



Consolidated Platform Configuration Guide, Cisco IOS Release 15.2(7)E (Catalyst 2960-X Switch)

First Published: 2019-03-27

Last Modified: 2022-09-29

Americas Headquarters

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

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

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

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

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

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

Any Internet Protocol (IP) addresses and phone numbers used in this document are not intended to be actual addresses and phone numbers. Any examples, command display output, network topology diagrams, and other figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses or phone numbers in illustrative content is unintentional and coincidental.

All printed copies and duplicate soft copies of this document are considered uncontrolled. See the current online version for the latest version.

Cisco has more than 200 offices worldwide. Addresses and phone numbers are listed on the Cisco website at www.cisco.com/go/offices.

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: www.cisco.com/go/trademarks. Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1721R)

© 2019 Cisco Systems, Inc. All rights reserved.



CONTENTS

Full Cisco Trademarks with Software License ?

CHAPTER 1

Using the Command-Line Interface 1

Information About Using the Command-Line Interface 1

Command Modes 1

Understanding Abbreviated Commands 3

No and Default Forms of Commands 3

CLI Error Messages 3

Configuration Logging 4

Using the Help System 4

How to Use the CLI to Configure Features 5

Configuring the Command History 5

Changing the Command History Buffer Size 5

Recalling Commands 6

Disabling the Command History Feature 6

Enabling and Disabling Editing Features 7

Editing Commands Through Keystrokes 7

Editing Command Lines That Wrap 8

Searching and Filtering Output of show and more Commands 9

Accessing the CLI 9

Accessing the CLI Through a Console Connection or Through Telnet 10

Accessing the CLI through Bluetooth 11

PART I

Interface and Hardware 13

CHAPTER 2

Configuring Interface Characteristics 15

Information About Configuring Interface Characteristics	15
Interface Types	15
Port-Based VLANs	15
Switch Ports	16
Switch Virtual Interfaces	17
EtherChannel Port Groups	18
Power over Ethernet Ports	18
Using the Switch USB Ports	18
USB Mini-Type B Console Port	18
USB Type A Ports	19
Interface Connections	20
Interface Configuration Mode	20
Default Ethernet Interface Configuration	21
Interface Speed and Duplex Mode	22
Speed and Duplex Configuration Guidelines	22
IEEE 802.3x Flow Control	23
How to Configure Interface Characteristics	24
Configuring Interfaces	24
Adding a Description for an Interface	25
Configuring a Range of Interfaces	26
Configuring and Using Interface Range Macros	27
Configuring Ethernet Interfaces	29
Setting the Interface Speed and Duplex Parameters	29
Configuring IEEE 802.3x Flow Control	30
Configuring SVI Autostate Exclude	31
Shutting Down and Restarting the Interface	32
Configuring the Console Media Type	33
Configuring the USB Inactivity Timeout	34
Monitoring Interface Characteristics	35
Monitoring Interface Status	35
Clearing and Resetting Interfaces and Counters	36
Configuration Examples for Interface Characteristics	37
Configuring a Range of Interfaces: Examples	37
Configuring and Using Interface Range Macros: Examples	37

Setting Interface Speed and Duplex Mode: Example	38
Configuring the Console Media Type: Example	38
Configuring the USB Inactivity Timeout: Example	38
Additional References for the Interface Characteristics Feature	39
Feature History and Information for Configuring Interface Characteristics	40

CHAPTER 3

Configuring Auto-MDIX 41

Prerequisites for Auto-MDIX	41
Restrictions for Auto-MDIX	41
Information About Configuring Auto-MDIX	41
Auto-MDIX on an Interface	41
How to Configure Auto-MDIX	42
Configuring Auto-MDIX on an Interface	42
Example for Configuring Auto-MDIX	43
Additional References	43
Feature History and Information for Auto-MDIX	44

CHAPTER 4

Configuring Ethernet Management Port 45

Prerequisites for Ethernet Management Ports	45
Information About the Ethernet Management Port	45
Ethernet Management Port Direct Connection to a Device	45
Ethernet Management Port Connection to Stack Devices using a Hub	46
Supported Features on the Ethernet Management Port	46
How to Configure the Ethernet Management Port	47
Disabling and Enabling the Ethernet Management Port	47
Additional References for Ethernet Management Ports	48
Feature History and Information for Ethernet Management Ports	48

CHAPTER 5

Configuring LLDP, LLDP-MED, and Wired Location Service 49

Information About LLDP, LLDP-MED, and Wired Location Service	49
LLDP	49
LLDP Supported TLVs	49
LLDP and Cisco Device Stacks	50
LLDP and Cisco Medianet	50

LLDP-MED	50
LLDP-MED Supported TLVs	50
Wired Location Service	51
Default LLDP Configuration	52
Restrictions for LLDP	53
How to Configure LLDP, LLDP-MED, and Wired Location Service	53
Enabling LLDP	53
Configuring LLDP Characteristics	54
Configuring LLDP-MED TLVs	56
Configuring Network-Policy TLV	57
Configuring Location TLV and Wired Location Service	60
Enabling Wired Location Service on the Device	62
Configuration Examples for LLDP, LLDP-MED, and Wired Location Service	63
Configuring Network-Policy TLV: Examples	63
Monitoring and Maintaining LLDP, LLDP-MED, and Wired Location Service	64
Additional References for LLDP, LLDP-MED, and Wired Location Service	65
Feature Information for LLDP, LLDP-MED, and Wired Location Service	65

CHAPTER 6

Configuring System MTU	67
Information About the MTU	67
System MTU Guidelines	67
How to Configure MTU	68
Configuring the System MTU	68
Configuration Examples for System MTU	69
Additional References for System MTU	69
Feature Information for System MTU	70

CHAPTER 7

Configuring Boot Fast	71
Configuring Boot Fast on the switch	71
Enabling Boot Fast	71
Disabling Boot Fast	72

CHAPTER 8

Configuring Power over Ethernet	73
Restrictions for PoE	73

Information About PoE	73
Power over Ethernet Ports	73
Supported Protocols and Standards	73
Powered-Device Detection and Initial Power Allocation	74
Power Management Modes	75
How to Configure PoE	78
Configuring a Power Management Mode on a PoE Port	78
Fast POE	80
Configuring Fast PoE	80
Budgeting Power for Devices Connected to a PoE Port	81
Budgeting Power to All PoE ports	82
Budgeting Power to a Specific PoE Port	83
Configuring Power Policing	84
Monitoring Power Status	86
Configuration Examples for Configuring PoE	86
Budgeting Power: Example	86
Additional References	87

CHAPTER 9

Configuring 2-event Classification	89
Information about 2-event Classification	89
Configuring 2-event Classification	89
Example: Configuring 2-Event Classification	90

CHAPTER 10

Configuring EEE	91
Restrictions for EEE	91
Information About EEE	91
EEE Overview	91
Default EEE Configuration	91
How to Configure EEE	91
Enabling or Disabling EEE	92
Monitoring EEE	93
Configuration Examples for Configuring EEE	93
Additional References	94
Feature History for Configuring EEE	94

PART II**IP Multicast Routing 95****CHAPTER 11****Configuring IGMP Snooping and Multicast VLAN Registration 97**

Prerequisites for Configuring IGMP Snooping and MVR 97

Prerequisites for IGMP Snooping 97

Prerequisites for MVR 98

Restrictions for Configuring IGMP Snooping and MVR 98

Restrictions for IGMP Snooping 98

Restrictions for MVR 98

Information About IGMP Snooping and MVR 99

IGMP Snooping 99

IGMP Versions 100

Joining a Multicast Group 100

Leaving a Multicast Group 102

Immediate Leave 103

IGMP Configurable-Leave Timer 103

IGMP Report Suppression 103

IGMP Snooping and Device Stacks 104

Default IGMP Snooping Configuration 104

Multicast VLAN Registration 104

MVR and IGMP 105

Modes of Operation 105

MVR and Switch Stacks 105

MVR in a Multicast Television Application 105

Default MVR Configuration 107

IGMP Filtering and Throttling 107

Default IGMP Filtering and Throttling Configuration 108

How to Configure IGMP Snooping and MVR 108

Enabling or Disabling IGMP Snooping on a Device 108

Enabling or Disabling IGMP Snooping on a VLAN Interface 109

Setting the Snooping Method 110

Configuring a Multicast Router Port 112

Configuring a Host Statically to Join a Group 113

Enabling IGMP Immediate Leave	114
Configuring the IGMP Leave Timer	115
Configuring TCN-Related Commands	116
Controlling the Multicast Flooding Time After a TCN Event	116
Recovering from Flood Mode	118
Disabling Multicast Flooding During a TCN Event	119
Configuring the IGMP Snooping Querier	120
Disabling IGMP Report Suppression	122
Configuring MVR Global Parameters	123
Configuring MVR Interfaces	125
Configuring IGMP Profiles	127
Applying IGMP Profiles	129
Setting the Maximum Number of IGMP Groups	130
Configuring the IGMP Throttling Action	131
Monitoring IGMP Snooping and MVR	133
Monitoring IGMP Snooping Information	133
Monitoring MVR	134
Monitoring IGMP Filtering and Throttling Configuration	135
Configuration Examples for IGMP Snooping and MVR	136
Example: Configuring IGMP Snooping Using CGMP Packets	136
Example: Enabling a Static Connection to a Multicast Router	136
Example: Configuring a Host Statically to Join a Group	136
Example: Enabling IGMP Immediate Leave	136
Example: Setting the IGMP Snooping Querier Source Address	136
Example: Setting the IGMP Snooping Querier Maximum Response Time	136
Example: Setting the IGMP Snooping Querier Timeout	137
Example: Setting the IGMP Snooping Querier Feature	137
Example: Configuring IGMP Profiles	137
Example: Applying IGMP Profile	137
Example: Setting the Maximum Number of IGMP Groups	137
Example: Configuring MVR Global Parameters	138
Example: Configuring MVR Interfaces	138
Additional References	138
Feature History and Information for IGMP Snooping	139

CHAPTER 12**Configuring Protocol Independent Multicast (PIM) 141**

- Prerequisites for PIM 141
- Restrictions for PIM 142
 - PIMv1 and PIMv2 Interoperability 142
 - Restrictions for Configuring PIM Stub Routing 142
 - Restrictions for Configuring Auto-RP and BSR 143
- Information About PIM 144
 - Protocol Independent Multicast 144
 - PIM Dense Mode 144
 - PIM Sparse Mode 145
 - Sparse-Dense Mode 145
 - PIM Versions 146
 - PIM Stub Routing 146
 - IGMP Helper 147
 - Rendezvous Points 148
 - Auto-RP 148
 - Sparse-Dense Mode for Auto-RP 149
 - Bootstrap Router 149
 - PIM Domain Border 149
 - Multicast Forwarding 150
 - Multicast Distribution Source Tree 150
 - Multicast Distribution Shared Tree 151
 - Source Tree Advantage 151
 - Shared Tree Advantage 152
 - PIM Shared Tree and Source Tree 152
 - Reverse Path Forwarding 154
 - RPF Check 155
 - Default PIM Routing Configuration 156
- How to Configure PIM 156
 - Enabling PIM Stub Routing 156
 - Configuring a Rendezvous Point 157
 - Manually Assigning an RP to Multicast Groups 158
 - Setting Up Auto-RP in a New Internetwork 160

Adding Auto-RP to an Existing Sparse-Mode Cloud	163
Configuring Sparse Mode with a Single Static RP(CLI)	165
Preventing Join Messages to False RPs	167
Filtering Incoming RP Announcement Messages	168
Configuring PIMv2 BSR	169
Defining the PIM Domain Border	170
Defining the IP Multicast Boundary	171
Configuring Candidate BSRs	172
Configuring the Candidate RPs	174
Delaying the Use of PIM Shortest-Path Tree	175
Modifying the PIM Router-Query Message Interval	177
Verifying PIM Operations	178
Verifying IP Multicast Operation in a PIM-SM or a PIM-SSM Network	178
Using PIM-Enabled Routers to Test IP Multicast Reachability	184
Monitoring and Troubleshooting PIM	186
Monitoring PIM Information	186
Monitoring the RP Mapping and BSR Information	186
Troubleshooting PIMv1 and PIMv2 Interoperability Problems	187
Configuration Examples for PIM	187
Example: Enabling PIM Stub Routing	187
Example: Verifying PIM Stub Routing	188
Example: Manually Assigning an RP to Multicast Groups	188
Example: Configuring Auto-RP	188
Example: Defining the IP Multicast Boundary to Deny Auto-RP Information	188
Example: Filtering Incoming RP Announcement Messages	188
Example: Preventing Join Messages to False RPs	189
Example: Configuring Candidate BSRs	189
Example: Configuring Candidate RPs	189
Additional References	190

CHAPTER 13

IPv6 Protocol Independent Multicast	193
Protocol Independent Multicast	193
PIM-Sparse Mode	193
IPv6 BSR: Configure RP Mapping	194

PIM-Source Specific Multicast 194

Routable Address Hello Option 195

PIM IPv6 Stub Routing 195

PART III

IPv6 197

CHAPTER 14

Configuring MLD Snooping 199

Finding Feature Information 199

Information About Configuring IPv6 MLD Snooping 199

Understanding MLD Snooping 200

MLD Messages 200

MLD Queries 201

Multicast Client Aging Robustness 201

Multicast Router Discovery 201

MLD Reports 202

MLD Done Messages and Immediate-Leave 202

Topology Change Notification Processing 202

MLD Snooping in Switch Stacks 203

How to Configure IPv6 MLD Snooping 203

Default MLD Snooping Configuration 203

MLD Snooping Configuration Guidelines 204

Enabling or Disabling MLD Snooping on the Switch 204

Enabling or Disabling MLD Snooping on a VLAN 205

Configuring a Static Multicast Group 206

Configuring a Multicast Router Port 207

Enabling MLD Immediate Leave 208

Configuring MLD Snooping Queries 209

Disabling MLD Listener Message Suppression 210

Displaying MLD Snooping Information 211

Configuration Examples for Configuring MLD Snooping 212

Configuring a Static Multicast Group: Example 212

Configuring a Multicast Router Port: Example 212

Enabling MLD Immediate Leave: Example 213

Configuring MLD Snooping Queries: Example 213

CHAPTER 15**Configuring IPv6 Unicast Routing 215**

- Finding Feature Information 215
- Information About Configuring IPv6 Host Functions 215
 - Understanding IPv6 216
 - IPv6 Addresses 216
 - Supported IPv6 Unicast Routing Features 216
 - IPv6 and Switch Stacks 220
 - Default IPv6 Configuration 220
 - Configuring IPv6 Addressing and Enabling IPv6 Routing 220
 - Configuring IPv6 ICMP Rate Limiting 222
 - Configuring Static Routing for IPv6 223
 - Displaying IPv6 226
- Configuration Examples for IPv6 Unicast Routing 226
 - Configuring IPv6 Addressing and Enabling IPv6 Routing: Example 226
 - Configuring IPv6 ICMP Rate Limiting: Example 227
 - Configuring Static Routing for IPv6: Example 227
 - Displaying IPv6: Example 227

CHAPTER 16**Configuring IPv6 ACL 229**

- Finding Feature Information 229
- Information About Configuring IPv6 ACLs 229
 - Understanding IPv6 ACLs 229
 - Supported ACL Features 230
 - IPv6 ACL Limitations 230
- Configuring IPv6 ACLs 231
 - Default IPv6 ACL Configuration 231
 - Interaction with Other Features and Switches 232
 - Creating IPv6 ACL 232
 - Applying an IPv6 ACL to an Interface 236
 - Displaying IPv6 ACLs 237
- Configuration Examples for IPv6 ACL 237
 - Example: Creating an IPv6 ACL 237
 - Example: Applying IPv6 ACLs 238

Example: Displaying IPv6 ACLs 238

PART IV

Layer 2 239

CHAPTER 17

Configuring Spanning Tree Protocol 241

Finding Feature Information 241

Restrictions for STP 241

Information About Spanning Tree Protocol 242

Spanning Tree Protocol 242

Spanning-Tree Topology and BPDUs 242

Bridge ID, Device Priority, and Extended System ID 244

Port Priority Versus Path Cost 245

Spanning-Tree Interface States 245

How a Device or Port Becomes the Root Device or Root Port 248

Spanning Tree and Redundant Connectivity 249

Spanning-Tree Address Management 249

Accelerated Aging to Retain Connectivity 249

Spanning-Tree Modes and Protocols 249

Supported Spanning-Tree Instances 250

Spanning-Tree Interoperability and Backward Compatibility 250

STP and IEEE 802.1Q Trunks 251

VLAN-Bridge Spanning Tree 251

Spanning Tree and Device Stacks 251

Default Spanning-Tree Configuration 252

How to Configure Spanning-Tree Features 253

Changing the Spanning-Tree Mode 253

Disabling Spanning Tree 254

Configuring the Root Device 255

Configuring a Secondary Root Device 256

Configuring Port Priority 257

Configuring Path Cost 258

Configuring the Device Priority of a VLAN 259

Configuring the Hello Time 260

Configuring the Forwarding-Delay Time for a VLAN 261

Configuring the Maximum-Aging Time for a VLAN	262
Configuring the Transmit Hold-Count	263
Monitoring Spanning-Tree Status	264
Feature Information for STP	264

CHAPTER 18

Configuring Multiple Spanning-Tree Protocol 265

Finding Feature Information	265
Prerequisites for MSTP	265
Restrictions for MSTP	266
Information About MSTP	266
MSTP Configuration	266
MSTP Configuration Guidelines	267
Root Switch	267
Multiple Spanning-Tree Regions	268
IST, CIST, and CST	268
Operations Within an MST Region	269
Operations Between MST Regions	269
IEEE 802.1s Terminology	270
Illustration of MST Regions	270
Hop Count	271
Boundary Ports	271
IEEE 802.1s Implementation	272
Port Role Naming Change	272
Interoperation Between Legacy and Standard Devices	273
Detecting Unidirectional Link Failure	273
MSTP and Device Stacks	274
Interoperability with IEEE 802.1D STP	274
RSTP Overview	275
Port Roles and the Active Topology	275
Rapid Convergence	276
Synchronization of Port Roles	277
Bridge Protocol Data Unit Format and Processing	278
Topology Changes	279
Protocol Migration Process	280

Default MSTP Configuration	280
About MST-to-PVST+ Interoperability (PVST+ Simulation)	281
About Detecting Unidirectional Link Failure	282
How to Configure MSTP Features	283
Specifying the MST Region Configuration and Enabling MSTP	283
Configuring the Root Device	285
Configuring a Secondary Root Device	286
Configuring Port Priority	287
Configuring Path Cost	288
Configuring the Device Priority	290
Configuring the Hello Time	291
Configuring the Forwarding-Delay Time	292
Configuring the Maximum-Aging Time	293
Configuring the Maximum-Hop Count	293
Specifying the Link Type to Ensure Rapid Transitions	294
Designating the Neighbor Type	295
Restarting the Protocol Migration Process	296
Configuring PVST+ Simulation	297
Enabling PVST+ Simulation on a Port	298
Examples	299
Examples: PVST+ Simulation	299
Examples: Detecting Unidirectional Link Failure	302
Monitoring MST Configuration and Status	303
Feature Information for MSTP	303

CHAPTER 19
Configuring Optional Spanning-Tree Features 305

Finding Feature Information	305
Restriction for Optional Spanning-Tree Features	305
Information About Optional Spanning-Tree Features	305
PortFast	305
BPDU Guard	306
BPDU Filtering	306
UplinkFast	307
Cross-Stack UplinkFast	308

How Cross-Stack UplinkFast Works	309
Events That Cause Fast Convergence	310
BackboneFast	310
EtherChannel Guard	312
Root Guard	313
Loop Guard	314
STP PortFast Port Types	314
Bridge Assurance	315
How to Configure Optional Spanning-Tree Features	317
Enabling PortFast	317
Enabling BPDU Guard	318
Enabling BPDU Filtering	320
Enabling UplinkFast for Use with Redundant Links	321
Disabling UplinkFast	322
Enabling BackboneFast	323
Enabling EtherChannel Guard	324
Enabling Root Guard	325
Enabling Loop Guard	326
Enabling PortFast Port Types	327
Configuring the Default Port State Globally	327
Configuring PortFast Edge on a Specified Interface	328
Configuring a PortFast Network Port on a Specified Interface	329
Enabling Bridge Assurance	330
Examples	331
Examples: Configuring PortFast Edge on a Specified Interface	331
Examples: Configuring a PortFast Network Port on a Specified Interface	332
Example: Configuring Bridge Assurance	333
Monitoring the Spanning-Tree Status	334
Feature Information for Optional Spanning-Tree Features	334

CHAPTER 20

Configuring Resilient Ethernet Protocol	335
Finding Feature Information	335
Overview of Resilient Ethernet Protocol	335
Link Integrity	337

