Onboard Failure Logging (OBFL)</b>	<b>60-1</b>
Prerequisites for OBFL	60-1
Restrictions for OBFL	60-2
Information About OBFL	60-2
Overview of OBFL	60-2
Information about Data Collected by OBFL	60-2
OBFL Data Overview	60-2
Temperature	60-3
Operational Uptime	60-4
Interrupts	60-6
Message Logging	60-7
Default Settings for OBFL	60-8
Enabling OBFL	60-8
Configuration Examples for OBFL	60-9
Enabling OBFL Message Logging: Example	60-9
OBFL Message Log: Example	60-9
OBFL Component Uptime Report: Example	60-10
OBFL Report for a Specific Time: Example	60-10
<b>Configuring SNMP</b>	<b>61-1</b>
About SNMP	61-1
SNMP Versions	61-2
SNMP Manager Functions	61-3
SNMP Agent Functions	61-4
SNMP Community Strings	61-4
Using SNMP to Access MIB Variables	61-4
SNMP Notifications	61-5
Configuring SNMP	61-5
Default SNMP Configuration	61-5
SNMP Configuration Guidelines	61-6
Disabling the SNMP Agent	61-7
Configuring Community Strings	61-7
Configuring SNMP Groups and Users	61-9
Configuring SNMP Notifications	61-11
Setting the Agent Contact and Location Information	61-14
Limiting TFTP Servers Used Through SNMP	61-15
SNMP Examples	61-15
Displaying SNMP Status	61-16

<b>Configuring NetFlow-lite</b>	<b>62-1</b>
About NetFlow Packet Sampling	62-2
Feature Interaction	62-2
System-wide Restrictions	62-2
Interface-level Restrictions	62-2
Monitor-level Restrictions	62-2
Configuring NetFlow Packet Sampling	62-2
Configuring Information about the External Collector	62-3
Example	62-3
Usage Guidelines	62-4
Configuring Sampling Parameters	62-4
Example	62-5
Usage Guidelines	62-5
Activating Sampling on an Interface or VLAN	62-5
Examples	62-6
Usage Guidelines	62-7
Display Commands	62-8
Clear Commands	62-9
<b>Configuring Flexible NetFlow</b>	<b>63-1</b>
VSS Environment	63-1
Non-VSS Environment	63-7
<b>Configuring Ethernet OAM and CFM</b>	<b>64-1</b>
About Ethernet CFM	64-2
Ethernet CFM and OAM Definitions	64-2
CFM Domain	64-2
Maintenance Associations and Maintenance Points	64-4
CFM Messages	64-5
Crosscheck Function and Static Remote MEPs	64-5
SNMP Traps and Fault Alarms	64-5
Configuration Error List	64-6
IP SLAs Support for CFM	64-6
Configuring Ethernet CFM	64-6
Ethernet CFM Default Configuration	64-7
Ethernet CFM Configuration Guidelines	64-7
Configuring the CFM Domain	64-8
Configuring Ethernet CFM Crosscheck	64-11
Configuring Static Remote MEP	64-13
Configuring a Port MEP	64-14

Configuring SNMP Traps	64-16
Configuring Fault Alarms	64-16
Configuring IP SLAs CFM Operation	64-18
Manually Configuring an IP SLAs CFM Probe or Jitter Operation	64-19
Configuring an IP SLAs Operation with Endpoint Discovery	64-21
Configuring CFM on C-VLAN (Inner VLAN)	64-24
Feature Support and Behavior	64-26
Platform Restrictions and Limitations	64-26
Understanding CFM ITU-T Y.1731 Fault Management	64-27
Y.1731 Terminology	64-27
Alarm Indication Signals	64-28
Ethernet Remote Defect Indication	64-28
Multicast Ethernet Loopback	64-29
Configuring Y.1731 Fault Management	64-29
Default Y.1731 Configuration	64-29
Configuring ETH-AIS	64-29
Using Multicast Ethernet Loopback	64-31
Managing and Displaying Ethernet CFM Information	64-31
About Ethernet OAM Protocol	64-33
OAM Features	64-34
OAM Messages	64-34
Enabling and Configuring Ethernet OAM	64-35
Ethernet OAM Default Configuration	64-35
Ethernet OAM Configuration Guidelines	64-35
Enabling Ethernet OAM on an Interface	64-36
Enabling Ethernet OAM Remote Loopback	64-37
Configuring Ethernet OAM Link Monitoring	64-38
Configuring Ethernet OAM Remote Failure Indications	64-42
Configuring Ethernet OAM Templates	64-45
Displaying Ethernet OAM Protocol Information	64-49
Ethernet CFM and Ethernet OAM Interaction	64-51
Configuring Ethernet OAM Interaction with CFM	64-51
Configuring the OAM Manager	64-52
Enabling Ethernet OAM	64-52
Example: Configuring Ethernet OAM and CFM	64-53
<b>Configuring Y.1731 (AIS and RDI)</b>	<b>65-1</b>
AIS and RDI Terminology	65-1
About Y.1731	65-2