Fast Convergence	338
VLAN Load Balancing	338
Spanning Tree Interaction	339
REP Ports	340
How to Configure Resilient Ethernet Protocol	340
Default REP Configuration	340
REP Configuration Guidelines	340
Configuring REP Administrative VLAN	342
Configuring a REP Interface	343
Setting Manual Preemption for VLAN Load Balancing	346
Configuring SNMP Traps for REP	347
Monitoring Resilient Ethernet Protocol Configuration	348
Configuration Examples for Resilient Ethernet Protocol	349
Example: Configuring the REP Administrative VLAN	349
Example: Configuring a REP Interface	350
Additional References for Resilient Ethernet Protocol	351
Feature Information for Resilient Ethernet Protocol	352

CHAPTER 21

Configuring EtherChannels	353
Finding Feature Information	353
Restrictions for EtherChannels	353
Information About EtherChannels	354
EtherChannel Overview	354
EtherChannel Modes	354
EtherChannel on Devices	355
EtherChannel Link Failover	355
Channel Groups and Port-Channel Interfaces	356
Port Aggregation Protocol	356
PAgP Modes	357
PAgP Learn Method and Priority	357
PAgP Interaction with Virtual Switches and Dual-Active Detection	358
PAgP Interaction with Other Features	358
Link Aggregation Control Protocol	359
LACP Modes	359

LACP Interaction with Other Features	359
EtherChannel On Mode	360
Load-Balancing and Forwarding Methods	360
MAC Address Forwarding	360
IP Address Forwarding	361
Load-Balancing Advantages	361
EtherChannel Load Deferral Overview	362
EtherChannel and Device Stacks	363
Device Stack and PAgP	363
Switch Stacks and LACP	363
Default EtherChannel Configuration	364
EtherChannel Configuration Guidelines	364
Layer 2 EtherChannel Configuration Guidelines	365
Auto-LAG	365
Auto-LAG Configuration Guidelines	366
How to Configure EtherChannels	367
Configuring Layer 2 EtherChannels	367
Configuring EtherChannel Load-Balancing	369
Configuring Port Channel Load Deferral	370
Configuring the PAgP Learn Method and Priority	372
Configuring LACP Hot-Standby Ports	373
Configuring the LACP System Priority	373
Configuring the LACP Port Priority	374
Configuring the LACP Port Channel Min-Links Feature	375
Configuring LACP Fast Rate Timer	376
Configuring Auto-LAG Globally	377
Configuring Auto-LAG on a Port Interface	378
Configuring Persistence with Auto-LAG	379
Monitoring EtherChannel, PAgP, and LACP Status	379
Configuration Examples for Configuring EtherChannels	380
Configuring Layer 2 EtherChannels: Examples	380
Example: Configuring Port Channel Load Deferral	381
Configuring Auto LAG: Examples	381
Configuring LACP Port Channel Min-Links: Examples	382

Example: Configuring LACP Fast Rate Timer	383
Additional References for EtherChannels	383
Feature Information for EtherChannels	384

CHAPTER 22

Configuring Link-State Tracking 385

Finding Feature Information	385
Restrictions for Configuring Link-State Tracking	385
Understanding Link-State Tracking	386
How to Configure Link-State Tracking	388
Monitoring Link-State Tracking	389
Configuring Link-State Tracking: Example	389
Additional References for Link-State Tracking	389
Feature Information for Link-State Tracking	390

CHAPTER 23

Configuring Flex Links and the MAC Address-Table Move Update Feature 391

Finding Feature Information	391
Restrictions for Configuring Flex Links and MAC Address-Table Move Update	391
Information About Flex Links and MAC Address-Table Move Update	392
Flex Links	392
Flex Links Configuration	392
VLAN Flex Links Load Balancing and Support	393
Multicast Fast Convergence with Flex Links Failover	393
Learning the Other Flex Links Port as the mrouter Port	393
Generating IGMP Reports	394
Leaking IGMP Reports	394
MAC Address-Table Move Update	394
Flex Links VLAN Load Balancing Configuration Guidelines	396
MAC Address-Table Move Update Configuration Guidelines	396
Default Flex Links and MAC Address-Table Move Update Configuration	396
How to Configure Flex Links and the MAC Address-Table Move Update Feature	396
Configuring Flex Links	396
Configuring a Preemption Scheme for a Pair of Flex Links	397
Configuring VLAN Load Balancing on Flex Links	398
Configuring MAC Address-Table Move Update	399

Configuring a Device to Obtain and Process MAC Address-Table Move Update Messages	400
Monitoring Flex Links, Multicast Fast Convergence, and MAC Address-Table Move Update	401
Configuration Examples for Flex Links	401
Configuring Flex Links: Examples	401
Configuring VLAN Load Balancing on Flex Links: Examples	401
Configuring the MAC Address-Table Move Update: Examples	403
Configuring Multicast Fast Convergence with Flex Links Failover: Examples	403
Additional References for Flex Links and MAC Address-Table Move Update	405
Feature Information for Flex Links and MAC Address-Table Move Update	406

CHAPTER 24

Configuring UniDirectional Link Detection 407

Finding Feature Information	407
Restrictions for Configuring UDLD	407
Information About UDLD	408
Modes of Operation	408
Normal Mode	408
Aggressive Mode	408
Methods to Detect Unidirectional Links	409
Neighbor Database Maintenance	409
Event-Driven Detection and Echoing	409
UDLD Reset Options	409
Default UDLD Configuration	410
How to Configure UDLD	410
Enabling UDLD Globally	410
Enabling UDLD on an Interface	411
Monitoring and Maintaining UDLD	412
Additional References for UDLD	412
Feature Information for UDLD	413

CHAPTER 25

Configuring the PPPoE Intermediate Agent 415

Restrictions for PPPoE Intermediate Agent	415
Information about PPPoE Intermediate Agent	415
How to Configure PPPoE IA	416
Enabling PPPoE IA on a Switch	416

Configuring the Access Node Identifier for PPPoE IA on a Switch	416
Configuring the Identifier String, Option, and Delimiter for PPPoE IA on a Switch	417
Configuring the Generic Error Message for PPPoE IA on a Switch	417
Enabling PPPoE IA on an Interface	418
Configuring the PPPoE IA Trust Setting on an Interface	419
Configuring PPPoE Intermediate Agent Rate Limiting Setting on an Interface	420
Configuring PPPoE IA Vendor-tag Stripping on an Interface	420
Configuring PPPoE Intermediate Agent Circuit-ID and Remote-ID on an Interface	421
Enabling PPPoE IA for a Specific VLAN on an Interface	422
Configuring PPPoE IA Circuit-ID and Remote-ID for a VLAN on an Interface	423
Configuration Examples for PPPoE IA	424
Example: Enabling PPPoE Intermediate Agent on a Switch	424
Example: Configuring the Access Node Identifier for PPPoE IA on a Switch	424
Example: Configuring the Identifier String, Option, and Delimiter for PPPoE IA on a Switch	424
Example: Configuring the Generic Error Message for PPPoE IA on a Switch	424
Example: Enabling PPPoE IA on an Interface	424
Example: Configuring the PPPoE Intermediate Agent Trust Setting on an Interface	425
Example: Configuring PPPoE Intermediate Agent Rate Limiting Setting on an Interface	425
Example: Configuring PPPoE IA Vendor-tag Stripping on an Interface	425
Example: Configuring PPPoE IA Circuit-ID and Remote-ID on an Interface	425
Example: Enabling PPPoE IA for a Specific VLAN on an Interface	425
Example: Configuring PPPoE IA Circuit-ID and Remote-ID for a VLAN on an Interface	426
Displaying Configuration Parameters	426
Clearing Packet Counters	428
Debugging PPPoE Intermediate Agent	428
Troubleshooting Tips	429
Feature Information for Configuring the PPPoE Intermediate Agent	429

PART V
Cisco Flexible NetFlow 431

CHAPTER 26
Configuring Flexible NetFlow 433

Prerequisites for Flexible NetFlow	433
Restrictions for Flexible NetFlow	434
Information About Flexible Netflow	436

Flexible NetFlow Overview	436
Original NetFlow and Benefits of Flexible NetFlow	436
Flexible NetFlow Components	437
Flow Records	437
Flow Exporters	438
Flow Monitors	439
Flow Samplers	441
Supported Flexible NetFlow Fields	441
Default Settings	442
How to Configure Flexible Netflow	443
Creating a Flow Record	443
Creating a Flow Exporter	445
Creating a Flow Monitor	447
Creating a Sampler	449
Applying a Flow to an Interface	450
Configuring NetFlow on SVI	452
Configuring Layer 2 NetFlow	452
Monitoring Flexible NetFlow	453
Configuration Examples for Flexible NetFlow	454
Example: Configuring a Flow	454
Additional References for NetFlow	455
Feature Information for Flexible NetFlow	455

PART VI

Openflow 457

CHAPTER 27

OpenFlow 459

Finding Feature Information	459
Prerequisites for OpenFlow	459
Restrictions for OpenFlow	460
Information About Open Flow	461
Overview of OpenFlow	461
OpenFlow Controller Operation	461
Cisco OpenFlow Feature Support	462
Supported Match and Actions and Pipelines	464

Configuring OpenFlow	467
Monitoring OpenFlow	471
Configuration Examples for OpenFlow	471

PART VII

QoS 477**CHAPTER 28****Configuring QoS 479**

Finding Feature Information	479
Prerequisites for QoS	479
QoS ACL Guidelines	480
Policing Guidelines	480
General QoS Guidelines	480
Restrictions for QoS	481
Information About QoS	482
QoS Implementation	482
Layer 2 Frame Prioritization Bits	483
Layer 3 Packet Prioritization Bits	483
End-to-End QoS Solution Using Classification	484
QoS Basic Model	484
Actions at Ingress Port	484
Actions at Egress Port	485
Classification Overview	485
Policing and Marking Overview	490
Mapping Tables Overview	491
Queueing and Scheduling Overview	492
Queueing and Scheduling on Ingress Queues	494
Queueing and Scheduling on Egress Queues	497
Packet Modification	501
Standard QoS Default Configuration	501
Default Ingress Queue Configuration	502
Default Egress Queue Configuration	503
Default Mapping Table Configuration	505
DSCP Maps	506
Default CoS-to-DSCP Map	506

Default IP-Precedence-to-DSCP Map	506
Default DSCP-to-CoS Map	507
How to Configure QoS	507
Enabling QoS Globally	507
Enabling VLAN-Based QoS on Physical Ports	508
Configuring Classification Using Port Trust States	509
Configuring the Trust State on Ports Within the QoS Domain	509
Configuring the CoS Value for an Interface	511
Configuring a Trusted Boundary to Ensure Port Security	513
Enabling DSCP Transparency Mode	515
Configuring the DSCP Trust State on a Port Bordering Another QoS Domain	516
Configuring a QoS Policy	519
Classifying Traffic by Using ACLs	519
Classifying Traffic by Using Class Maps	526
Classifying Traffic by Using Class Maps and Filtering IPv6 Traffic	528
Classifying, Policing, and Marking Traffic on Physical Ports by Using Policy Maps	530
Classifying, Policing, and Marking Traffic by Using Aggregate Policers	535
Configuring DSCP Maps	537
Configuring the CoS-to-DSCP Map	537
Configuring the IP-Precedence-to-DSCP Map	538
Configuring the Policed-DSCP Map	539
Configuring the DSCP-to-CoS Map	540
Configuring the DSCP-to-DSCP-Mutation Map	541
Configuring Ingress Queue Characteristics	543
Configuration Guidelines	543
Mapping DSCP or CoS Values to an Ingress Queue and Setting WTD Thresholds	543
Allocating Buffer Space Between the Ingress Queues	545
Allocating Bandwidth Between the Ingress Queues	546
Configuring Egress Queue Characteristics	548
Configuration Guidelines	548
Allocating Buffer Space to and Setting WTD Thresholds for an Egress Queue-Set	548
Mapping DSCP or CoS Values to an Egress Queue and to a Threshold ID	551
Configuring SRR Shaped Weights on Egress Queues	554
Configuring SRR Shared Weights on Egress Queues	556

Configuring the Egress Expedite Queue	557
Limiting the Bandwidth on an Egress Interface	558
Monitoring Standard QoS	560
Configuration Examples for QoS	560
Example: Configuring Port to the DSCP-Trusted State and Modifying the DSCP-to-DSCP-Mutation Map	560
Examples: Classifying Traffic by Using ACLs	561
Examples: Classifying Traffic by Using Class Maps	562
Examples: Classifying, Policing, and Marking Traffic on Physical Ports Using Policy Maps	563
Examples: Classifying, Policing, and Marking Traffic by Using Aggregate Policers	564
Examples: Configuring DSCP Maps	565
Examples: Configuring Ingress Queue Characteristics	567
Examples: Configuring Egress Queue Characteristics	567
Where to Go Next	568
Additional References	568
Feature History and Information for QoS	569

CHAPTER 29

Configuring Auto-QoS	571
Finding Feature Information	571
Prerequisites for Auto-QoS	571
Restrictions for Auto-QoS	572
Information about Configuring Auto-QoS	572
Auto-QoS Overview	572
Auto-QoS Compact Overview	572
Generated Auto-QoS Configuration	572
VoIP Device Specifics	573
Enhanced Auto-QoS for Video, Trust, and Classification	574
Auto-QoS Configuration Migration	574
Auto-QoS Configuration Guidelines	575
Auto-QoS VoIP Considerations	575
Auto-QoS Enhanced Considerations	576
Effects of Auto-QoS on Running Configuration	576
Effects of Auto-QoS Compact on Running Configuration	576
How to Configure Auto-QoS	577

Configuring Auto-QoS	577
Enabling Auto-QoS	577
Enabling Auto-Qos Compact	579
Troubleshooting Auto-QoS	580
Monitoring Auto-QoS	580
Configuration Examples for Auto-Qos	581
Examples: Global Auto-QoS Configuration	581
Examples: Auto-QoS Generated Configuration for VoIP Devices	583
Examples: Auto-QoS Generated Configuration for VoIP Devices	585
Examples: Auto-QoS Generated Configuration For Enhanced Video, Trust, and Classify Devices	586
auto qos global compact	589
Where to Go Next for Auto-QoS	589
Additional References for Auto-QoS	589
Feature History and Information for Auto-QoS	590

PART VIII
Network Management 591

CHAPTER 30
Configuring Cisco IOS Configuration Engine 593

Prerequisites for Configuring the Configuration Engine	593
Restrictions for Configuring the Configuration Engine	593
Information About Configuring the Configuration Engine	594
Cisco Configuration Engine Software	594
Configuration Service	595
Event Service	595
NameSpace Mapper	596
Cisco Networking Services IDs and Device Hostnames	596
ConfigID	596
DeviceID	596
Hostname and DeviceID	597
Hostname, DeviceID, and ConfigID	597
Cisco IOS CNS Agents	597
Initial Configuration	597
Incremental (Partial) Configuration	598
Synchronized Configuration	598

Automated CNS Configuration	598
How to Configure the Configuration Engine	599
Enabling the CNS Event Agent	599
Enabling the Cisco IOS CNS Agent	601
Enabling an Initial Configuration for Cisco IOS CNS Agent	602
Refreshing DeviceIDs	607
Enabling a Partial Configuration for Cisco IOS CNS Agent	609
Monitoring CNS Configurations	610
Additional References	611
Feature History and Information for the Configuration Engine	612

CHAPTER 31
Configuring the Cisco Discovery Protocol 613

Information About CDP	613
Cisco Discovery Protocol Overview	613
CDP and Stacks	614
Default Cisco Discovery Protocol Configuration	614
How to Configure CDP	614
Configuring Cisco Discovery Protocol Characteristics	614
Disabling Cisco Discovery Protocol	616
Enabling Cisco Discovery Protocol	617
Disabling Cisco Discovery Protocol on an Interface	618
Enabling Cisco Discovery Protocol on an Interface	619
Monitoring and Maintaining Cisco Discovery Protocol	621
Additional References	621
Feature History and Information for Cisco Discovery Protocol	622

CHAPTER 32
Configuring Simple Network Management Protocol 623

Prerequisites for SNMP	623
Restrictions for SNMP	625
Information About SNMP	625
SNMP Overview	625
SNMP Manager Functions	626
SNMP Agent Functions	626
SNMP Community Strings	627

SNMP MIB Variables Access	627
SNMP Notifications	627
SNMP ifIndex MIB Object Values	628
Default SNMP Configuration	628
SNMP Configuration Guidelines	629
How to Configure SNMP	630
Disabling the SNMP Agent	630
Configuring Community Strings	631
Configuring SNMP Groups and Users	633
Configuring SNMP Notifications	636
Setting the Agent Contact and Location Information	641
Limiting TFTP Servers Used Through SNMP	642
Monitoring SNMP Status	643
SNMP Examples	644
Additional References	645
Feature History and Information for Simple Network Management Protocol	646

CHAPTER 33

Configuring SPAN and RSPAN	647
Prerequisites for SPAN and RSPAN	647
Restrictions for SPAN and RSPAN	647
Information About SPAN and RSPAN	649
SPAN and RSPAN	649
Local SPAN	649
Remote SPAN	650
SPAN and RSPAN Concepts and Terminology	651
SPAN and RSPAN Interaction with Other Features	656
SPAN and RSPAN and Device Stacks	657
Flow-Based SPAN	657
Default SPAN and RSPAN Configuration	658
Configuration Guidelines	659
SPAN Configuration Guidelines	659
RSPAN Configuration Guidelines	659
FSPAN and FRSPAN Configuration Guidelines	659
How to Configure SPAN and RSPAN	659

Creating a Local SPAN Session	659
Creating a Local SPAN Session and Configuring Incoming Traffic	662
Specifying VLANs to Filter	664
Configuring a VLAN as an RSPAN VLAN	666
Creating an RSPAN Source Session	667
Specifying VLANs to Filter	669
Creating an RSPAN Destination Session	671
Creating an RSPAN Destination Session and Configuring Incoming Traffic	673
Configuring an FSPAN Session	675
Configuring an FRSPAN Session	678
Monitoring SPAN and RSPAN Operations	681
SPAN and RSPAN Configuration Examples	681
Example: Configuring Local SPAN	681
Examples: Creating an RSPAN VLAN	682
Additional References	683
Feature History and Information for SPAN and RSPAN	684

PART IX
Routing 687

CHAPTER 34
Configuring IP Unicast Routing 689

Finding Feature Information	689
Information About Configuring IP Unicast Routing	689
Information About IP Routing	690
Types of Routing	690
IP Routing and Switch Stacks	690
Configuring IP Unicast Routing	691
Enabling IP Unicast Routing	692
Assigning IP Addresses to SVIs	693
Configuring Static Unicast Routes	695
Monitoring and Maintaining the IP Network	696

CHAPTER 35
Configuring IPv6 First Hop Security 697

Finding Feature Information	697
Prerequisites for First Hop Security in IPv6	697

Restrictions for First Hop Security in IPv6	698
Information about First Hop Security in IPv6	698
How to Configure an IPv6 Snooping Policy	701
How to Attach an IPv6 Snooping Policy to an Interface	702
How to Attach an IPv6 Snooping Policy to a Layer 2 EtherChannel Interface	704
How to Configure the IPv6 Binding Table Content	705
How to Configure an IPv6 Neighbor Discovery Inspection Policy	706
How to Attach an IPv6 Neighbor Discovery Inspection Policy to an Interface	707
How to Attach an IPv6 Neighbor Discovery Inspection Policy to a Layer 2 EtherChannel Interface	708
How to Attach an IPv6 Neighbor Discovery Multicast Suppress Policy on a Device	709
How to Attach an IPv6 Neighbor Discovery Multicast Suppress Policy on an Interface	710
How to Attach an IPv6 Neighbor Discovery Multicast Suppress Policy to a Layer 2 EtherChannel Interface	711
How to Configure an IPv6 Router Advertisement Guard Policy	712
How to Attach an IPv6 Router Advertisement Guard Policy to an Interface	714
How to Attach an IPv6 Router Advertisement Guard Policy to a Layer 2 EtherChannel Interface	715
How to Configure an IPv6 DHCP Guard Policy	716
How to Attach an IPv6 DHCP Guard Policy to an Interface or a VLAN on an Interface	718
How to Attach an IPv6 DHCP Guard Policy to a Layer 2 EtherChannel Interface	719
How to Configure IPv6 Source Guard	720
How to Attach an IPv6 Source Guard Policy to an Interface	721
How to attach an IPv6 Source Guard Policy to a Layer 2 EtherChannel Interface	722
How to Configure IPv6 Prefix Guard	722
How to Attach an IPv6 Prefix Guard Policy to an Interface	723
How to attach an IPv6 Prefix Guard Policy to a Layer 2 EtherChannel Interface	724
Configuration Examples for IPv6 First Hop Security	725
Examples: How to attach an IPv6 Source Guard Policy to a Layer 2 EtherChannel Interface	725
Examples: How to attach an IPv6 Prefix Guard Policy to a Layer 2 EtherChannel Interface	725
Additional References	725
 CHAPTER 36	
Routing Information Protocol	727
Prerequisites for RIP	727
Restrictions for RIP	727

Information About Routing Information Protocol	727
RIP Overview	727
RIP Routing Updates	728
Authentication in RIP	728
RIP Routing Metric	729
RIP Versions	729
Exchange of Routing Information	729
Neighbor Router Authentication	730
How to Configure Routing Information Protocol	731
Enabling RIP and Configuring RIP Parameters	731
Specifying a RIP Version and Enabling Authentication	732
Configuration Examples for Routing Information Protocol	734
Example: Enabling RIP and Configuring RIP Parameters	734
Example: Specifying a RIP Version and Enabling Authentication	734
Additional References for RIP	734
Feature Information for RIP	735

CHAPTER 37
Open Shortest Path First (OSPF) 737

Information About OSPF	737
OSPF for Routed Access	738
OSPF Area Parameters	738
Other OSPF Parameters	738
LSA Group Pacing	739
Loopback Interfaces	739
How to Configure OSPF	740
Default OSPF Configuration	740
Configuring Basic OSPF Parameters	741
Configuring OSPF Interfaces	742
Configuring OSPF Area Parameters	744
Configuring Other OSPF Parameters	746
Changing LSA Group Pacing	748
Configuring a Loopback Interface	749
Monitoring OSPF	750
Configuration Examples for OSPF	751

Example: Configuring Basic OSPF Parameters 751

CHAPTER 38

IPv6 Open Shortest Path First version 3 753

IPv6 Routing: OSPFv3 753

Prerequisites for IPv6 Routing: OSPFv3 753

Restrictions for IPv6 Routing: OSPFv3 753

Information About IPv6 Routing: OSPFv3 753

How OSPFv3 Works 753

Comparison of OSPFv3 and OSPF Version 2 754

LSA Types for OSPFv3 754

NBMA in OSPFv3 755

Load Balancing in OSPFv3 756

Addresses Imported into OSPFv3 756

OSPFv3 Customization 756

Force SPF in OSPFv3 758

How to Configure Load Balancing in OSPFv3 758

Configuring the OSPFv3 Device Process 758

Configuring NBMA Interfaces in OSPFv3 760

Forcing an SPF Calculation 761

Verifying OSPFv3 Configuration and Operation 762

Configuration Examples for Load Balancing in OSPFv3 765

Example: Configuring the OSPFv3 Device Process 765

Example: Configuring NBMA Interfaces 765

Example: Forcing SPF Configuration 766

Additional References 766

Feature Information for IPv6 Routing: OSPFv3 767

CHAPTER 39

Configuring Policy-Based Routing (PBR) 769

Policy-Based Routing 769

Information About Policy-Based Routing 769

Policy-Based Routing Using Object Tracking 770

How to Configure PBR 770

Verifying Next-Hop IP Using Object Tracking 773

Feature Information for Configuring PBR 775

PART X**Security 777**

CHAPTER 40**Security Features Overview 779**

Security Features Overview 779

CHAPTER 41**Preventing Unauthorized Access 783**

Preventing Unauthorized Access 783

CHAPTER 42**Controlling Switch Access with Passwords and Privilege Levels 785**

Restrictions for Controlling Switch Access with Passwords and Privileges 785

Restrictions and Guidelines for Reversible Password Types 785

Restrictions and Guidelines for Irreversible Password Types 785

Information About Passwords and Privilege Levels 786

Default Password and Privilege Level Configuration 786

Additional Password Security 786

Password Recovery 786

Terminal Line Telnet Configuration 787

Username and Password Pairs 787

Privilege Levels 787

How to Control Switch Access with Passwords and Privilege Levels 788

Setting or Changing a Static Enable Password 788

Protecting Enable and Enable Secret Passwords with Encryption 789

Disabling Password Recovery 791

Setting a Telnet Password for a Terminal Line 792

Configuring Username and Password Pairs 793

Setting the Privilege Level for a Command 795

Changing the Default Privilege Level for Lines 796

Logging into and Exiting a Privilege Level 797

Monitoring Switch Access 797

Configuration Examples for Setting Passwords and Privilege Levels 798

Example: Setting or Changing a Static Enable Password 798

Example: Protecting Enable and Enable Secret Passwords with Encryption 798

Example: Setting a Telnet Password for a Terminal Line 798

Example: Setting the Privilege Level for a Command	798
Additional References	798

CHAPTER 43

Configuring TACACS+ 801

Finding Feature Information	801
Prerequisites for TACACS+	801
Restrictions for TACACS+	802
Information About TACACS+	803
TACACS+ and Switch Access	803
TACACS+ Overview	803
TACACS+ Operation	804
Method List	805
TACACS AV Pairs	805
TACACS Authentication and Authorization AV Pairs	805
TACACS Accounting AV Pairs	813
Configuring AAA Server Group Selection Based on DNIS	824
TACACS+ Configuration Options	826
TACACS+ Login Authentication	826
TACACS+ Authorization for Privileged EXEC Access and Network Services	826
TACACS+ Authentication	826
TACACS+ Authorization	826
TACACS+ Accounting	827
Default TACACS+ Configuration	827
Per VRF for TACACS Servers	827
How to Configure TACACS+	827
Identifying the TACACS+ Server Host and Setting the Authentication Key	827
Configuring TACACS+ Login Authentication	829
Configuring TACACS+ Authorization for Privileged EXEC Access and Network Services	831
Starting TACACS+ Accounting	832
Establishing a Session with a Router if the AAA Server is Unreachable	834
Establishing a Session with a Router if the AAA Server is Unreachable	834
Configuring Per VRF on a TACACS Server	834
Verifying Per VRF for TACACS Servers	836
Monitoring TACACS+	837

Configuration Examples for TACACS+	837
Example: TACACS Authorization	837
Example: TACACS Accounting	838
Example: TACACS Authentication	838
Example: Configuring Per VRF for TACACS Servers	840
Additional References for TACACS+	841
Feature Information for TACACS+	841

CHAPTER 44
Configuring RADIUS 843

Prerequisites for Configuring RADIUS	843
Restrictions for Configuring RADIUS	844
Information about RADIUS	844
RADIUS and Switch Access	844
RADIUS Overview	844
RADIUS Operation	845
Default RADIUS Configuration	846
RADIUS Server Host	846
RADIUS Login Authentication	846
AAA Server Groups	847
AAA Authorization	847
RADIUS Accounting	847
Vendor-Specific RADIUS Attributes	847
RADIUS Disconnect-Cause Attribute Values	859
RADIUS Progress Codes	863
Vendor-Proprietary RADIUS Server Communication	863
Enhanced Test Command	864
How to Configure RADIUS	864
Identifying the RADIUS Server Host	864
Configuring Settings for All RADIUS Servers	866
Configuring RADIUS Login Authentication	867
Defining AAA Server Groups	870
Configuring RADIUS Authorization for User Privileged Access and Network Services	871
Starting RADIUS Accounting	872
Verifying Attribute 196	874

Configuring the Device to Use Vendor-Specific RADIUS Attributes	874
Configuring the Device for Vendor-Proprietary RADIUS Server Communication	875
Configuring a User Profile and Associating it with the RADIUS Record	877
Verifying the Enhanced Test Command Configuration	877
Configuration Examples for RADIUS	878
Examples: Identifying the RADIUS Server Host	878
Example: Using Two Different RADIUS Group Servers	878
Examples: AAA Server Groups	878
Troubleshooting Tips for RADIUS Progress Codes	879
Examples: Configuring the Switch to Use Vendor-Specific RADIUS Attributes	879
Example: Configuring the Switch for Vendor-Proprietary RADIUS Server Communication	880
Example: User Profile Associated With the test aaa group Command	880
Additional References for RADIUS	881
Feature Information for RADIUS	882

CHAPTER 45

RADIUS Server Load Balancing 883

Prerequisites for RADIUS Server Load Balancing	883
Restrictions for RADIUS Server Load Balancing	883
Information About RADIUS Server Load Balancing	884
RADIUS Server Load Balancing Overview	884
Transaction Load Balancing Across RADIUS Server Groups	884
RADIUS Server Status and Automated Testing	885
How to Configure RADIUS Server Load Balancing	886
Enabling Load Balancing for a Named RADIUS Server Group	886
Enabling Load Balancing for a Global RADIUS Server Group	886
Troubleshooting RADIUS Server Load Balancing	887
Configuration Examples for RADIUS Server Load Balancing	889
Example: Enabling Load Balancing for a Named RADIUS Server Group	889
Example: Enabling Load Balancing for a Global RADIUS Server Group	891
Example: Monitoring Idle Timer	893
Example: Configuring the Preferred Server with the Same Authentication and Authorization Server	894
Example: Configuring the Preferred Server with Different Authentication and Authorization Servers	894

Example: Configuring the Preferred Server with Overlapping Authentication and Authorization Servers	895
Example: Configuring the Preferred Server with Authentication Servers As a Subset of Authorization Servers	895
Example: Configuring the Preferred Server with Authentication Servers As a Superset of Authorization Servers	896
Additional References for RADIUS Server Load Balancing	896
Feature Information for RADIUS Server Load Balancing	897

CHAPTER 46
RADIUS Change of Authorization Support 899

Information About RADIUS Change-of-Authorization	899
RADIUS Change of Authorization	899
Change-of-Authorization Requests	901
RFC 5176 Compliance	901
Preconditions	902
CoA Request Response Code	902
Session Identification	902
Session Identification	903
CoA ACK Response Code	904
CoA NAK Response Code	904
Session Reauthentication	904
Session Reauthentication in a Switch Stack	904
Session Termination	905
CoA Activate Service Command	905
CoA Deactivate Service Command	906
CoA Request: Disable Host Port	907
CoA Request: Bounce-Port	907
CoA Session Query Command	908
CoA Session Reauthenticate Command	908
CoA Session Terminate Command	909
Stacking Guidelines for Session Termination	909
Stacking Guidelines for CoA-Request Bounce-Port	909
Stacking Guidelines for CoA-Request Disable-Port	910
How to Configure RADIUS Change-of-Authorization	910

Configuring CoA on the Device	910
Monitoring and Troubleshooting CoA Functionality	912
Additional References for RADIUS Change-of-Authorization	913
Feature Information for RADIUS Change-of-Authorization Support	913

CHAPTER 47

Configuring Kerberos 915

Finding Feature Information	915
Prerequisites for Controlling Switch Access with Kerberos	915
Information About Kerberos	916
Kerberos and Switch Access	916
Kerberos Overview	916
Kerberos Operation	918
Kerberos Operation	918
Authenticating to a Boundary Switch	918
Obtaining a TGT from a KDC	919
Authenticating to Network Services	919
How to Configure Kerberos	920
Configuring the KDC Using Kerberos Commands	920
Adding Users to the KDC Database	921
Creating and Extracting a SRVTAB on the KDC	921
Configuring the Device to Use the Kerberos Protocol	922
Configuration Examples for Kerberos	926
Example: Defining a Kerberos Realm	926
Example: Copying a SRVTAB File	927
Example: Configuring Kerberos	927
Example: Encrypting a Telnet Session	936
Additional References	936
Feature Information for Kerberos	937

CHAPTER 48

Configuring Accounting 939

Prerequisites for Configuring Accounting	939
Restrictions for Configuring Accounting	939
Information About Configuring Accounting	940
Named Method Lists for Accounting	940

Method Lists and Server Groups	941
AAA Accounting Methods	941
Accounting Record Types	942
AAA Accounting Methods	942
AAA Accounting Types	942
Network Accounting	942
EXEC Accounting	945
Command Accounting	946
Connection Accounting	947
System Accounting	948
Resource Accounting	949
VRRS Accounting	951
AAA Accounting Enhancements	952
AAA Broadcast Accounting	952
AAA Session MIB	952
Accounting Attribute-Value Pairs	953
How to Configure Accounting	953
Configuring AAA Accounting Using Named Method Lists	953
Configuring RADIUS System Accounting	954
Suppressing Generation of Accounting Records for Null Username Sessions	956
Generating Interim Accounting Records	956
Generating Accounting Records for Failed Login or Session	956
Specifying Accounting NETWORK-Stop Records Before EXEC-Stop Records	957
Configuring AAA Resource Failure Stop Accounting	957
Configuring AAA Resource Accounting for Start-Stop Records	957
Configuring AAA Broadcast Accounting	958
Configuring Per-DNIS AAA Broadcast Accounting	958
Configuring AAA Session MIB	958
Configuring VRRS Accounting	959
Establishing a Session with a Device if the AAA Server is Unreachable	960
Monitoring Accounting	961
Troubleshooting Accounting	961
Configuration Examples for Accounting	961
Example Configuring Named Method List	961

Example Configuring AAA Resource Accounting	964
Example Configuring AAA Broadcast Accounting	964
Example Configuring Per-DNIS AAA Broadcast Accounting	964
Example AAA Session MIB	965
Example Configuring VRRS Accounting	965
Additional References for Configuring Accounting	966
Feature Information for Configuring Accounting	966

CHAPTER 49

Configuring Local Authentication and Authorization	969
How to Configure Local Authentication and Authorization	969
Configuring the Switch for Local Authentication and Authorization	969
Monitoring Local Authentication and Authorization	971
Additional References	971
Feature Information for Local Authentication and Authorization	972

CHAPTER 50

MAC Authentication Bypass	973
Prerequisites for Configuring MAC Authentication Bypass	973
Information About MAC Authentication Bypass	974
Overview of the Cisco IOS Auth Manager	974
Overview of the Configurable MAB Username and Password	974
How to Configure MAC Authentication Bypass	975
Enabling MAC Authentication Bypass	975
Enabling Reauthentication on a Port	976
Specifying the Security Violation Mode	978
Enabling Configurable MAB Username and Password	979
Configuration Examples for MAC Authentication Bypass	980
Example: MAC Authentication Bypass Configuration	980
Example: Enabling Configurable MAB Username and Password	980
Additional References for MAC Authentication Bypass	980
Feature Information for MAC Authentication Bypass	981

CHAPTER 51

Password Strength and Management for Common Criteria	983
Restrictions for Password Strength and Management for Common Criteria	983
Information About Password Strength and Management for Common Criteria	983

Password Composition Policy	983
Password Length Policy	984
Password Lifetime Policy	984
Password Expiry Policy	984
Password Change Policy	984
User Reauthentication Policy	985
Support for Framed (Noninteractive) Session	985
How to Configure Password Strength and Management for Common Criteria	985
Configuring the Password Security Policy	985
Verifying the Common Criteria Policy	987
Configuration Examples for Password Strength and Management for Common Criteria	988
Example: Password Strength and Management for Common Criteria	988
Additional References for Password Strength and Management for Common Criteria	989
Feature Information for Password Strength and Management for Common Criteria	989

CHAPTER 52

AAA-SERVER-MIB Set Operation	991
Prerequisites for AAA-SERVER-MIB Set Operation	991
Restrictions for AAA-SERVER-MIB Set Operation	991
Information About AAA-SERVER-MIB Set Operation	991
CISCO-AAA-SERVER-MIB	991
CISCO-AAA-SERVER-MIB Set Operation	992
How to Configure AAA-SERVER-MIB Set Operation	992
Configuring AAA-SERVER-MIB Set Operations	992
Verifying SNMP Values	992
Configuration Examples for AAA-SERVER-MIB Set Operation	993
RADIUS Server Configuration and Server Statistics Example	993
Additional References for AAA-SERVER-MIB Set Operation	995
Feature Information for AAA-SERVER-MIB Set Operation	995

CHAPTER 53

Configuring Secure Shell	997
Prerequisites for Configuring Secure Shell	997
Restrictions for Configuring Secure Shell	998
Information About Configuring Secure Shell	998
SSH and Device Access	998

SSH Servers, Integrated Clients, and Supported Versions	998
RSA Authentication Support	999
SSL Configuration Guidelines	999
Secure Copy Protocol Overview	999
Secure Copy Protocol	1000
How Secure Copy Works	1000
Reverse Telnet	1000
Reverse SSH	1000
How to Configure Secure Shell	1001
Setting Up the Device to Run SSH	1001
Configuring the SSH Server	1002
Invoking an SSH Client	1004
Troubleshooting Tips	1005
Configuring Reverse SSH for Console Access	1005
Configuring Reverse SSH for Modem Access	1007
Troubleshooting Reverse SSH on the Client	1008
Troubleshooting Reverse SSH on the Server	1009
Monitoring the SSH Configuration and Status	1009
Configuring Secure Copy	1010
Configuration Examples for Secure Shell	1011
Example: Secure Copy Configuration Using Local Authentication	1011
Example: SCP Server-Side Configuration Using Network-Based Authentication	1011
Example Reverse SSH Console Access	1012
Example Reverse SSH Modem Access	1012
Example: Monitoring the SSH Configuration and Status	1012
Additional References for Secure Shell	1013
Feature Information for Configuring Secure Shell	1013

CHAPTER 54

Secure Shell Version 2 Support	1015
Information About Secure Shell Version 2 Support	1015
Secure Shell Version 2	1015
Secure Shell Version 2 Enhancements	1016
Secure Shell Version 2 Enhancements for RSA Keys	1016
SNMP Trap Generation	1017

SSH Keyboard Interactive Authentication	1018
How to Configure Secure Shell Version 2 Support	1018
Configuring a Device for SSH Version 2 Using a Hostname and Domain Name	1018
Configuring a Device for SSH Version 2 Using RSA Key Pairs	1019
Configuring the Cisco SSH Server to Perform RSA-Based User Authentication	1020
Configuring the Cisco IOS SSH Client to Perform RSA-Based Server Authentication	1022
Starting an Encrypted Session with a Remote Device	1024
Enabling Secure Copy Protocol on the SSH Server	1024
Verifying the Status of the Secure Shell Connection	1026
Verifying the Secure Shell Status	1027
Monitoring and Maintaining Secure Shell Version 2	1028
Configuration Examples for Secure Shell Version 2 Support	1031
Example: Configuring Secure Shell Version 2	1031
Example: Starting an Encrypted Session with a Remote Device	1031
Example: Configuring Server-Side SCP	1032
Example: Setting an SNMP Trap	1032
Examples: SSH Keyboard Interactive Authentication	1033
Example: Enabling Client-Side Debugs	1033
Example: Enabling ChPass with a Blank Password Change	1033
Example: Enabling ChPass and Changing the Password on First Login	1034
Example: Enabling ChPass and Expiring the Password After Three Logins	1034
Example: SNMP Debugging	1035
Examples: SSH Debugging Enhancements	1035
Additional References for Secure Shell Version 2 Support	1036
Feature Information for Secure Shell Version 2 Support	1037

CHAPTER 55

Configuring SSH File Transfer Protocol	1039
Prerequisites for SSH File Transfer Protocol	1039
Restrictions for SSH File Transfer Protocol	1039
Information About SSH File Transfer Protocol	1039
How to Configure SSH File Transfer Protocol	1040
Configuring SFTP	1040
Perform an SFTP Copy Operation	1041
Example: Configuring SSH File Transfer Protocol	1041

Additional References	1041
Feature Information for SSH File Transfer Protocol	1042

CHAPTER 56

X.509v3 Certificates for SSH Authentication	1043
Prerequisites for X.509v3 Certificates for SSH Authentication	1043
Restrictions for X.509v3 Certificates for SSH Authentication	1043
Information About X.509v3 Certificates for SSH Authentication	1044
X.509v3 Certificates for SSH Authentication Overview	1044
Server and User Authentication Using X.509v3	1044
OCSP Response Stapling	1044
How to Configure X.509v3 Certificates for SSH Authentication	1045
Configuring Digital Certificates for Server Authentication	1045
Configuring Digital Certificates for User Authentication	1046
Verifying the Server and User Authentication Using Digital Certificates	1048
Configuration Examples for X.509v3 Certificates for SSH Authentication	1052
Example: Configuring Digital Certificates for Server Authentication	1052
Example: Configuring Digital Certificate for User Authentication	1052
Additional References for X.509v3 Certificates for SSH Authentication	1053
Feature Information for X.509v3 Certificates for SSH Authentication	1053

CHAPTER 57

Configuring Secure Socket Layer HTTP	1055
Information About Secure Socket Layer HTTP	1055
Secure HTTP Servers and Clients Overview	1055
Certificate Authority Trustpoints	1056
CipherSuites	1057
Default SSL Configuration	1058
SSL Configuration Guidelines	1058
How to Configure Secure Socket Layer HTTP	1058
Configuring the Secure HTTP Server	1058
Configuring the Secure HTTP Client	1062
Configuring a CA Trustpoint	1063
Monitoring Secure HTTP Server and Client Status	1065
Configuration Examples for Secure Socket Layer HTTP	1065
Example: Configuring Secure Socket Layer HTTP	1065