Server MEP	65-2
Alarm Indication Signal	65-2
Ethernet Remote Defect Indication	65-3
Configuring Y.1731	65-4
Y.1731 Configuration Guidelines	65-4
Configuring AIS Parameters	65-5
Clearing MEP from the AIS Defect Condition	65-6
Clearing SMEP from the AIS Defect Condition	65-6
Displaying Y.1731 Information	65-6
<b>Configuring Call Home</b>	<b>66-1</b>
About Call Home	66-2
Obtaining Smart Call Home	66-2
Configuring Call Home	66-3
Configuring Contact Information	66-4
Configuring Destination Profiles	66-5
Copying a Destination Profile	66-6
Subscribing to Alert Groups	66-6
Configuring Periodic Notification	66-8
Configuring Message Severity Threshold	66-8
Configuring Syslog Pattern Matching	66-9
Configuring General E-Mail Options	66-9
Enabling Call Home	66-10
Testing Call Home Communications	66-10
Sending a Call Home Test Message Manually	66-11
Sending a Call Home Alert Group Message Manually	66-11
Sending a Request for an Analysis and Report	66-12
Sending the Output of a Command	66-13
Configuring and Enabling Smart Call Home	66-13
Displaying Call Home Configuration Information	66-14
Call Home Default Settings	66-18
Alert Group Trigger Events and Commands	66-18
Message Contents	66-21
Syslog Alert Notification in Long-Text Format Example	66-25
Syslog Alert Notification in XML Format Example	66-28
<b>Configuring Cisco IOS IP SLA Operations</b>	<b>67-1</b>
Understanding Cisco IOS IP SLAs	67-2
Using Cisco IOS IP SLAs to Measure Network Performance	67-3
IP SLAs Responder and IP SLAs Control Protocol	67-4

Response Time Computation for IP SLAs	67-4
IP SLAs Operation Scheduling	67-5
IP SLAs Operation Threshold Monitoring	67-5
Configuring IP SLAs Operations	67-6
IP SLA Default Configuration	67-6
IP SLA Configuration Guidelines	67-6
Configuring the IP SLAs Responder	67-7
Analyzing IP Service Levels by Using the UDP Jitter Operation	67-8
Analyzing IP Service Levels by Using the ICMP Echo Operation	67-11
Monitoring IP SLAs Operations	67-13
<b>Configuring RMON</b>	<b>67-1</b>
About RMON	67-1
Configuring RMON	67-3
Default RMON Configuration	67-3
Configuring RMON Alarms and Events	67-3
Configuring RMON Collection on an Interface	67-5
Displaying RMON Status	67-6
<b>Performing Diagnostics</b>	<b>69-1</b>
Configuring Online Diagnostics	69-1
Configuring On-Demand Online Diagnostics	69-2
Scheduling Online Diagnostics	69-2
Performing Diagnostics	69-3
Starting and Stopping Online Diagnostic Tests	69-3
Displaying Online Diagnostic Tests and Test Results	69-4
Displaying Data Path Online Diagnostics Test Results	69-7
Line Card Online Diagnostics	69-8
Troubleshooting with Online Diagnostics	69-8
Power-On Self-Test Diagnostics	69-10
Overview of Power-On Self-Test Diagnostics	69-10
POST Result Example	69-11
Power-On Self-Test Results	69-13
Sample Display of the POST on an Active Supervisor Engine	69-13
Sample Display of the POST on a Standby Supervisor Engine	69-16
Troubleshooting the Test Failures	69-20
<b>Configuring WCCP Version 2 Services</b>	<b>70-1</b>
About WCCP	70-1
Overview	70-2

Hardware Acceleration	70-2
.Understanding WCCP Configuration	70-3
WCCP Features	70-4
HTTP and Non-HTTP Services Support	70-4
Multiple Routers Support	70-4
MD5 Security	70-5
Web Content Packet Return	70-5
Restrictions for WCCP	70-5
Configuring WCCP	70-6
Configuring a Service Group Using WCCP	70-6
Specifying a Web Cache Service	70-8
Using Access Lists for a WCCP Service Group	70-8
Setting a Password for a Router and Cache Engines	70-9
Verifying and Monitoring WCCP Configuration Settings	70-9
WCCP Configuration Examples	70-10
Performing a General WCCP Configuration Example	70-10
Running a Web Cache Service Example	70-10
Running a Reverse Proxy Service Example	70-10
Running TCP-Promiscuous Service Example	70-11
Running Redirect Access-List Example	70-11
Using Access Lists Example	70-11
Setting a Password for a Switch and Content Engines Example	70-11
Verifying WCCP Settings Example	70-12
<b>Configuring MIB Support</b>	<b>71-1</b>
Determining MIB Support for Cisco IOS Releases	71-1
Using Cisco IOS MIB Tools	71-2
Downloading and Compiling MIBs	71-2
Guidelines for Working with MIBs	71-3
Downloading MIBs	71-3
Compiling MIBs	71-4
Enabling SNMP Support	71-4
<b>ROM Monitor</b>	<b>72-1</b>
Entering the ROM Monitor	72-1
ROM Monitor Commands	72-2
ROM Monitor Command Descriptions	72-3
Configuration Register	72-3
Changing the Configuration Register Manually	72-3

- Changing the Configuration Register Using Prompts 72-4
- Console Download 72-4
  - Error Reporting 72-5
- Debug Commands 72-5
- Exiting the ROM Monitor 72-6

---

**INDEX**