Additional References for Secure Socket Layer HTTP 1067

Feature Information for Secure Socket Layer HTTP 1067

Glossary 1067

CHAPTER 58

Certification Authority Interoperability 1069

Prerequisites For Certification Authority 1069

Restrictions for Certification Authority 1069

Information About Certification Authority 1069

CA Supported Standards 1069

Purpose of CAs 1070

Implementing IPsec Without CAs 1071

Implementing IPsec With CAs 1071

Implementing IPsec with Multiple Root CAs 1071

How CA Certificates Are Used by IPsec Devices 1072

Registration Authorities 1072

How to Configure Certification Authority 1072

Managing NVRAM Memory Usage 1072

Configuring the Device Host Name and IP Domain Name 1073

Generating an RSA Key Pair 1074

Declaring a Certification Authority 1075

Configuring a Root CA (Trusted Root) 1076

Authenticating the CA 1077

Requesting Signed Certificates 1078

Monitoring and Maintaining Certification Authority 1079

Requesting a Certificate Revocation List 1079

Querying a Certification Revocation List 1079

Deleting RSA Keys from a Device 1080

Deleting Public Keys for a Peer 1081

Deleting Certificates from the Configuration 1082

Viewing Keys and Certificates 1083

CHAPTER 59

Access Control List Overview 1085

Information About Access Control Lists 1085

Definition of an Access List 1085

Functions of an Access Control List	1086
Purpose of IP Access Lists	1086
Reasons to Configure ACLs	1086
Software Processing of an Access List	1087
Access List Rules	1087
Helpful Hints for Creating IP Access Lists	1088
IP Packet Fields You Can Filter to Control Access	1089
Source and Destination Addresses	1089
Wildcard Mask for Addresses in an Access List	1089
Access List Sequence Numbers	1090
ACL Supported Types	1090
Supported ACLs	1091
ACL Precedence	1091
Port ACLs	1091
Router ACLs	1092
Access Control Entries	1093
ACEs and Fragmented and Unfragmented Traffic	1093
ACEs and Fragmented and Unfragmented Traffic Examples	1093

CHAPTER 60

Configuring IPv4 Access Control Lists	1095
Prerequisites for Configuring IPv4 Access Control Lists	1095
Restrictions for Configuring IPv4 Access Control Lists	1095
Information About Configuring IPv4 Access Control Lists	1096
ACL Overview	1096
Standard and Extended IPv4 ACLs	1097
IPv4 ACL Switch Unsupported Features	1097
Access List Numbers	1097
Numbered Standard IPv4 ACLs	1098
Numbered Extended IPv4 ACLs	1098
Named IPv4 ACLs	1099
Benefits of IP Access List Entry Sequence Numbering	1100
Sequence Numbering Behavior	1100
Including comments in ACLs	1101
Hardware and Software Treatment of IP ACLs	1101

Time Ranges for ACLs	1102
IPv4 ACL Interface Considerations	1102
Apply an Access Control List to an Interface	1103
ACL Logging	1104
How to Configure ACLs	1104
Configuring IPv4 ACLs	1104
Creating a Numbered Standard ACL	1104
Creating a Numbered Extended ACL (CLI)	1106
Creating Named Standard ACLs	1109
Creating Extended Named ACLs	1111
Configuring an Access Control Entry with Noncontiguous Ports	1112
Consolidating Access List Entries with Noncontiguous Ports into One Access List Entry	1114
Sequencing Access-List Entries and Revising the Access List	1115
Configuring Commented IP ACL Entries	1118
Configuring Time Ranges for ACLs	1119
Applying an IPv4 ACL to a Terminal Line	1120
Applying an IPv4 ACL to an Interface (CLI)	1122
Monitoring IPv4 ACLs	1123
Configuration Examples for ACLs	1124
ACLs in a Small Networked Office	1124
Example: Numbered ACLs	1124
Examples: Extended ACLs	1125
Examples: Named ACLs	1125
Example: Configuring an Access Control Entry with Noncontiguous Ports	1126
Example: Consolidating Access List Entries with Noncontiguous Ports into One Access List Entry	1126
Example Resequencing Entries in an Access List	1127
Example Adding an Entry with a Sequence Number	1128
Example Adding an Entry with No Sequence Number	1128
Examples: Configuring Commented IP ACL Entries	1128
Examples: Using Time Ranges with ACLs	1129
Examples: Time Range Applied to an IP ACL	1130
Examples: ACL Logging	1130
Examples: Troubleshooting ACLs	1131

Additional References	1133
Feature Information for IPv4 Access Control Lists	1133

CHAPTER 61

IPv6 Access Control Lists	1135
Prerequisites for IPv6 ACLs	1135
Restrictions for IPv6 ACLs	1135
Information About Configuring IPv6 ACLs	1136
ACL Overview	1136
IPv6 ACLs Overview	1137
Understanding IPv6 ACLs	1137
Interactions with Other Features and Switches	1138
Default Configuration for IPv6 ACLs	1138
Supported ACL Features	1139
IPv6 Port-Based Access Control List Support	1139
ACLs and Traffic Forwarding	1139
How to Configure IPv6 ACLs	1139
Configuring IPv6 ACLs	1139
Attaching an IPv6 ACL to an Interface	1143
Monitoring IPv6 ACLs	1144
Configuring PACL Mode and Applying IPv6 PACL on an Interface	1145
Configuring IPv6 ACL Extensions for Hop by Hop Filtering	1146
Configuration Examples for IPv6 ACLs	1147
Example: Configuring IPv6 ACLs	1147
Example: Applying IPv6 ACLs	1148
Example: Configuring PACL Mode and Applying IPv6 PACL on an Interface	1148
Example: IPv6 ACL Extensions for Hop by Hop Filtering	1148
Additional References	1149
Feature Information for IPv6 Access Control Lists	1149

CHAPTER 62

ACL Support for Filtering IP Options	1151
Prerequisites for ACL Support for Filtering IP Options	1151
Information About ACL Support for Filtering IP Options	1151
IP Options	1151
Benefits of Filtering IP Options	1152

Benefits of Filtering on TCP Flags	1152
TCP Flags	1152
How to Configure ACL Support for Filtering IP Options	1153
Filtering Packets That Contain IP Options	1153
Filtering Packets That Contain TCP Flags	1154
Configuration Examples for ACL Support for Filtering IP Options	1156
Example: Filtering Packets That Contain IP Options	1156
Example: Filtering Packets That Contain TCP Flags	1157
Additional References for ACL Support for Filtering IP Options	1157
Feature Information for Creating an IP Access List to Filter	1158

CHAPTER 63
VLAN Access Control Lists 1159

Information About VLAN Access Control Lists	1159
VLAN Maps	1159
VLAN Map Configuration Guidelines	1160
VLAN Maps with Router ACLs	1160
VLAN Maps and Router ACL Configuration Guidelines	1161
How to Configure VLAN Access Control Lists	1161
Creating Named MAC Extended ACLs	1161
Applying a MAC ACL to a Layer 2 Interface	1163
Configuring VLAN Maps	1164
Creating a VLAN Map	1166
Applying a VLAN Map to a VLAN	1167
Configuration Examples for ACLs and VLAN Maps	1168
Example: Creating an ACL and a VLAN Map to Deny a Packet	1168
Example: Creating an ACL and a VLAN Map to Permit a Packet	1168
Example: Default Action of Dropping IP Packets and Forwarding MAC Packets	1169
Example: Default Action of Dropping MAC Packets and Forwarding IP Packets	1169
Example: Default Action of Dropping All Packets	1170
Configuration Examples for Using VLAN Maps in Your Network	1170
Example: Wiring Closet Configuration	1170
Example: Restricting Access to a Server on Another VLAN	1172
Example: Denying Access to a Server on Another VLAN	1172
Configuration Examples of Router ACLs and VLAN Maps Applied to VLANs	1173

Example: ACLs and Switched Packets 1173

Example: ACLs and Bridged Packets 1173

Example: ACLs and Routed Packets 1174

Example: ACLs and Multicast Packets 1175

CHAPTER 64

Configuring DHCP 1177

Restrictions for DHCP 1177

Information About DHCP 1177

DHCP Server 1177

DHCP Relay Agent 1177

DHCP Snooping 1178

Option-82 Data Insertion 1179

Cisco IOS DHCP Server Database 1182

DHCP Snooping Binding Database 1182

DHCP Snooping and Switch Stacks 1183

How to Configure DHCP Features 1184

Default DHCP Snooping Configuration 1184

DHCP Snooping Configuration Guidelines 1185

Configuring the DHCP Server 1185

DHCP Server and Switch Stacks 1185

Configuring the DHCP Relay Agent 1185

Specifying the Packet Forwarding Address 1186

Prerequisites for Configuring DHCP Snooping and Option 82 1188

Enabling DHCP Snooping and Option 82 1189

Enabling the Cisco IOS DHCP Server Database 1192

Monitoring DHCP Snooping Information 1192

Configuring DHCP Server Port-Based Address Allocation 1193

Information About Configuring DHCP Server Port-Based Address Allocation 1193

Default Port-Based Address Allocation Configuration 1193

Port-Based Address Allocation Configuration Guidelines 1193

Enabling the DHCP Snooping Binding Database Agent 1193

Enabling DHCP Server Port-Based Address Allocation 1195

Monitoring DHCP Server Port-Based Address Allocation 1197

Additional References 1197

Feature Information for DHCP Snooping and Option 82 1197

CHAPTER 65

Configuring IP Source Guard 1199

Information About IP Source Guard 1199

IP Source Guard 1199

IP Source Guard for Static Hosts 1199

IP Source Guard Configuration Guidelines 1200

How to Configure IP Source Guard 1201

Enabling IP Source Guard 1201

Configuring IP Source Guard for Static Hosts on a Layer 2 Access Port 1202

Monitoring IP Source Guard 1204

Additional References 1205

CHAPTER 66

Configuring Dynamic ARP Inspection 1207

Restrictions for Dynamic ARP Inspection 1207

Understanding Dynamic ARP Inspection 1208

Interface Trust States and Network Security 1210

Rate Limiting of ARP Packets 1211

Relative Priority of ARP ACLs and DHCP Snooping Entries 1211

Logging of Dropped Packets 1211

Default Dynamic ARP Inspection Configuration 1212

Relative Priority of ARP ACLs and DHCP Snooping Entries 1212

Configuring ARP ACLs for Non-DHCP Environments 1212

Configuring Dynamic ARP Inspection in DHCP Environments 1215

Limiting the Rate of Incoming ARP Packets 1217

Performing Dynamic ARP Inspection Validation Checks 1219

Monitoring DAI 1221

Verifying the DAI Configuration 1221

Additional References 1222

CHAPTER 67

Configuring IEEE 802.1x Port-Based Authentication 1223

Information About 802.1x Port-Based Authentication 1223

Port-Based Authentication Process 1224

Port-Based Authentication Initiation and Message Exchange 1226

Authentication Manager for Port-Based Authentication	1228
Port-Based Authentication Methods	1228
Per-User ACLs and Filter-Ids	1228
Port-Based Authentication Manager CLI Commands	1229
Ports in Authorized and Unauthorized States	1230
Port-Based Authentication and Switch Stacks	1231
802.1x Host Mode	1232
802.1x Multiple Authentication Mode	1232
Multi-auth Per User VLAN assignment	1233
MAC Move	1234
MAC Replace	1235
802.1x Accounting	1235
802.1x Accounting Attribute-Value Pairs	1236
802.1x Readiness Check	1237
Switch-to-RADIUS-Server Communication	1237
802.1x Authentication with VLAN Assignment	1237
802.1x Authentication with Per-User ACLs	1239
802.1x Authentication with Downloadable ACLs and Redirect URLs	1240
Cisco Secure ACS and Attribute-Value Pairs for the Redirect URL	1241
Cisco Secure ACS and Attribute-Value Pairs for Downloadable ACLs	1242
VLAN ID-Based MAC Authentication	1242
802.1x Authentication with Guest VLAN	1242
802.1x Authentication with Restricted VLAN	1243
802.1x Authentication with Inaccessible Authentication Bypass	1244
Inaccessible Authentication Bypass Support on Multiple-Authentication Ports	1245
Inaccessible Authentication Bypass Authentication Results	1245
Inaccessible Authentication Bypass Feature Interactions	1245
802.1x Critical Voice VLAN	1246
802.1x User Distribution	1247
802.1x User Distribution Configuration Guidelines	1247
IEEE 802.1x Authentication with Voice VLAN Ports	1248
IEEE 802.1x Authentication with Port Security	1248
IEEE 802.1x Authentication with Wake-on-LAN	1248
IEEE 802.1x Authentication with MAC Authentication Bypass	1249

Network Admission Control Layer 2 IEEE 802.1x Validation	1250
Flexible Authentication Ordering	1250
Open1x Authentication	1251
Multidomain Authentication	1251
Limiting Login for Users	1253
802.1x Supplicant and Authenticator Switches with Network Edge Access Topology (NEAT)	1253
Voice Aware 802.1x Security	1254
Common Session ID	1255
How to Configure 802.1x Port-Based Authentication	1256
Default 802.1x Authentication Configuration	1256
802.1x Authentication Configuration Guidelines	1257
802.1x Authentication	1257
VLAN Assignment, Guest VLAN, Restricted VLAN, and Inaccessible Authentication Bypass	1258
MAC Authentication Bypass	1259
Maximum Number of Allowed Devices Per Port	1259
Configuring 802.1x Readiness Check	1259
Configuring Voice Aware 802.1x Security	1261
Configuring 802.1x Violation Modes	1263
Configuring 802.1x Authentication	1264
Configuring 802.1x Port-Based Authentication	1265
Configuring the Switch-to-RADIUS-Server Communication	1267
Configuring the Host Mode	1268
Configuring Periodic Re-Authentication	1269
Changing the Quiet Period	1271
Changing the Switch-to-Client Retransmission Time	1272
Setting the Switch-to-Client Frame-Retransmission Number	1273
Setting the Re-Authentication Number	1274
Enabling MAC Move	1275
Disabling MAC Move	1276
Enabling MAC Replace	1277
Configuring 802.1x Accounting	1278
Configuring a Guest VLAN	1279
Configuring a Restricted VLAN	1280
Configuring Number of Authentication Attempts on a Restricted VLAN	1282

Configuring 802.1x Inaccessible Authentication Bypass with Critical Voice VLAN	1283
Example of Configuring Inaccessible Authentication Bypass	1286
Configuring 802.1x Authentication with WoL	1287
Configuring MAC Authentication Bypass	1288
Formatting a MAC Authentication Bypass Username and Password	1289
Configuring 802.1x User Distribution	1290
Example of Configuring VLAN Groups	1291
Configuring NAC Layer 2 802.1x Validation	1291
Configuring Limiting Login for Users	1293
Configuring an Authenticator Switch with NEAT	1294
Configuring a Supplicant Switch with NEAT	1296
Configuring 802.1x Authentication with Downloadable ACLs and Redirect URLs	1298
Configuring Downloadable ACLs	1298
Configuring a Downloadable Policy	1300
Configuring VLAN ID-based MAC Authentication	1302
Configuring Flexible Authentication Ordering	1303
Configuring Open1x	1304
Disabling 802.1x Authentication on the Port	1306
Resetting the 802.1x Authentication Configuration to the Default Values	1306
Monitoring 802.1x Statistics and Status	1307
Additional References for IEEE 802.1x Port-Based Authentication	1308
Feature Information for 802.1x Port-Based Authentication	1309

CHAPTER 68
Configuring Web-Based Authentication 1311

Information About Web-Based Authentication	1311
Web-Based Authentication Overview	1311
Device Roles	1312
Host Detection	1313
Session Creation	1313
Authentication Process	1314
Using Authentication Proxy	1314
When to Use the Authentication Proxy	1315
Applying Authentication Proxy	1315
Local Web Authentication Banner	1316

Web Authentication Customizable Web Pages	1319
Web Authentication Redirection to Original URL Overview	1321
Web-based Authentication Interactions with Other Features	1323
Default Web-Based Authentication Configuration	1325
Web-Based Authentication Configuration Guidelines and Restrictions	1325
How to Configure Web-Based Authentication	1326
Configuring the Authentication Rule and Interfaces	1326
Configuring AAA Authentication	1328
Configuring Switch-to-RADIUS-Server Communication	1329
Configuring the HTTP Server	1330
Customizing the Authentication Proxy Web Pages	1331
Specifying a Redirection URL for Successful Login	1333
Configuring Web-Based Authentication Parameters	1333
Configuring a Web Authentication Local Banner	1334
Configuring Web-Based Authentication without SVI	1335
Configuring Web-Based Authentication with VRF Aware	1336
Removing Web-Based Authentication Cache Entries	1337
Verifying Web-Based Authentication Status	1338
Displaying Web-Based Authentication Status	1338
Monitoring HTTP Authentication Proxy	1339
Verifying HTTPS Authentication Proxy	1339
Configuration Examples for Web-Based Authentication	1340
Example: Configuring the Authentication Rule and Interfaces	1340
Example: AAA Configuration	1340
Example: HTTP Server Configuration	1341
Example: Customizing the Authentication Proxy Web Pages	1341
Example: Specifying a Redirection URL for Successful Login	1341
Additional References for Web-Based Authentication	1342
Feature Information for Web-Based Authentication	1342

CHAPTER 69
Auto Identity 1343

Auto Identity	1343
Information About Auto Identity	1343
Auto Identity Overview	1343

Auto Identity Global Template	1344
Auto Identity Interface Templates	1344
Auto Identity Built-in Policies	1345
Auto Identity Class Maps Templates	1345
Auto Identity Parameter Maps	1346
Auto Identity Service Templates	1346
How to Configure Auto Identity	1346
Configuring Auto Identity Globally	1346
Configuring Auto Identity at an Interface Level	1347
Configuration Examples for Auto Identity	1349
Example: Configuring Auto Identity Globally	1349
Example: Configuring Auto Identity at an Interface Level	1349
Verifying Auto Identity	1349
Feature Information for Auto Identity	1352

CHAPTER 70

Configuring Port-Based Traffic Control	1355
Overview of Port-Based Traffic Control	1356
Finding Feature Information	1356
Information About Storm Control	1356
Storm Control	1356
How Traffic Activity is Measured	1356
Traffic Patterns	1357
How to Configure Storm Control	1358
Configuring Storm Control and Threshold Levels	1358
Configuring Small-Frame Arrival Rate	1360
Finding Feature Information	1362
Information About Protected Ports	1362
Protected Ports	1362
Default Protected Port Configuration	1363
Protected Ports Guidelines	1363
How to Configure Protected Ports	1363
Configuring a Protected Port	1363
Monitoring Protected Ports	1365
Where to Go Next	1365

Additional References	1365
Feature Information	1366
Finding Feature Information	1366
Information About Port Blocking	1366
Port Blocking	1366
How to Configure Port Blocking	1366
Blocking Flooded Traffic on an Interface	1366
Monitoring Port Blocking	1368
Where to Go Next	1368
Additional References	1368
Feature Information	1369
Prerequisites for Port Security	1369
Restrictions for Port Security	1369
Information About Port Security	1370
Port Security	1370
Types of Secure MAC Addresses	1370
Sticky Secure MAC Addresses	1370
Security Violations	1371
Port Security Aging	1372
Port Security and Switch Stacks	1372
Default Port Security Configuration	1372
Port Security Configuration Guidelines	1373
Overview of Port-Based Traffic Control	1374
How to Configure Port Security	1374
Enabling and Configuring Port Security	1374
Enabling and Configuring Port Security Aging	1380
Configuration Examples for Port Security	1381
Additional References	1382
Finding Feature Information	1383
Information About Protocol Storm Protection	1383
Protocol Storm Protection	1383
Default Protocol Storm Protection Configuration	1383
How to Configure Protocol Storm Protection	1384
Enabling Protocol Storm Protection	1384

Monitoring Protocol Storm Protection 1385

Additional References 1385

CHAPTER 71

Configuring FIPS 1387

Information About FIPS and Common Criteria 1387

CHAPTER 72

Configuring Control Plane Policing 1389

Restrictions for Control Plane Policing 1389

Control Plane Policing 1389

Configuring Control Plane Policing 1390

Examples: Configuring CoPP 1391

PART XI

Configuring Cisco IOS IP SLAs 1393

CHAPTER 73

Configuring Cisco IP SLAs 1395

Restrictions on SLAs 1395

Information About SLAs 1395

Cisco IOS IP Service Level Agreements (SLAs) 1395

Network Performance Measurement with Cisco IOS IP SLAs 1396

IP SLA Responder and IP SLA Control Protocol 1397

Response Time Computation for IP SLAs 1398

How to Configure IP SLAs Operations 1399

Default Configuration 1399

Configuration Guidelines 1399

Configuring the IP SLA Responder 1399

Monitoring IP SLA Operations 1400

Additional References 1401

Feature History and Information for Service Level Agreements 1402

PART XII

Stacking 1403

CHAPTER 74

Managing Switch Stacks 1405

Prerequisites for Switch Stacks 1405

Restrictions for Switch Stacks 1405

Information About Switch Stacks	1406
Switch Stack Overview	1406
Supported Features in a Switch Stack	1406
Switch Stack Membership	1407
Changes to Switch Stack Membership	1408
Stack Member Numbers	1408
Stack Member Priority Values	1410
Switch Stack Bridge ID and MAC Address	1410
Persistent MAC Address on the Switch Stack	1410
Active and Standby Switch Election and Reelection	1411
Switch Stack Configuration Files	1412
Offline Configuration to Provision a Stack Member	1413
Effects of Adding a Provisioned Switch to a Switch Stack	1414
Effects of Replacing a Provisioned Switch in a Switch Stack	1415
Effects of Removing a Provisioned Switch from a Switch Stack	1415
Stack Protocol Version	1415
Major Stack Protocol Version Number Incompatibility Among Stack-Capable Switches	1415
Minor Stack Protocol Version Number Incompatibility Among Stack-Capable Switches	1415
Auto-Upgrade	1416
Auto-Advise	1416
SDM Template Mismatch in Switch Stacks	1419
Switch Stack Management Connectivity	1419
Connectivity to Specific Stack Members	1419
Connectivity to the Switch Stack Through an IP Address	1420
Connectivity to the Switch Stack Through Console Ports or Ethernet Management Ports	1420
How to Configure a Switch Stack	1421
Enabling the Persistent MAC Address Feature	1421
Assigning a Stack Member Number	1422
Setting the Stack Member Priority Value	1423
Setting the Stack Port Speed to 10 Gbps	1424
Provisioning a New Member for a Switch Stack	1425
Removing Provisioned Switch Information	1426
Troubleshooting the Switch Stack	1427
Accessing the CLI of a Specific Member	1427

Temporarily Disabling a Stack Port	1427
Reenabling a Stack Port While Another Member Starts	1428
Monitoring the Device Stack	1429
Configuration Examples for Switch Stacks	1429
Switch Stack Configuration Scenarios	1429
Enabling the Persistent MAC Address Feature: Example	1431
Provisioning a New Member for a Switch Stack: Example	1431
Additional References for Switch Stacks	1432

CHAPTER 75

FlexStack-Extended 1433

Restrictions for FlexStack-Extended	1433
Information About FlexStack-Extended	1433
FlexStack-Extended	1433
FlexStack-Extended on Catalyst 2960-X and 2960-XR Switches	1434
Default Port Configurations	1435
FlexStack-Extended LED	1436
How to Configure FlexStack-Extended	1436
Configuring a Stack Port as a Network Port	1436
Configuring a Network Port as a Stack Port	1437
Configuring the Stack Speed	1439
Configuration Examples for FlexStack-Extended	1439
Examples: Configuring FlexStack-Extended	1439
Feature Information for FlexStack-Extended	1440

PART XIII

System Management 1441

CHAPTER 76

Administering the System 1443

Information About Administering the Device	1443
System Time and Date Management	1443
System Clock	1443
Real Time Clock	1444
Network Time Protocol	1444
NTP Stratum	1445
NTP Associations	1446

NTP Security	1446
NTP Implementation	1446
NTP Version 4	1447
System Name and Prompt	1447
Stack System Name and Prompt	1447
Default System Name and Prompt Configuration	1447
DNS	1448
Default DNS Settings	1448
Login Banners	1448
Default Banner Configuration	1448
MAC Address Table	1448
MAC Address Table Creation	1449
MAC Addresses and VLANs	1449
Default MAC Address Table Settings	1449
ARP Table Management	1450
How to Administer the Device	1450
Configuring the Time and Date Manually	1450
Setting the System Clock	1450
Configuring the Time Zone	1451
Configuring Summer Time (Daylight Saving Time)	1452
Configuring a System Name	1455
Setting Up DNS	1456
Configuring a Message-of-the-Day Login Banner	1457
Configuring a Login Banner	1458
Managing the MAC Address Table	1460
Changing the Address Aging Time	1460
Configuring MAC Address Change Notification Traps	1461
Configuring MAC Address Move Notification Traps	1463
Configuring MAC Threshold Notification Traps	1465
Adding and Removing Static Address Entries	1466
Configuring Unicast MAC Address Filtering	1467
Monitoring and Maintaining Administration of the Device	1468
Configuration Examples for Device Administration	1469
Example: Setting the System Clock	1469

Examples: Configuring Summer Time	1470
Example: Configuring a MOTD Banner	1470
Example: Configuring a Login Banner	1470
Example: Configuring MAC Address Change Notification Traps	1471
Example: Configuring MAC Threshold Notification Traps	1471
Example: Adding the Static Address to the MAC Address Table	1471
Example: Configuring Unicast MAC Address Filtering	1472
Additional References for Switch Administration	1472
Feature History and Information for Device Administration	1473

CHAPTER 77

Performing Device Setup Configuration 1475

Information About Performing Device Setup Configuration	1475
Boot Process	1475
Devices Information Assignment	1476
Default Switch Information	1476
DHCP-Based Autoconfiguration Overview	1477
DHCP Client Request Process	1477
DHCP-based Autoconfiguration and Image Update	1478
Restrictions for DHCP-based Autoconfiguration	1478
DHCP Autoconfiguration	1479
DHCP Auto-Image Update	1479
DHCP Server Configuration Guidelines	1479
Purpose of the TFTP Server	1480
Purpose of the DNS Server	1481
How to Obtain Configuration Files	1481
How to Control Environment Variables	1482
Common Environment Variables	1483
Environment Variables for TFTP	1485
Scheduled Reload of the Software Image	1485
How to Perform Device Setup Configuration	1486
Configuring DHCP Autoconfiguration (Only Configuration File)	1486
Configuring DHCP Auto-Image Update (Configuration File and Image)	1488
Configuring the Client to Download Files from DHCP Server	1490
Manually Assigning IP Information to Multiple SVIs	1491

Configuring the NVRAM Buffer Size	1493
Modifying the Device Startup Configuration	1494
Specifying the Filename to Read and Write the System Configuration	1494
Manually Booting the Switch	1495
Configuring a Scheduled Software Image Reload	1496
Monitoring Device Setup Configuration	1497
Example: Verifying the Device Running Configuration	1497
Examples: Displaying Software Install	1498
Configuration Examples for Performing Device Setup	1498
Example: Configuring a Device as a DHCP Server	1498
Example: Configuring DHCP Auto-Image Update	1498
Example: Configuring a Device to Download Configurations from a DHCP Server	1498
Example: Configuring NVRAM Buffer Size	1499
Additional References for Performing Switch Setup	1500
Feature History and Information For Performing Device Setup Configuration	1501

CHAPTER 78

Configuring AVC with DNS-AS	1503
Prerequisites for AVC with DNS-AS	1503
Restrictions and Guidelines for AVC with DNS-AS	1503
Information About AVC with DNS-AS	1504
Overview of AVC with DNS-AS	1504
Key Concepts for AVC with DNS-AS	1505
AVC with DNS-AS Process Flow	1506
DNS Snooping Process	1506
DNS-AS Client Process	1507
Figure: AVC with DNS-AS Process Flow	1507
Stacking and AVC with DNS-AS	1508
Default Configuration for AVC with DNS-AS	1508
How to Configure AVC with DNS-AS	1508
Generating Metadata Streams	1508
Configuring a DNS Server as the Authoritative Server	1510
Enabling AVC with DNS-AS	1511
Maintaining the List of Trusted Domains	1511
Configuring QoS for AVC with DNS-AS	1512

Configuring FNF for AVC with DNS-AS	1515
Option Templates	1516
Sample FNF Configuration for AVC with DNS-AS	1518
Monitoring AVC with DNS-AS	1521
Troubleshooting AVC with DNS-AS	1524
Feature History and Information for AVC with DNS-AS	1525

CHAPTER 79

Configuring SDM Templates	1527
Finding Feature Information	1527
Information About Configuring SDM Templates	1527
Restrictions for SDM Templates	1527
SDM Templates	1528
Default and LAN Base Templates	1528
SDM Templates and Switch Stacks	1530
How to Configure SDM Templates	1530
Setting the SDM Template	1530
Configuration Examples for SDM Templates	1531
Examples: Displaying SDM Templates	1531
Examples: Configuring SDM Templates	1532
Additional References for SDM Templates	1533
Feature History and Information for Configuring SDM Templates	1534

CHAPTER 80

Configuring System Message Logs	1535
Restrictions for Configuring System Message Logs	1535
Information About Configuring System Message Logs	1535
System Message Logging	1535
System Log Message Format	1536
Default System Message Logging Settings	1537
Enabling Syslog Trap Messages	1537
How to Configure System Message Logs	1538
Setting the Message Display Destination Device	1538
Synchronizing Log Messages	1539
Disabling Message Logging	1541
Enabling and Disabling Time Stamps on Log Messages	1541

Enabling and Disabling Sequence Numbers in Log Messages	1542
Defining the Message Severity Level	1543
Limiting Syslog Messages Sent to the History Table and to SNMP	1544
Logging Messages to a UNIX Syslog Daemon	1544
Monitoring and Maintaining System Message Logs	1546
Monitoring Configuration Archive Logs	1546
Configuration Examples for System Message Logs	1546
Example: Switch System Message	1546
Additional References for System Message Logs	1546
Feature History and Information For System Message Logs	1547

CHAPTER 81
Configuring Online Diagnostics 1549

Information About Configuring Online Diagnostics	1549
Online Diagnostics	1549
How to Configure Online Diagnostics	1550
Starting Online Diagnostic Tests	1550
Configuring Online Diagnostics	1550
Scheduling Online Diagnostics	1550
Configuring Health-Monitoring Diagnostics	1551
Monitoring and Maintaining Online Diagnostics	1554
Displaying Online Diagnostic Tests and Test Results	1554
Configuration Examples for Online Diagnostic Tests	1555
Starting Online Diagnostic Tests	1555
Example: Configure a Health Monitoring Test	1555
Examples: Schedule Diagnostic Test	1556
Displaying Online Diagnostics: Examples	1556
Additional References for Online Diagnostics	1558
Feature History and Information for Configuring Online Diagnostics	1559

CHAPTER 82
Troubleshooting the Software Configuration 1561

Information About Troubleshooting the Software Configuration	1561
Software Failure on a Switch	1561
Lost or Forgotten Password on a Device	1561
Power over Ethernet Ports	1562

Disabled Port Caused by Power Loss	1562
Disabled Port Caused by False Link-Up	1562
Ping	1563
Layer 2 Traceroute	1563
Layer 2 Traceroute Guidelines	1563
IP Traceroute	1564
Time Domain Reflector Guidelines	1565
Debug Commands	1566
Onboard Failure Logging on the Switch	1566
Possible Symptoms of High CPU Utilization	1566
How to Troubleshoot the Software Configuration	1567
Recovering from a Software Failure	1567
Recovering from a Lost or Forgotten Password	1569
Procedure with Password Recovery Enabled	1570
Procedure with Password Recovery Disabled	1572
Recovering from a Command Switch Failure	1574
Replacing a Failed Command Switch with a Cluster Member	1574
Replacing a Failed Command Switch with Another Switch	1576
Preventing Switch Stack Problems	1577
Preventing Autonegotiation Mismatches	1578
Troubleshooting SFP Module Security and Identification	1579
Monitoring SFP Module Status	1579
Executing Ping	1579
Monitoring Temperature	1580
Monitoring the Physical Path	1580
Executing IP Traceroute	1580
Running TDR and Displaying the Results	1581
Redirecting Debug and Error Message Output	1581
Using the show platform forward Command	1581
Configuring OBFL	1581
Verifying Troubleshooting of the Software Configuration	1582
Displaying OBFL Information	1582
Example: Verifying the Problem and Cause for High CPU Utilization	1584
Scenarios for Troubleshooting the Software Configuration	1585

Scenarios to Troubleshoot Power over Ethernet (PoE)	1585
Configuration Examples for Troubleshooting Software	1587
Example: Pinging an IP Host	1587
Example: Performing a Traceroute to an IP Host	1588
Example: Enabling All System Diagnostics	1589
Additional References for Troubleshooting Software Configuration	1589
Feature History and Information for Troubleshooting Software Configuration	1590

CHAPTER 83**Information About Licensing 1591**

Restrictions for Configuring Licenses	1591
Information About Licensing	1591
Overview of License Levels	1591
Base Licenses	1592
Add-On Licenses	1592
License States	1592
Guidelines for License Types	1593
Ordering with Smart Accounts	1593
License Activation for Switch Stacks	1594
How to Configure Add-On License Levels	1594
Activating an Image Based Add-on License	1594
Rehosting a License	1595
Monitoring Licenses	1595
Configuration Examples for License Levels	1596
Reference	1596
Example: Displaying the detailed license information	1596
Example: Displaying a summary of the license information	1596
Example: Displaying the end user license agreement	1597
Feature History for Information About Licensing	1597

PART XIV**Working with the Cisco IOS File System, Configuration Files, and Software Images 1599**

CHAPTER 84**Working with the Cisco IOS File System, Configuration Files, and Software Images 1601**

Working with the Flash File System	1601
Information About the Flash File System	1601

Displaying Available File Systems	1601
Setting the Default File System	1604
Displaying Information About Files on a File System	1604
Changing Directories and Displaying the Working Directory	1605
Creating Directories	1606
Removing Directories	1606
Copying Files	1606
Copying Files from One Device in a Stack to Another Device in the Same Stack	1607
Deleting Files	1608
Creating, Displaying and Extracting Files	1608
Working with Configuration Files	1610
Information on Configuration Files	1610
Guidelines for Creating and Using Configuration Files	1610
Configuration File Types and Location	1611
Creating a Configuration File By Using a Text Editor	1611
Copying Configuration Files By Using TFTP	1612
Preparing to Download or Upload a Configuration File By Using TFTP	1612
Downloading the Configuration File By Using TFTP	1612
Uploading the Configuration File By Using TFTP	1613
Copying a Configuration File from the Device to an FTP Server	1614
Understanding the FTP Username and Password	1614
Preparing to Download or Upload a Configuration File By Using FTP	1614
Downloading a Configuration File By Using FTP	1615
Uploading a Configuration File By Using FTP	1616
Copying Configuration Files By Using RCP	1617
Preparing to Download or Upload a Configuration File By Using RCP	1617
Downloading a Configuration File By Using RCP	1618
Uploading a Configuration File By Using RCP	1619
Clearing Configuration Information	1620
Clearing the Startup Configuration File	1620
Deleting a Stored Configuration File	1620
Replacing and Rolling Back Configurations	1620
Information on Configuration Replacement and Rollback	1621
Configuration Archive	1621

Configuration Replace	1621
Configuration Rollback	1621
Configuration Guidelines	1622
Configuring the Configuration Archive	1622
Performing a Configuration Replacement or Rollback Operation	1623
Working with Software Images	1624
Information on Working with Software Images	1624
Image Location on the Switch	1625
File Format of Images on a Server or Cisco.com	1625
Copying Image Files Using TFTP	1626
Preparing to Download or Upload an Image File By Using TFTP	1627
Downloading an Image File By Using TFTP	1628
Uploading an Image File Using TFTP	1629
Copying Image Files Using FTP	1630
Preparing to Download or Upload an Image File By Using FTP	1630
Downloading an Image File By Using FTP	1631
Uploading an Image File By Using FTP	1633
Copying Image Files Using RCP	1634
Preparing to Download or Upload an Image File Using RCP	1634
Downloading an Image File using RCP	1635
Uploading an Image File using RCP	1637
Copying an Image File from One Stack Member to Another	1638

PART XV Data Sanitization 1639

CHAPTER 85	Data Sanitization	1641
	Example: Data Sanitization	1642

PART XVI Embedded Event Manager 1645

CHAPTER 86	Embedded Event Manager Overview	1647
	Information About Embedded Event Manager	1647
	Embedded Event Manager	1647
	Embedded Event Manager 1.0	1648

Embedded Event Manager 2.0	1649
Embedded Event Manager 2.1	1649
Embedded Event Manager 2.1 (Software Modularity)	1650
Embedded Event Manager 2.2	1650
Embedded Event Manager 2.3	1651
Embedded Event Manager 2.4	1651
Embedded Event Manager 3.0	1652
Embedded Event Manager 3.1	1653
Embedded Event Manager 3.2	1653
Embedded Event Manager 4.0	1654
EEM Event Detectors Available by Cisco IOS Release	1655
Event Detectors	1657
EEM Actions Available by Cisco IOS Release	1661
Embedded Event Manager Actions	1662
Embedded Event Manager Environment Variables	1662
Embedded Event Manager Policy Creation	1664
Where to Go Next	1665
Feature Information for Embedded Event Manager 4.0 Overview	1665
Additional References	1665

CHAPTER 87

Information About Writing EEM Policies Using the Cisco IOS CLI	1669
Prerequisites for Writing EEM Policies Using the Cisco IOS CLI	1669
Information About Writing EEM Policies Using the Cisco IOS CLI	1669
Embedded Event Manager Policies	1669
EEM Applet	1670
EEM Script	1670
Embedded Event Manager Built-In Environment Variables Used in EEM Applets	1670
How to Write EEM Policies Using the Cisco IOS CLI	1681
Registering and Defining an Embedded Event Manager Applet	1681
EEM Environment Variables	1681
Alphabetical Order of EEM Action Labels	1682
Troubleshooting Tips	1685
Registering and Defining an EEM Tel Script	1685
Unregistering Embedded Event Manager Policies	1686

Suspending All Embedded Event Manager Policy Execution	1688
Displaying Embedded Event Manager History Data	1689
Displaying Embedded Event Manager Registered Policies	1690
Configuring Event SNMP Notification	1691
Configuring Multiple Event Support	1692
Setting the Event Configuration Parameters	1692
Configuring EEM Class-Based Scheduling	1694
Holding a Scheduled EEM Policy Event or Event Queue	1695
Resuming Execution of EEM Policy Events or Event Queues	1696
Clearing Pending EEM Policy Events or Event Queues	1697
Modifying the Scheduling Parameters of EEM Policy Events or Event Queues	1698
Verifying Class-Based Active EEM Policies	1700
Verifying Class-Based Active EEM Policies	1700
Verifying Pending EEM Policies	1701
Configuring EEM Applet (Interactive CLI) Support	1701
Reading and Writing Input from the Active Console for Synchronous EEM Applets	1701
Configuring SNMP Library Extensions	1704
Prerequisites	1704
SNMP Get and Set Operations	1704
SNMP Traps and Inform Requests	1706
Configuring EEM Applet for SNMP Get and Set Operations	1707
Configuring EEM Applet for SNMP OID Notifications	1709
Configuring Variable Logic for EEM Applets	1711
Prerequisites	1712
Configuring Variable Logic for EEM Applets	1712
Specifying a Loop of Conditional Blocks	1712
Specifying if else Conditional Blocks	1713
Specifying foreach Iterating Statements	1715
Using Regular Expressions	1716
Incrementing the Values of Variables	1717
Configuring Event SNMP Object	1717
Disabling AAA Authorization	1719
Configuring Description of an Embedded Event Manager Applet	1720
Configuration Examples for Writing Embedded Event Manager Policies Using Tcl	1721

Embedded Event Manager Applet Configuration Examples	1721
Configuration Examples for Embedded Event Manager Applet	1726
Example Identity Event Detector	1726
Example MAT Event Detector	1726
Example Neighbor-Discovery Event Detector	1726
Embedded Event Manager Manual Policy Execution Examples	1726
Embedded Event Manager Watchdog System Monitor (Cisco IOS) Event Detector Configuration Example	1727
Configuration SNMP Library Extensions Examples	1728
SNMP Get Operations Examples	1728
SNMP GetID Operations Examples	1729
Set Operations Examples	1730
Generating SNMP Notifications Examples	1730
Configuring Variable Logic for EEM Applets Examples	1732
Configuring Event SNMP-Object Examples	1735
Configuring Description of an EEM Applet Examples	1736
Additional References	1736
Feature Information for Writing EEM 4.0 Policies Using the Cisco IOS CLI	1737

CHAPTER 88

Writing Embedded Event Manager Policies Using Tcl 1739

Prerequisites for Writing Embedded Event Manager Policies Using Tcl	1739
Information About Writing Embedded Event Manager Policies Using Tcl	1739
EEM Policies	1739
EEM Policy Tcl Command Extension Categories	1741
General Flow of EEM Event Detection and Recovery	1741
Safe-Tcl	1742
Bytecode Support for EEM 2.4	1744
Registration Substitution	1744
Cisco File Naming Convention for EEM	1745
How to Write Embedded Event Manager Policies Using Tcl	1746
Registering and Defining an EEM Tcl Script	1746
Displaying EEM Registered Policies	1748
Unregistering EEM Policies	1749
Suspending EEM Policy Execution	1751

Managing EEM Policies	1752
Modifying History Table Size and Displaying EEM History Data	1753
Displaying Software Modularity Process Reliability Metrics Using EEM	1754
Troubleshooting Tips	1756
Modifying the Sample EEM Policies	1756
Sample EEM Policies	1756
Programming EEM Policies with Tcl	1758
Tcl Policy Structure and Requirements	1758
EEM Entry Status	1760
EEM Exit Status	1760
EEM Policies and Cisco Error Number	1761
Troubleshooting Tips	1767
Creating an EEM User Tcl Library Index	1768
Creating an EEM User Tcl Package Index	1771
Configuration Examples for Writing Embedded Event Manager Policies Using Tcl	1773
Assigning a Username for a Tcl Session Examples	1773
EEM Event Detector Demo Examples	1773
Programming Policies with Tcl Sample Scripts Example	1781
Debugging Embedded Event Manager Policies Examples	1790
Tracing Tcl set Command Operations Example	1792
RPC Event Detector Example	1793
Additional References	1794

CHAPTER 89
Signed Tcl Scripts 1797

Prerequisites for Signed Tcl Scripts	1797
Restrictions for Signed Tcl Scripts	1797
Information About Signed Tcl Scripts	1798
Cisco PKI	1798
RSA Key Pair	1798
Certificate and Trustpoint	1799
How to Configure Signed Tcl Scripts	1799
Generating a Key Pair	1799
Generating a Certificate	1800
Signing the Tcl Scripts	1801

Verifying the Signature	1802
Converting the Signature into Nonbinary Data	1803
Configuring the Device with a Certificate	1806
Verifying the Trustpoint	1809
Verifying the Signed Tcl Script	1809
What to Do Next	1810
Configuration Examples for Signed Tcl Script	1810
Generating a Key Pair Example	1810
Generating a Certificate Example	1811
Signing the Tcl Scripts Example	1811
Verifying the Signature Example	1812
Converting the Signature with Nonbinary Data Example	1812
Configuring the Device with a Certificate Example	1814
Additional References	1815
Feature Information for Signed Tcl Scripts	1816
Glossary	1816
Notices	1817
OpenSSL Open SSL Project	1817
License Issues	1817

CHAPTER 90

EEM CLI Library Command Extensions 1821

cli_close	1822
cli_exec	1822
cli_get_ttyname	1823
cli_open	1823
cli_read	1824
cli_read_drain	1824
cli_read_line	1825
cli_read_pattern	1825
cli_run	1826
cli_run_interactive	1827
cli_write	1828
EEM 4.0 CLI Library XML-PI Support	1831
EEM CLI Library XML-PI Support	1831

CHAPTER 91	EEM Context Library Command Extensions	1833
	context_retrieve	1833
	context_save	1836
CHAPTER 92	EEM Event Registration Tcl Command Extensions	1841
	event_register_appl	1842
	event_register_cli	1844
	event_register_counter	1847
	event_register_gold	1849
	event_register_identity	1855
	event_register_interface	1857
	event_register_ioswdsysmon	1862
	event_register_ipsla	1865
	event_register_mat	1868
	event_register_neighbor_discovery	1870
	event_register_nf	1873
	event_register_none	1876
	event_register_oir	1878
	event_register_process	1880
	event_register_resource	1882
	event_register_rf	1884
	event_register_routing	1887
	event_register_rpc	1889
	event_register_snmp	1891
	event_register_snmp_notification	1895
	event_register_snmp_object	1897
	event_register_syslog	1900
	event_register_timer	1902
	event_register_timer_subscriber	1906
	event_register_track	1908
	event_register_wdsysmon	1910
CHAPTER 93	EEM Event Tcl Command Extensions	1925

event_completion 1925
 event_completion_with_wait 1926
 event_publish 1927
 event_wait 1930

CHAPTER 94 EEM Library Debug Command Extensions 1933

cli_debug 1933
 smtp_debug 1933

CHAPTER 95 EEM Multiple Event Support Tcl Command Extensions 1935

attribute 1935
 correlate 1936
 trigger 1937

CHAPTER 96 EEM SMTP Library Command Extensions 1939

smtp_send_email 1940
 smtp_subst 1941

CHAPTER 97 EEM System Information Tcl Command Extensions 1943

sys_reqinfo_cli_freq 1944
 sys_reqinfo_cli_history 1945
 sys_reqinfo_cpu_all 1945
 sys_reqinfo_crash_history 1946
 sys_reqinfo_mem_all 1947
 sys_reqinfo_proc 1948
 sys_reqinfo_proc_all 1950
 sys_reqinfo_routename 1950
 sys_reqinfo_snmp 1951
 sys_reqinfo_syslog_freq 1952
 sys_reqinfo_syslog_history 1953

CHAPTER 98 EEM Utility Tcl Command Extensions 1955

appl_read 1956

appl_reqinfo	1956
appl_setinfo	1957
counter_modify	1958
description	1959
fts_get_stamp	1960
register_counter	1961
register_timer	1962
timer_arm	1964
timer_cancel	1965
unregister_counter	1966

PART XVII
VLAN 1969

CHAPTER 99
Configuring VTP 1971

Finding Feature Information	1971
Prerequisites for VTP	1971
Restrictions for VTP	1972
Information About VTP	1972
VTP	1972
VTP Domain	1973
VTP Modes	1973
VTP Advertisements	1974
VTP Version 2	1975
VTP Version 3	1975
VTP Pruning	1976
VTP and Device Stacks	1976
VTP Configuration Guidelines	1977
VTP Configuration Requirements	1977
VTP Settings	1977
Domain Names for Configuring VTP	1977
Passwords for the VTP Domain	1978
VTP Version	1978
Default VTP Configuration	1979
How to Configure VTP	1979

Configuring VTP Mode	1979
Configuring a VTP Version 3 Password	1981
Configuring a VTP Version 3 Primary Server	1982
Enabling the VTP Version	1983
Enabling VTP Pruning	1984
Configuring VTP on a Per-Port Basis	1985
Adding a VTP Client to a VTP Domain	1987
Monitoring VTP	1988
Configuration Examples for VTP	1989
Example: Configuring a Switch as the Primary Server	1989
Example: Configuring Switch as VTP Server	1989
Example: Enabling VTP on the Interface	1990
Example: Creating the VTP Password	1990
Where to Go Next	1990
Additional References	1990
Feature History and Information for VTP	1991

CHAPTER 100

Configuring VLANs 1993

Finding Feature Information	1993
Prerequisites for VLANs	1993
Restrictions for VLANs	1994
Information About VLANs	1994
Logical Networks	1994
Supported VLANs	1995
VLAN Port Membership Modes	1995
VLAN Configuration Files	1996
Normal-Range VLAN Configuration Guidelines	1997
Extended-Range VLAN Configuration Guidelines	1998
Default VLAN Configurations	1998
Default Ethernet VLAN Configuration	1998
How to Configure VLANs	1999
How to Configure Normal-Range VLANs	1999
Creating or Modifying an Ethernet VLAN	2000
Deleting a VLAN	2001

Assigning Static-Access Ports to a VLAN	2002
How to Configure Extended-Range VLANs	2004
Creating an Extended-Range VLAN	2004
Monitoring VLANs	2005
Configuration Examples	2007
Example: Creating a VLAN Name	2007
Example: Configuring a Port as Access Port	2007
Example: Creating an Extended-Range VLAN	2008
Where to Go Next	2008
Additional References	2008
Feature History and Information for VLAN	2009

CHAPTER 101

Configuring VLAN Trunks	2011
Finding Feature Information	2011
Prerequisites for VLAN Trunks	2011
Information About VLAN Trunks	2012
Trunking Overview	2012
Trunking Modes	2012
Layer 2 Interface Modes	2012
Allowed VLANs on a Trunk	2013
Load Sharing on Trunk Ports	2013
Network Load Sharing Using STP Priorities	2013
Network Load Sharing Using STP Path Cost	2014
Feature Interactions	2014
Default Layer 2 Ethernet Interface VLAN Configuration	2014
How to Configure VLAN Trunks	2015
Configuring an Ethernet Interface as a Trunk Port	2015
Configuring a Trunk Port	2015
Defining the Allowed VLANs on a Trunk	2017
Changing the Pruning-Eligible List	2018
Configuring the Native VLAN for Untagged Traffic	2019
Configuring Trunk Ports for Load Sharing	2021
Configuring Load Sharing Using STP Port Priorities	2021
Configuring Load Sharing Using STP Path Cost	2024

Configuration Examples for VLAN Trunking	2026
Example: Configuring a Trunk Port	2026
Example: Removing a VLAN from a Port	2026
Where to Go Next	2027
Additional References	2027
Feature History and Information for VLAN Trunks	2028

CHAPTER 102

Configuring Private VLANs 2029

Prerequisites for Private VLANs	2029
Secondary and Primary VLAN Configuration	2029
Private VLAN Port Configuration	2031
Restrictions for Private VLANs	2032
Limitations with Other Features	2032
Information About Private VLANs	2033
Private VLAN Domains	2033
Secondary VLANs	2034
Private VLANs Ports	2034
Private VLANs in Networks	2035
IP Addressing Scheme with Private VLANs	2035
Private VLANs Across Multiple Devices	2036
Private VLAN Interaction with Other Features	2036
Private VLANs and Unicast, Broadcast, and Multicast Traffic	2036
Private VLANs and SVIs	2037
Private VLANs and Device Stacks	2037
Private VLAN Configuration Tasks	2037
Default Private VLAN Configuration	2038
How to Configure Private VLANs	2038
Configuring and Associating VLANs in a Private VLAN	2038
Configuring a Layer 2 Interface as a Private VLAN Host Port	2041
Configuring a Layer 2 Interface as a Private VLAN Promiscuous Port	2043
Mapping Secondary VLANs to a Primary VLAN Layer 3 VLAN Interface	2044
Monitoring Private VLANs	2046
Configuration Examples for Private VLANs	2046
Example: Configuring a Primary VLAN, Isolated VLAN, and a Community of VLANs	2046

Example: Configuring an Interface as a Host Port	2047
Example: Configuring an Interface as a Private VLAN Promiscuous Port	2047
Example: Mapping Secondary VLANs to a Primary VLAN Interface	2048
Example: Monitoring Private VLANs	2048
Where to Go Next	2048
Additional References	2049
Feature History and Information for Private VLANs	2049

CHAPTER 103**Configuring IEEE 802.1Q and Layer 2 Protocol Tunneling 2051**

Prerequisites for Configuring Tunneling	2051
IEEE 802.1Q Tunneling	2051
Information about Tunneling	2052
IEEE 802.1Q and Layer 2 Protocol Overview	2052
IEEE 802.1Q Tunneling	2052
IEEE 802.1Q Tunneling Configuration Guidelines	2054
Native VLANs	2055
System MTU	2056
Default IEEE 802.1Q Tunneling Configuration	2056
How to Configure Tunneling	2056
Configuring an IEEE 802.1Q Tunneling Port	2056
Configuring the SP Edge Switch	2058
Configuring the Customer Device	2061
Configuration Examples for IEEE 802.1Q and Layer 2 Protocol Tunneling	2063
Example: Configuring an IEEE 802.1Q Tunneling Port	2063
Examples: Configuring the SP Edge and Customer Switches	2064
Monitoring Tunneling Status	2065
Where to Go Next	2065
Additional References	2066
Feature History and Information for Tunneling	2067

CHAPTER 104**Configuring VMPS 2069**

Finding Feature Information	2069
Prerequisites for VMPS	2069
Restrictions for VMPS	2069

Information About VMPS	2070
Dynamic VLAN Assignments	2070
Dynamic-Access Port VLAN Membership	2071
Default VMPS Client Configuration	2071
How to Configure VMPS	2072
Entering the IP Address of the VMPS	2072
Configuring Dynamic-Access Ports on VMPS Clients	2073
Reconfirming VLAN Memberships	2074
Changing the Reconfirmation Interval	2075
Changing the Retry Count	2076
Troubleshooting Dynamic-Access Port VLAN Membership	2077
Monitoring the VMPS	2077
Configuration Example for VMPS	2078
Example: VMPS Configuration	2078
Where to Go Next	2079
Additional References	2080
Feature History and Information for VMPS	2080

CHAPTER 105

Configuring Voice VLANs	2081
Finding Feature Information	2081
Prerequisites for Voice VLANs	2081
Restrictions for Voice VLANs	2082
Information About Voice VLAN	2082
Voice VLANs	2082
Cisco IP Phone Voice Traffic	2082
Cisco IP Phone Data Traffic	2083
Voice VLAN Configuration Guidelines	2083
Default Voice VLAN Configuration	2084
How to Configure Voice VLAN	2084
Configuring Cisco IP Phone Voice Traffic	2084
Configuring the Priority of Incoming Data Frames	2086
Monitoring Voice VLAN	2088
Configuration Examples	2088
Example: Configuring Cisco IP Phone Voice Traffic	2088

Example: Configuring the Priority of Incoming Data Frames	2088
Where to Go Next	2088
Additional References	2089
Feature History and Information for Voice VLAN	2089



CHAPTER 1

Using the Command-Line Interface

- [Information About Using the Command-Line Interface, on page 1](#)
- [How to Use the CLI to Configure Features, on page 5](#)

Information About Using the Command-Line Interface



Note Search options on the GUI and CLI are case sensitive.

Command Modes

The Cisco IOS user interface is divided into many different modes. The commands available to you depend on which mode you are currently in. Enter a question mark (?) at the system prompt to obtain a list of commands available for each command mode.

You can start a CLI session through a console connection, through Telnet, an SSH, or by using the browser.

When you start a session, you begin in user mode, often called user EXEC mode. Only a limited subset of the commands are available in user EXEC mode. For example, most of the user EXEC commands are one-time commands, such as **show** commands, which show the current configuration status, and **clear** commands, which clear counters or interfaces. The user EXEC commands are not saved when the device reboots.

To have access to all commands, you must enter privileged EXEC mode. Normally, you must enter a password to enter privileged EXEC mode. From this mode, you can enter any privileged EXEC command or enter global configuration mode.

Using the configuration modes (global, interface, and line), you can make changes to the running configuration. If you save the configuration, these commands are stored and used when the device reboots. To access the various configuration modes, you must start at global configuration mode. From global configuration mode, you can enter interface configuration mode and line configuration mode .

This table describes the main command modes, how to access each one, the prompt you see in that mode, and how to exit the mode.

Table 1: Command Mode Summary

Mode	Access Method	Prompt	Exit Method	About This Mode
User EXEC	Begin a session using Telnet, SSH, or console.	Device>	Enter logout or quit .	Use this mode to <ul style="list-style-type: none"> • Change terminal settings. • Perform basic tests. • Display system information.
Privileged EXEC	While in user EXEC mode, enter the enable command.	Device#	Enter disable to exit.	Use this mode to verify commands that you have entered. Use a password to protect access to this mode.
Global configuration	While in privileged EXEC mode, enter the configure command.	Device(config)#	To exit to privileged EXEC mode, enter exit or end , or press Ctrl-Z .	Use this mode to configure parameters that apply to the entire device.
VLAN configuration	While in global configuration mode, enter the vlan <i>vlan-id</i> command.	Device(config-vlan)#	To exit to global configuration mode, enter the exit command. To return to privileged EXEC mode, press Ctrl-Z or enter end .	Use this mode to configure VLAN parameters. When VTP mode is transparent, you can create extended-range VLANs (VLAN IDs greater than 1005) and save configurations in the device startup configuration file.

Mode	Access Method	Prompt	Exit Method	About This Mode
Interface configuration	While in global configuration mode, enter the interface command (with a specific interface).	Device (config-if) #	To exit to global configuration mode, enter exit . To return to privileged EXEC mode, press Ctrl-Z or enter end .	Use this mode to configure parameters for the Ethernet ports.
Line configuration	While in global configuration mode, specify a line with the line vty or line console command.	Device (config-line) #	To exit to global configuration mode, enter exit . To return to privileged EXEC mode, press Ctrl-Z or enter end .	Use this mode to configure parameters for the terminal line.

Understanding Abbreviated Commands

You need to enter only enough characters for the device to recognize the command as unique.

This example shows how to enter the **show configuration** privileged EXEC command in an abbreviated form:

```
Device# show conf
```

No and Default Forms of Commands

Almost every configuration command also has a **no** form. In general, use the **no** form to disable a feature or function or reverse the action of a command. For example, the **no shutdown** interface configuration command reverses the shutdown of an interface. Use the command without the keyword **no** to reenabling a disabled feature or to enable a feature that is disabled by default.

Configuration commands can also have a **default** form. The **default** form of a command returns the command setting to its default. Most commands are disabled by default, so the **default** form is the same as the **no** form. However, some commands are enabled by default and have variables set to certain default values. In these cases, the **default** command enables the command and sets variables to their default values.

CLI Error Messages

This table lists some error messages that you might encounter while using the CLI to configure your device.

Table 2: Common CLI Error Messages

Error Message	Meaning	How to Get Help
% Ambiguous command: "show con"	You did not enter enough characters for your device to recognize the command.	Reenter the command followed by a question mark (?) without any space between the command and the question mark. The possible keywords that you can enter with the command appear.
% Incomplete command.	You did not enter all of the keywords or values required by this command.	Reenter the command followed by a question mark (?) with a space between the command and the question mark. The possible keywords that you can enter with the command appear.
% Invalid input detected at '^' marker.	You entered the command incorrectly. The caret (^) marks the point of the error.	Enter a question mark (?) to display all of the commands that are available in this command mode. The possible keywords that you can enter with the command appear.

Configuration Logging

You can log and view changes to the device configuration. You can use the Configuration Change Logging and Notification feature to track changes on a per-session and per-user basis. The logger tracks each configuration command that is applied, the user who entered the command, the time that the command was entered, and the parser return code for the command. This feature includes a mechanism for asynchronous notification to registered applications whenever the configuration changes. You can choose to have the notifications sent to the syslog.



Note Only CLI or HTTP changes are logged.

Using the Help System

You can enter a question mark (?) at the system prompt to display a list of commands available for each command mode. You can also obtain a list of associated keywords and arguments for any command.

Procedure

	Command or Action	Purpose
Step 1	help Example: Device# help	Obtains a brief description of the help system in any command mode.

	Command or Action	Purpose
Step 2	<i>abbreviated-command-entry ?</i> Example: Device# di? dir disable disconnect	Obtains a list of commands that begin with a particular character string.
Step 3	<i>abbreviated-command-entry <Tab></i> Example: Device# sh conf<tab> Device# show configuration	Completes a partial command name.
Step 4	? Example: Device> ?	Lists all commands available for a particular command mode.
Step 5	<i>command ?</i> Example: Device> show ?	Lists the associated keywords for a command.
Step 6	<i>command keyword ?</i> Example: Device(config)# cdp holdtime ? <10-255> Length of time (in sec) that receiver must keep this packet	Lists the associated arguments for a keyword.

How to Use the CLI to Configure Features

Configuring the Command History

The software provides a history or record of commands that you have entered. The command history feature is particularly useful for recalling long or complex commands or entries, including access lists. You can customize this feature to suit your needs.

Changing the Command History Buffer Size

By default, the device records ten command lines in its history buffer. You can alter this number for a current terminal session or for all sessions on a particular line. This procedure is optional.

Procedure

	Command or Action	Purpose
Step 1	terminal history [<i>size number-of-lines</i>] Example: Device# terminal history size 200	Changes the number of command lines that the device records during the current terminal session in privileged EXEC mode. You can configure the size from 0 to 256.

Recalling Commands

To recall commands from the history buffer, perform one of the actions listed in this table. These actions are optional.



Note The arrow keys function only on ANSI-compatible terminals such as VT100s.

Procedure

	Command or Action	Purpose
Step 1	Ctrl-P or use the up arrow key	Recalls commands in the history buffer, beginning with the most recent command. Repeat the key sequence to recall successively older commands.
Step 2	Ctrl-N or use the down arrow key	Returns to more recent commands in the history buffer after recalling commands with Ctrl-P or the up arrow key. Repeat the key sequence to recall successively more recent commands.
Step 3	show history Example: Device# show history	Lists the last several commands that you just entered in privileged EXEC mode. The number of commands that appear is controlled by the setting of the terminal history global configuration command and the history line configuration command.

Disabling the Command History Feature

The command history feature is automatically enabled. You can disable it for the current terminal session or for the command line. This procedure is optional.

Procedure

	Command or Action	Purpose
Step 1	terminal no history Example: Device# terminal no history	Disables the feature during the current terminal session in privileged EXEC mode.

Enabling and Disabling Editing Features

Although enhanced editing mode is automatically enabled, you can disable it and reenables it.

Procedure

	Command or Action	Purpose
Step 1	terminal editing Example: Device# <code>terminal editing</code>	Reenables the enhanced editing mode for the current terminal session in privileged EXEC mode.
Step 2	terminal no editing Example: Device# <code>terminal no editing</code>	Disables the enhanced editing mode for the current terminal session in privileged EXEC mode.

Editing Commands Through Keystrokes

The keystrokes help you to edit the command lines. These keystrokes are optional.



Note The arrow keys function only on ANSI-compatible terminals such as VT100s.

Table 3: Editing Commands

Editing Commands	Description
Ctrl-B or use the left arrow key	Moves the cursor back one character.
Ctrl-F or use the right arrow key	Moves the cursor forward one character.
Ctrl-A	Moves the cursor to the beginning of the command line.
Ctrl-E	Moves the cursor to the end of the command line.
Esc B	Moves the cursor back one word.
Esc F	Moves the cursor forward one word.
Ctrl-T	Transposes the character to the left of the cursor with the character located at the cursor.
Delete or Backspace key	Erases the character to the left of the cursor.
Ctrl-D	Deletes the character at the cursor.
Ctrl-K	Deletes all characters from the cursor to the end of the command line.
Ctrl-U or Ctrl-X	Deletes all characters from the cursor to the beginning of the command line.

Ctrl-W	Deletes the word to the left of the cursor.
Esc D	Deletes from the cursor to the end of the word.
Esc C	Capitalizes at the cursor.
Esc L	Changes the word at the cursor to lowercase.
Esc U	Capitalizes letters from the cursor to the end of the word.
Ctrl-V or Esc Q	Designates a particular keystroke as an executable command, perhaps as a shortcut.
Return key	<p>Scrolls down a line or screen on displays that are longer than the terminal screen can display.</p> <p>Note The More prompt is used for any output that has more lines than can be displayed on the terminal screen, including show command output. You can use the Return and Space bar keystrokes whenever you see the More prompt.</p>
Space bar	Scrolls down one screen.
Ctrl-L or Ctrl-R	Redisplays the current command line if the device suddenly sends a message to your screen.

Editing Command Lines That Wrap

You can use a wraparound feature for commands that extend beyond a single line on the screen. When the cursor reaches the right margin, the command line shifts ten spaces to the left. You cannot see the first ten characters of the line, but you can scroll back and check the syntax at the beginning of the command. The keystroke actions are optional.

To scroll back to the beginning of the command entry, press **Ctrl-B** or the left arrow key repeatedly. You can also press **Ctrl-A** to immediately move to the beginning of the line.



Note The arrow keys function only on ANSI-compatible terminals such as VT100s.

The following example shows how to wrap a command line that extends beyond a single line on the screen.

Procedure

	Command or Action	Purpose
Step 1	<p>access-list</p> <p>Example:</p> <pre>Device(config)# access-list 101 permit tcp 10.15.22.25 255.255.255.0 10.15.22.35 Device(config)# \$ 101 permit tcp 10.15.22.25 255.255.255.0 10.15.22.35</pre>	<p>Displays the global configuration command entry that extends beyond one line.</p> <p>When the cursor first reaches the end of the line, the line is shifted ten spaces to the left and redisplayed. The dollar sign (\$) shows that the line has been scrolled to the left. Each time the</p>

	Command or Action	Purpose
	<pre>255.25 Device(config)# \$t tcp 10.15.22.25 255.255.255.0 131.108.1.20 255.255.255.0 eq Device(config)# \$15.22.25 255.255.255.0 10.15.22.35 255.255.255.0 eq 45</pre>	cursor reaches the end of the line, the line is again shifted ten spaces to the left.
Step 2	Ctrl-A Example: <pre>Device(config)# access-list 101 permit tcp 10.15.22.25 255.255.255.0 10.15.25</pre>	Checks the complete syntax. The dollar sign (\$) appears at the end of the line to show that the line has been scrolled to the right.
Step 3	Return key	Execute the commands. The software assumes that you have a terminal screen that is 80 columns wide. If you have a different width, use the terminal width privileged EXEC command to set the width of your terminal. Use line wrapping with the command history feature to recall and modify previous complex command entries.

Searching and Filtering Output of show and more Commands

You can search and filter the output for **show** and **more** commands. This is useful when you need to sort through large amounts of output or if you want to exclude output that you do not need to see. Using these commands is optional.

Procedure

	Command or Action	Purpose
Step 1	<pre>{show more} command {begin include exclude} regular-expression</pre> Example: <pre>Device# show interfaces include protocol Vlan1 is up, line protocol is up Vlan10 is up, line protocol is down GigabitEthernet1/0/1 is up, line protocol is down GigabitEthernet1/0/2 is up, line protocol is up</pre>	Searches and filters the output. Expressions are case sensitive. For example, if you enter exclude output , the lines that contain output are not displayed, but the lines that contain output appear.

Accessing the CLI

You can access the CLI through a console connection, through Telnet, a SSH, or by using the browser.

You manage the switch stack and the stack member interfaces through the stack's active switch. You cannot manage stack members on an individual switch basis. You can connect to the stack's active switch through the console port or the Ethernet management port of one or more stack members. Be careful with using multiple CLI sessions on the stack's active switch. Commands that you enter in one session are not displayed in the other sessions. Therefore, it is possible to lose track of the session from which you entered commands.



Note We recommend using one CLI session when managing the switch stack.

If you want to configure a specific stack member port, you must include the stack member number in the CLI command interface notation.

To debug the standby switch, use the **session standby ios** privileged EXEC command from the active switch to access the IOS console of the standby switch. To debug a specific stack member, use the **session switch stack-member-number** privileged EXEC command from the active switch to access the diagnostic shell of the stack member. For more information about these commands, see the switch command reference.

To debug a specific stack member, you can start a CLI session from the stack master by using the **session stack-member-number** privileged EXEC command. The stack member number is appended to the system prompt. For example, *Switch-2#* is the prompt for stack member 2 where the system prompt for the stack master is *Switch*. Only the **show** and **debug** commands are available in a CLI session to a specific stack member. You can also use the **remote command stack-member-number LINE** privileged EXEC command on the stack master to enable debugging on a member switch without first starting a session.

Accessing the CLI Through a Console Connection or Through Telnet

Before you can access the CLI, you must connect a terminal or a PC to the device console or connect a PC to the Ethernet management port and then power on the device, as described in the hardware installation guide that shipped with your device.

If your device is already configured, you can access the CLI through a local console connection or through a remote Telnet session, but your device must first be configured for this type of access.

You can use one of these methods to establish a connection with the device:

Procedure

- Connect the device console port to a management station or dial-up modem, or connect the Ethernet management port to a PC. For information about connecting to the console or Ethernet management port, see the device hardware installation guide.
- Use any Telnet TCP/IP or encrypted Secure Shell (SSH) package from a remote management station. The device must have network connectivity with the Telnet or SSH client, and the device must have an enable secret password configured.
 - The device supports up to 16 simultaneous Telnet sessions. Changes made by one Telnet user are reflected in all other Telnet sessions.
 - The device supports up to five simultaneous secure SSH sessions.

After you connect through the console port, through the Ethernet management port, through a Telnet session or through an SSH session, the user EXEC prompt appears on the management station.

Accessing the CLI through Bluetooth

You can access the CLI through Bluetooth connectivity by pairing the switch to a computer.



Note This feature is available on Cisco IOS Release 15.2(5)E2 and higher.

1. Connect a Bluetooth dongle to the USB port on your switch and power on the switch.
2. Turn on Bluetooth on your computer and discover the switch.
3. Pair the computer to the switch.
4. Connect to the switch as an access point.
 - If you are connecting from a Windows computer: Go to *Devices & Printers*, select the switch, click on the *Connect Using* tab and select *Access point*.
 - If you are connecting from a Mac computer: On the menu bar, click the Bluetooth icon, hover over the switch name, and click *Connect to Network*.

Once a connection is established, you can open a management window and configure the switch.



PART I

Interface and Hardware

- [Configuring Interface Characteristics, on page 15](#)
- [Configuring Auto-MDIX, on page 41](#)
- [Configuring Ethernet Management Port, on page 45](#)
- [Configuring LLDP, LLDP-MED, and Wired Location Service, on page 49](#)
- [Configuring System MTU, on page 67](#)
- [Configuring Boot Fast, on page 71](#)
- [Configuring Power over Ethernet, on page 73](#)
- [Configuring 2-event Classification, on page 89](#)
- [Configuring EEE, on page 91](#)



CHAPTER 2

Configuring Interface Characteristics

- [Information About Configuring Interface Characteristics, on page 15](#)
- [How to Configure Interface Characteristics, on page 24](#)
- [Monitoring Interface Characteristics, on page 35](#)
- [Configuration Examples for Interface Characteristics, on page 37](#)
- [Additional References for the Interface Characteristics Feature, on page 39](#)
- [Feature History and Information for Configuring Interface Characteristics, on page 40](#)

Information About Configuring Interface Characteristics

Interface Types

This section describes the different types of interfaces supported by the device. The rest of the chapter describes configuration procedures for physical interface characteristics.



Note

The stack ports on the rear of the stacking-capable devices are not Ethernet ports and cannot be configured.

Port-Based VLANs

A VLAN is a switched network that is logically segmented by function, team, or application, without regard to the physical location of the users. Packets received on a port are forwarded only to ports that belong to the same VLAN as the receiving port. Network devices in different VLANs cannot communicate with one another without a Layer 3 device to route traffic between the VLANs.

VLAN partitions provide hard firewalls for traffic in the VLAN, and each VLAN has its own MAC address table. A VLAN comes into existence when a local port is configured to be associated with the VLAN, when the VLAN Trunking Protocol (VTP) learns of its existence from a neighbor on a trunk, or when a user creates a VLAN. VLANs can be formed with ports across the stack.

To configure VLANs, use the **vlan *vlan-id*** global configuration command to enter VLAN configuration mode. The VLAN configurations for normal-range VLANs (VLAN IDs 1 to 1005) are saved in the VLAN database. If VTP is version 1 or 2, to configure extended-range VLANs (VLAN IDs 1006 to 4094), you must first set VTP mode to transparent. Extended-range VLANs created in transparent mode are not added to the VLAN

database but are saved in the device running configuration. With VTP version 3, you can create extended-range VLANs in client or server mode. These VLANs are saved in the VLAN database.

In a switch stack, the VLAN database is downloaded to all switches in a stack, and all switches in the stack build the same VLAN database. The running configuration and the saved configuration are the same for all switches in a stack.

Add ports to a VLAN by using the **switchport** interface configuration commands:

- Identify the interface.
- For a trunk port, set trunk characteristics, and, if desired, define the VLANs to which it can belong.
- For an access port, set and define the VLAN to which it belongs.

Switch Ports

Switch ports are Layer 2-only interfaces associated with a physical port. Switch ports belong to one or more VLANs. A switch port can be an access port or a trunk port. You can configure a port as an access port or trunk port or let the Dynamic Trunking Protocol (DTP) operate on a per-port basis to set the switchport mode by negotiating with the port on the other end of the link. switch ports are used for managing the physical interface and associated Layer 2 protocols and do not handle routing or bridging.

Configure switch ports by using the **switchport** interface configuration commands.

Access Ports

An access port belongs to and carries the traffic of only one VLAN (unless it is configured as a voice VLAN port). 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 a tagged packet (Inter-Switch Link [ISL] or IEEE 802.1Q tagged), the packet is dropped, and the source address is not learned.

The types of access ports supported are:

- Static access ports are manually assigned to a VLAN (or through a RADIUS server for use with IEEE 802.1x).
- VLAN membership of dynamic access ports is learned through incoming packets. By default, a dynamic access port is not a member of any VLAN, and forwarding to and from the port is enabled only when the VLAN membership of the port is discovered. Dynamic access ports on the device are assigned to a VLAN by a VLAN Membership Policy Server (VMPS). The VMPS can be a Catalyst 6500 series switch; the device cannot be a VMPS server.

You can also configure an access port with an attached Cisco IP Phone to use one VLAN for voice traffic and another VLAN for data traffic from a device attached to the phone.

Trunk Ports

A trunk port carries the traffic of multiple VLANs and by default is a member of all VLANs in the VLAN database.

The device supports only IEEE 802.1Q trunk ports. An IEEE 802.1Q trunk port supports simultaneous tagged and untagged traffic. An IEEE 802.1Q trunk port is assigned a default port VLAN ID (PVID), and all untagged traffic travels on the port default PVID. All untagged traffic and tagged traffic with a NULL VLAN ID are assumed to belong to the port default PVID. A packet with a VLAN ID equal to the outgoing port default PVID is sent untagged. All other traffic is sent with a VLAN tag.

Although by default, a trunk port is a member of every VLAN known to the VTP, you can limit VLAN membership by configuring an allowed list of VLANs for each trunk port. The list of allowed VLANs does not affect any other port but the associated trunk port. By default, all possible VLANs (VLAN ID 1 to 4094) are in the allowed list. A trunk port can become a member of a VLAN only if VTP knows of the VLAN and if the VLAN is in the enabled state. If VTP learns of a new, enabled VLAN and the VLAN is in the allowed list for a trunk port, the trunk port automatically becomes a member of that VLAN and traffic is forwarded to and from the trunk port for that VLAN. If VTP learns of a new, enabled VLAN that is not in the allowed list for a trunk port, the port does not become a member of the VLAN, and no traffic for the VLAN is forwarded to or from the port.

Switch Virtual Interfaces

A switch virtual interface (SVI) represents a VLAN of switch ports as one interface to the routing or bridging function in the system. You can associate only one SVI with a VLAN. You configure an SVI for a VLAN only to route between VLANs or to provide IP host connectivity to the device. By default, an SVI is created for the default VLAN (VLAN 1) to permit remote device administration. Additional SVIs must be explicitly configured.



Note You cannot delete interface VLAN 1.

SVIs provide IP host connectivity only to the system. SVIs are created the first time that you enter the **vlan** interface configuration command for a VLAN interface. The VLAN corresponds to the VLAN tag associated with data frames on an ISL or IEEE 802.1Q encapsulated trunk or the VLAN ID configured for an access port. Configure a VLAN interface for each VLAN for which you want to route traffic, and assign it an IP address.

You can also use the interface range command to configure existing VLAN SVIs within the range. The commands entered under the interface range command are applied to all existing VLAN SVIs within the range. You can enter the command **interface range create vlan x - y** to create all VLANs in the specified range that do not already exist. When the VLAN interface is created, **interface range vlan id** can be used to configure the VLAN interface.

Although the switch stack or device supports a total of 1005 VLANs and SVIs, the interrelationship between the number of SVIs and routed ports and the number of other features being configured might impact CPU performance because of hardware limitations.

When you create an SVI, it does not become active until it is associated with a physical port.

SVI Autostate Exclude

The line state of an SVI with multiple ports on a VLAN is in the *up* state when it meets these conditions:

- The VLAN exists and is active in the VLAN database on the device
- The VLAN interface exists and is not administratively down.
- At least one Layer 2 (access or trunk) port exists, has a link in the *up* state on this VLAN, and is in the spanning-tree forwarding state on the VLAN.



Note The protocol link state for VLAN interfaces come up when the first switchport belonging to the corresponding VLAN link comes up and is in STP forwarding state.

The default action, when a VLAN has multiple ports, is that the SVI goes down when all ports in the VLAN go down. You can use the SVI autostate exclude feature to configure a port so that it is not included in the SVI line-state up-or-down calculation. For example, if the only active port on the VLAN is a monitoring port, you might configure autostate exclude on that port so that the VLAN goes down when all other ports go down. When enabled on a port, **autostate exclude** applies to all VLANs that are enabled on that port.

The VLAN interface is brought up when one Layer 2 port in the VLAN has had time to converge (transition from STP listening-learning state to forwarding state). This prevents features such as routing protocols from using the VLAN interface as if it were fully operational and minimizes other problems.

EtherChannel Port Groups

EtherChannel port groups treat multiple switch ports as one switch port. These port groups act as a single logical port for high-bandwidth connections between devices or between devices and servers. An EtherChannel balances the traffic load across the links in the channel. If a link within the EtherChannel fails, traffic previously carried over the failed link changes to the remaining links. You can group multiple trunk ports into one logical trunk port or multiple access ports into one logical access port. Most protocols operate over either single ports or aggregated switch ports and do not recognize the physical ports within the port group. Exceptions are the DTP, the Cisco Discovery Protocol (CDP), and the Port Aggregation Protocol (PAgP), which operate only on physical ports.

When you configure an EtherChannel, you create a port-channel logical interface and assign an interface to the EtherChannel. For Layer 2 interfaces, use the **channel-group** interface configuration command to dynamically create the port-channel logical interface. This command binds the physical and logical ports together.

Power over Ethernet Ports

A PoE-capable switch port automatically supplies power to one of these connected devices if the device senses that there is no power on the circuit:

- a Cisco pre-standard powered device (such as a Cisco IP Phone or a Cisco Aironet Access Point)
- an IEEE 802.3af-compliant powered device

A powered device can receive redundant power when it is connected to a PoE switch port and to an AC power source. The device does not receive redundant power when it is only connected to the PoE port.

Using the Switch USB Ports

The device has three USB ports on the front panel — a USB mini-Type B console port and two USB Type A ports.

USB Mini-Type B Console Port

The device has the following console ports:

- USB mini-Type B console connection

- RJ-45 console port

Console output appears on devices connected to both ports, but console input is active on only one port at a time. By default, the USB connector takes precedence over the RJ-45 connector.



Note Windows PCs require a driver for the USB port. See the hardware installation guide for driver installation instructions.

Use the supplied USB Type A-to-USB mini-Type B cable to connect a PC or other device to the device. The connected device must include a terminal emulation application. When the device detects a valid USB connection to a powered-on device that supports host functionality (such as a PC), input from the RJ-45 console is immediately disabled, and input from the USB console is enabled. Removing the USB connection immediately reenables input from the RJ-45 console connection. An LED on the device shows which console connection is in use.

Console Port Change Logs

At software startup, a log shows whether the USB or the RJ-45 console is active. Each device in a stack issues this log. Every device always first displays the RJ-45 media type.

In the sample output, Device 1 has a connected USB console cable. Because the bootloader did not change to the USB console, the first log from Device 1 shows the RJ-45 console. A short time later, the console changes and the USB console log appears. Device 2 and Device 3 have connected RJ-45 console cables.

```
switch-stack-1
*Mar  1 00:01:00.171: %USB_CONSOLE-6-MEDIA_RJ45: Console media-type is RJ45.
*Mar  1 00:01:00.431: %USB_CONSOLE-6-MEDIA_USB: Console media-type is USB.
```

```
switch-stack-2
*Mar  1 00:01:09.835: %USB_CONSOLE-6-MEDIA_RJ45: Console media-type is RJ45.
```

```
switch-stack-3
*Mar  1 00:01:10.523: %USB_CONSOLE-6-MEDIA_RJ45: Console media-type is RJ45.
```

When the USB cable is removed or the PC de-activates the USB connection, the hardware automatically changes to the RJ-45 console interface:

```
switch-stack-1
Mar  1 00:20:48.635: %USB_CONSOLE-6-MEDIA_RJ45: Console media-type is RJ45.
```

You can configure the console type to always be RJ-45, and you can configure an inactivity timeout for the USB connector.

USB Type A Ports

The USB Type A ports provide access to external USB flash devices, also known as thumb drives or USB keys. The switch supports Cisco 64 MB, 256 MB, 512 MB, 1 GB, 4 GB, and 8 GB flash drives. You can use standard Cisco IOS command-line interface (CLI) commands to read, write, erase, and copy to or from the flash device. You can also configure the switch to boot from the USB flash drive.

For information about configuring the switch to boot from a USB flash drive, refer to the *Catalyst 2960-X Switch System Management Configuration Guide*.

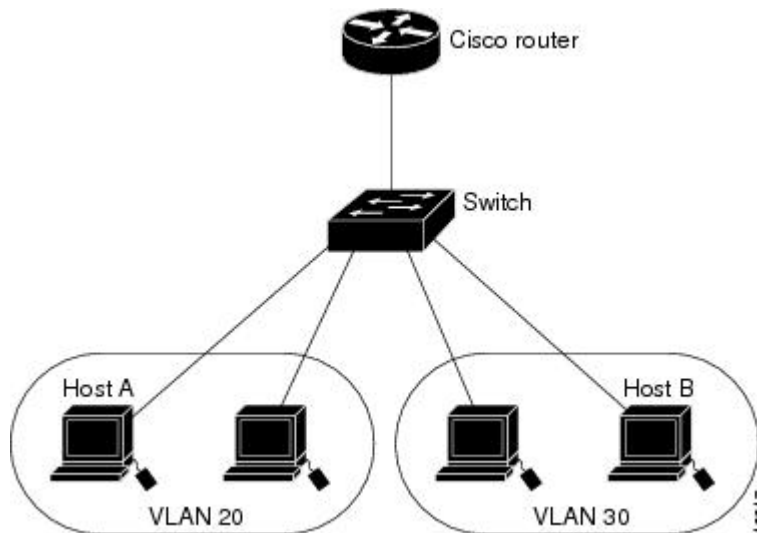
For information about reading, writing, erasing, and copying files to or from the flash device, refer to the *Catalyst 2960-X Switch Managing Cisco IOS Image Files Configuration Guide*.

Interface Connections

Devices within a single VLAN can communicate directly through any switch. Ports in different VLANs cannot exchange data without going through a routing device.

In the following configuration example, when Host A in VLAN 20 sends data to Host B in VLAN 30, the data must go from Host A to the device, to the router, back to the device, and then to Host B.

Figure 1: Connecting VLANs with the Switch



With a standard Layer 2 switch, ports in different VLANs have to exchange information through a router.



Note The Catalyst 3560-CX and 2960-CX switches do not support stacking. Ignore all references to stacking throughout this book.

Interface Configuration Mode

The device supports these interface types:

- Physical ports—device ports and routed ports
- VLANs—switch virtual interfaces
- Port channels—EtherChannel interfaces

You can also configure a range of interfaces.

To configure a physical interface (port), specify the interface type, module number, and device port number, and enter interface configuration mode.

- **Type**—Gigabit Ethernet (gigabitethernet or gi) for 10/100/1000 Mb/s Ethernet ports, or small form-factor pluggable (SFP) module Gigabit Ethernet interfaces (gigabitethernet or gi).
- **Stack member number**—The number that identifies the switch within the stack. The range is 1 to 8 for a stack of Catalyst 2960-X switches, and 1 to 4 for a mixed stack of Catalyst 2960-X and Catalyst 2960-S switches. The switch number is assigned the first time the switch initializes. The default switch number, before it is integrated into a switch stack, is 1. When a switch has been assigned a stack member number, it keeps that number until another is assigned to it.

You can use the switch port LEDs in Stack mode to identify the stack member number of a switch.

- **Module number**—The module or slot number on the switch (always 0).
- **Port number**—The interface number on the switch. The 10/100/1000 port numbers always begin at 1, starting with the far left port when facing the front of the switch, for example, gigabitethernet1/0/1 or gigabitethernet1/0/8. For a switch with 10/100/1000 ports and SFP module ports, SFP module ports are numbered consecutively following the 10/100/1000 ports.

You can identify physical interfaces by physically checking the interface location on the switch. You can also use the **show** privileged EXEC commands to display information about a specific interface or all the interfaces on the switch. The remainder of this chapter primarily provides physical interface configuration procedures.

These are examples of how to identify interfaces on a stacking-capable switch:

- To configure 10/100/1000 port 4 on a standalone device, enter this command:

```
Device(config)# interface gigabitethernet1/0/4
```

- To configure 10/100/1000 port 4 on stack member 3, enter this command:

```
Device(config)# interface gigabitethernet1/0/4
```

Default Ethernet Interface Configuration

This table shows the Ethernet interface default configuration, including some features that apply only to Layer 2 interfaces.

Table 4: Default Layer 2 Ethernet Interface Configuration

Feature	Default Setting
Operating mode	Layer 2 or switching mode (switchport command).
Allowed VLAN range	VLANs 1– 4094.
Default VLAN (for access ports)	VLAN 1.
Native VLAN (for IEEE 802.1Q trunks)	VLAN 1.
802.1p priority-tagged traffic	Drop all packets tagged with VLAN 0.
VLAN trunking	Switchport mode dynamic auto (supports DTP).

Feature	Default Setting
Port enable state	All ports are enabled.
Port description	None defined.
Speed	Autonegotiate. (Not supported on the 10-Gigabit interfaces.)
Duplex mode	Autonegotiate. (Not supported on the 10-Gigabit interfaces.)
Flow control	Flow control is set to receive: off . It is always off for sent packets.
EtherChannel (PAgP)	Disabled on all Ethernet ports.
Port blocking (unknown multicast and unknown unicast traffic)	Disabled (not blocked).
Broadcast, multicast, and unicast storm control	Disabled.
Protected port	Disabled.
Port security	Disabled.
Port Fast	Disabled.
Auto-MDIX	Enabled. Note The device might not support a pre-standard powered device—such as Cisco IP phones and access points that do not fully support IEEE 802.3af—if that powered device is connected to the device through a crossover cable. This is regardless of whether auto-MIDX is enabled on the switch port.
Power over Ethernet (PoE)	Enabled (auto).
Keepalive messages	Disabled on SFP module ports; enabled on all other ports.

Interface Speed and Duplex Mode

Ethernet interfaces on the switch operate at 10, 100, or 1000 Mb/s and in either full- or half-duplex mode. In full-duplex mode, two stations can send and receive traffic at the same time. Normally, 10-Mb/s ports operate in half-duplex mode, which means that stations can either receive or send traffic.

Switch modules include Gigabit Ethernet (10/100/1000-Mb/s) ports and small form-factor pluggable (SFP) module slots supporting SFP modules.

Speed and Duplex Configuration Guidelines

When configuring an interface speed and duplex mode, note these guidelines:

- Do not disable Auto-Negotiation on PoE switches.
- Gigabit Ethernet (10/100/1000-Mb/s) ports support all speed options and all duplex options (auto, half, and full). However, Gigabit Ethernet ports operating at 1000 Mb/s do not support half-duplex mode.
- For SFP module ports, the speed and duplex CLI options change depending on the SFP module type:
 - The 1000BASE-x (where -x is -BX, -CWDM, -LX, -SX, and -ZX) SFP module ports support the **nonegotiate** keyword in the **speed** interface configuration command. Duplex options are not supported.
 - The 1000BASE-T SFP module ports support the same speed and duplex options as the 10/100/1000-Mb/s ports.
 -
- If both ends of the line support autonegotiation, we highly recommend the default setting of **auto** negotiation.
- If one interface supports autonegotiation and the other end does not, configure duplex and speed on both interfaces; do not use the **auto** setting on the supported side.
- When STP is enabled and a port is reconfigured, the device can take up to 30 seconds to check for loops. The port LED is amber while STP reconfigures.
- As best practice, we suggest configuring the speed and duplex options on a link to auto or to fixed on both the ends. If one side of the link is configured to auto and the other side is configured to fixed, the link will not be up and this is expected.

**Caution**

Changing the interface speed and duplex mode configuration might shut down and re-enable the interface during the reconfiguration.

IEEE 802.3x Flow Control

Flow control enables connected Ethernet ports to control traffic rates during congestion by allowing congested nodes to pause link operation at the other end. If one port experiences congestion and cannot receive any more traffic, it notifies the other port by sending a pause frame to stop sending until the condition clears. Upon receipt of a pause frame, the sending device stops sending any data packets, which prevents any loss of data packets during the congestion period.

**Note**

The switch ports can receive, but not send, pause frames.

Use the **flowcontrol** interface configuration command to set the interface's ability to **receive** pause frames to **on**, **off**, or **desired**.

When set to **desired**, an interface can operate with an attached device that is required to send flow-control packets or with an attached device that is not required to but can send flow-control packets.

These rules apply to flow control settings on the device:

- **receive on** (or **desired**): The port cannot send 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.



Note For details on the command settings and the resulting flow control resolution on local and remote ports, see the **flowcontrol** interface configuration command in the command reference for this release.

How to Configure Interface Characteristics

Configuring Interfaces

These general instructions apply to all interface configuration processes.

Procedure

	Command or Action	Purpose
Step 1	enable Example: <pre>Device> enable</pre>	Enables privileged EXEC mode. <ul style="list-style-type: none"> • Enter your password if prompted.
Step 2	configure terminal Example: <pre>Device# configure terminal</pre>	Enters global configuration mode.
Step 3	interface Example: <pre>Device(config)# interface gigabitethernet 1/0/1 Device(config-if)#</pre>	Identifies the interface type, the device number (only on stacking-capable switches), and the number of the connector. Note You do not need to add a space between the interface type and the interface number. For example, in the preceding line, you can specify either gigabitethernet 1/0/1 , gigabitethernet1/0/1 , gi 1/0/1 , or gi1/0/1 .
Step 4	Follow each interface command with the interface configuration commands that the interface requires.	Defines the protocols and applications that will run on the interface. The commands are collected and applied to the interface when you

	Command or Action	Purpose
		enter another interface command or enter end to return to privileged EXEC mode.
Step 5	interface range or interface range macro	(Optional) Configures a range of interfaces. Note Interfaces configured in a range must be the same type and must be configured with the same feature options.
Step 6	show interfaces	Displays a list of all interfaces on or configured for the switch. A report is provided for each interface that the device supports or for the specified interface.

Adding a Description for an Interface

Procedure

	Command or Action	Purpose
Step 1	enable Example: Device> enable	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	configure terminal Example: Device# configure terminal	Enters global configuration mode.
Step 3	interface <i>interface-id</i> Example: Device(config)# interface gigabitethernet 1/0/2	Specifies the interface for which you are adding a description, and enter interface configuration mode.
Step 4	description <i>string</i> Example: Device(config-if)# description Connects to Marketing	Adds a description (up to 240 characters) for an interface.

	Command or Action	Purpose
Step 5	end Example: Device (config-if) # end	Returns to privileged EXEC mode.
Step 6	show interfaces <i>interface-id</i> description	Verifies your entry.
Step 7	copy running-config startup-config Example: Device# copy running-config startup-config	(Optional) Saves your entries in the configuration file.

Configuring a Range of Interfaces

To configure multiple interfaces with the same configuration parameters, use the **interface range** global configuration command. When you enter the interface-range configuration mode, all command parameters that you enter are attributed to all interfaces within that range until you exit this mode.

Procedure

	Command or Action	Purpose
Step 1	enable Example: Device> enable	Enables privileged EXEC mode. <ul style="list-style-type: none"> • Enter your password if prompted.
Step 2	configure terminal Example: Device# configure terminal	Enters global configuration mode.
Step 3	interface range { <i>port-range</i> macro <i>macro_name</i> } Example: Device (config) # interface range macro	Specifies the range of interfaces (VLANs or physical ports) to be configured, and enter interface-range configuration mode. <ul style="list-style-type: none"> • You can use the interface range command to configure up to five port ranges or a previously defined macro. • The macro variable is explained in the section on <i>Configuring and Using Interface Range Macros</i>.

	Command or Action	Purpose
		<ul style="list-style-type: none"> • In a comma-separated <i>port-range</i>, you must enter the interface type for each entry and enter spaces before and after the comma. • In a hyphen-separated <i>port-range</i>, you do not need to re-enter the interface type, but you must enter a space before the hyphen. <p>Note Use the normal configuration commands to apply the configuration parameters to all interfaces in the range. Each command is executed as it is entered.</p>
Step 4	end Example: Device(config)# end	Returns to privileged EXEC mode.
Step 5	show interfaces [<i>interface-id</i>] Example: Device# show interfaces	Verifies the configuration of the interfaces in the range.
Step 6	copy running-config startup-config Example: Device# copy running-config startup-config	(Optional) Saves your entries in the configuration file.

Configuring and Using Interface Range Macros

You can create an interface range macro to automatically select a range of interfaces for configuration. Before you can use the **macro** keyword in the **interface range macro** global configuration command string, you must use the **define interface-range** global configuration command to define the macro.

Procedure

	Command or Action	Purpose
Step 1	enable Example: Device> enable	Enables privileged EXEC mode. <ul style="list-style-type: none"> • Enter your password if prompted.

	Command or Action	Purpose
Step 2	configure terminal Example: <pre>Device# configure terminal</pre>	Enters global configuration mode.
Step 3	define interface-range <i>macro_name</i> <i>interface-range</i> Example: <pre>Device(config)# define interface-range enet_list gigabitethernet 1/0/1 - 2</pre>	<p>Defines the interface-range macro, and save it in NVRAM.</p> <ul style="list-style-type: none"> • The <i>macro_name</i> is a 32-character maximum character string. • A macro can contain up to five comma-separated interface ranges. • Each <i>interface-range</i> must consist of the same port type. <p>Note Before you can use the macro keyword in the interface range macro global configuration command string, you must use the define interface-range global configuration command to define the macro.</p>
Step 4	interface range macro <i>macro_name</i> Example: <pre>Device(config)# interface range macro enet_list</pre>	<p>Selects the interface range to be configured using the values saved in the interface-range macro called <i>macro_name</i>.</p> <p>You can now use the normal configuration commands to apply the configuration to all interfaces in the defined macro.</p>
Step 5	end Example: <pre>Device(config)# end</pre>	Returns to privileged EXEC mode.
Step 6	show running-config include define Example: <pre>Device# show running-config include define</pre>	Shows the defined interface range macro configuration.
Step 7	copy running-config startup-config Example: <pre>Device# copy running-config</pre>	(Optional) Saves your entries in the configuration file.

	Command or Action	Purpose
	<code>startup-config</code>	

Configuring Ethernet Interfaces

Setting the Interface Speed and Duplex Parameters

Procedure

	Command or Action	Purpose
Step 1	enable Example: <pre>Device> enable</pre>	Enables privileged EXEC mode. <ul style="list-style-type: none"> • Enter your password if prompted.
Step 2	configure terminal Example: <pre>Device# configure terminal</pre>	Enters global configuration mode.
Step 3	interface <i>interface-id</i> Example: <pre>Device(config)# interface gigabitethernet 1/0/3</pre>	Specifies the physical interface to be configured, and enter interface configuration mode.
Step 4	speed {10 100 1000 2500 5000 10000 auto [10 100 1000 2500 5000 10000] nonegotiate} Example: <pre>Device(config-if)# speed 10</pre>	Enter the appropriate speed parameter for the interface: <ul style="list-style-type: none"> • Enter 10, 100, 1000, 2500, 5000, or 10000 to set a specific speed for the interface. • Enter auto to enable the interface to autonegotiate speed with the connected device. If you specify a speed and also set the auto keyword, the port autonegotiates only at the specified speeds. • The nonegotiate keyword is available only for SFP module ports. SFP module ports operate only at 1000 Mb/s but can be configured to not negotiate if connected to a device that does not support autonegotiation.

	Command or Action	Purpose
Step 5	duplex {auto full half} Example: <pre>Device(config-if)# duplex half</pre>	<p>This command is not available on a 10-Gigabit Ethernet interface.</p> <p>Enter the duplex parameter for the interface.</p> <p>Enable half-duplex mode (for interfaces operating only at 10 or 100 Mb/s). You cannot configure half-duplex mode for interfaces operating at 1000 Mb/s.</p> <p>You can configure the duplex setting when the speed is set to auto.</p>
Step 6	end Example: <pre>Device(config-if)# end</pre>	Returns to privileged EXEC mode.
Step 7	show interfaces <i>interface-id</i> Example: <pre>Device# show interfaces gigabitethernet 1/0/3</pre>	Displays the interface speed and duplex mode configuration.
Step 8	copy running-config startup-config Example: <pre>Device# copy running-config startup-config</pre>	(Optional) Saves your entries in the configuration file.

Configuring IEEE 802.3x Flow Control

Procedure

	Command or Action	Purpose
Step 1	configure terminal Example: <pre>Device# configure terminal</pre>	Enters global configuration mode
Step 2	interface <i>interface-id</i> Example: <pre>Device(config)# interface gigabitethernet</pre>	Specifies the physical interface to be configured, and enter interface configuration mode.

	Command or Action	Purpose
	<code>1/0/1</code>	
Step 3	flowcontrol {receive} {on off desired} Example: <pre>Device(config-if)# flowcontrol receive on</pre>	Configures the flow control mode for the port.
Step 4	end Example: <pre>Device(config-if)# end</pre>	Returns to privileged EXEC mode.
Step 5	show interfaces <i>interface-id</i> Example: <pre>Device# show interfaces gigabitethernet 1/0/1</pre>	Verifies the interface flow control settings.
Step 6	copy running-config startup-config Example: <pre>Device# copy running-config startup-config</pre>	(Optional) Saves your entries in the configuration file.

Configuring SVI Autostate Exclude

Procedure

	Command or Action	Purpose
Step 1	enable Example: <pre>Device> enable</pre>	Enables privileged EXEC mode. <ul style="list-style-type: none"> • Enter your password if prompted.
Step 2	configure terminal Example: <pre>Device# configure terminal</pre>	Enters global configuration mode.

	Command or Action	Purpose
Step 3	interface <i>interface-id</i> Example: <pre>Device(config)# interface gigabitethernet1/0/2</pre>	Specifies a Layer 2 interface (physical port or port channel), and enter interface configuration mode.
Step 4	switchport autostate exclude Example: <pre>Device(config-if)# switchport autostate exclude</pre>	Excludes the access or trunk port when defining the status of an SVI line state (up or down)
Step 5	end Example: <pre>Device(config-if)# end</pre>	Returns to privileged EXEC mode.
Step 6	show running config interface <i>interface-id</i>	(Optional) Shows the running configuration. Verifies the configuration.
Step 7	copy running-config startup-config Example: <pre>Device# copy running-config startup-config</pre>	(Optional) Saves your entries in the configuration file.

Shutting Down and Restarting the Interface

Shutting down an interface disables all functions on the specified interface and marks the interface as unavailable on all monitoring command displays. This information is communicated to other network servers through all dynamic routing protocols. The interface is not mentioned in any routing updates.

Procedure

	Command or Action	Purpose
Step 1	enable Example: <pre>Device> enable</pre>	Enables privileged EXEC mode. <ul style="list-style-type: none"> • Enter your password if prompted.
Step 2	configure terminal Example:	Enters global configuration mode.

	Command or Action	Purpose
	Device# configure terminal	
Step 3	interface {vlan <i>vlan-id</i> } { gigabitethernet <i>interface-id</i> } { port-channel <i>port-channel-number</i> } Example: Device(config)# interface gigabitethernet 1/0/2	Selects the interface to be configured.
Step 4	shutdown Example: Device(config-if)# shutdown	Shuts down an interface.
Step 5	no shutdown Example: Device(config-if)# no shutdown	Restarts an interface.
Step 6	end Example: Device(config-if)# end	Returns to privileged EXEC mode.
Step 7	show running-config Example: Device# show running-config	Verifies your entries.

Configuring the Console Media Type

Follow these steps to set the console media type to RJ-45. If you configure the console as RJ-45, USB console operation is disabled, and input comes only through the RJ-45 connector.

This configuration applies to all switches in a stack.

Procedure

	Command or Action	Purpose
Step 1	enable	Enables privileged EXEC mode.

	Command or Action	Purpose
	Example: Device> enable	<ul style="list-style-type: none"> Enter your password if prompted.
Step 2	configure terminal Example: Device# configure terminal	Enters global configuration mode.
Step 3	line console 0 Example: Device(config)# line console 0	Configures the console and enters line configuration mode.
Step 4	media-type rj45 Example: Device(config-line)# media-type rj45	Configures the console media type to be only RJ-45 port. If you do not enter this command and both types are connected, the USB port is used by default.
Step 5	end Example: Device(config)# end	Returns to privileged EXEC mode.
Step 6	copy running-config startup-config Example: Device# copy running-config startup-config	(Optional) Saves your entries in the configuration file.

Configuring the USB Inactivity Timeout

The configurable inactivity timeout reactivates the RJ-45 console port if the USB console port is activated but no input activity occurs on it for a specified time period. When the USB console port is deactivated due to a timeout, you can restore its operation by disconnecting and reconnecting the USB cable.

Procedure

	Command or Action	Purpose
Step 1	enable Example:	Enables privileged EXEC mode. <ul style="list-style-type: none"> Enter your password if prompted.

	Command or Action	Purpose
	Device> enable	
Step 2	configure terminal Example: Device# configure terminal	Enters global configuration mode.
Step 3	line console 0 Example: Device(config)# line console 0	Configures the console and enters line configuration mode.
Step 4	usb-inactivity-timeout <i>timeout-minutes</i> Example: Device(config-line)# usb-inactivity-timeout 30	Specify an inactivity timeout for the console port. The range is 1 to 240 minutes. The default is to have no timeout configured.
Step 5	copy running-config startup-config Example: Device# copy running-config startup-config	(Optional) Saves your entries in the configuration file.

Monitoring Interface Characteristics

Monitoring Interface Status

Commands entered at the privileged EXEC prompt display information about the interface, including the versions of the software and the hardware, the configuration, and statistics about the interfaces.

Table 5: Show Commands for Interfaces

Command	Purpose
show interfaces <i>interface-number</i> downshift <i>module-number</i>	Displays the downshift status details of the specified interfaces and modules.
show interfaces <i>interface-id</i> status [err-disabled]	Displays interface status or a list of interfaces in the error-disabled state.

Command	Purpose
show interfaces [<i>interface-id</i>] switchport	Displays administrative and operational status of switching (nonrouting) ports. You can use this command to find out if a port is in routing or in switching mode.
show interfaces [<i>interface-id</i>] description	Displays the description configured on an interface or all interfaces and the interface status.
show ip interface [<i>interface-id</i>]	Displays the usability status of all interfaces configured for IP routing or the specified interface.
show interface [<i>interface-id</i>] stats	Displays the input and output packets by the switching path for the interface.
show interfaces <i>interface-id</i>	(Optional) Displays speed and duplex on the interface.
show interfaces transceiver dom-supported-list	(Optional) Displays Digital Optical Monitoring (DOM) status on the connect SFP modules.
show interfaces transceiver properties	(Optional) Displays temperature, voltage, or amount of current on the interface.
show interfaces [<i>interface-id</i>] [{ transceiver properties detail }] <i>module number</i>	Displays physical and operational status about an SFP module.
show running-config interface [<i>interface-id</i>]	Displays the running configuration in RAM for the interface.
show version	Displays the hardware configuration, software version, the names and sources of configuration files, and the boot images.
show controllers ethernet-controller <i>interface-id</i> phy	Displays the operational state of the auto-MDIX feature on the interface.

Clearing and Resetting Interfaces and Counters

Table 6: Clear Commands for Interfaces

Command	Purpose
clear counters [<i>interface-id</i>]	Clears interface counters.
clear interface <i>interface-id</i>	Resets the hardware logic on an interface.
clear line [<i>number</i> console 0 vty number]	Resets the hardware logic on an asynchronous serial line.



Note The **clear counters** privileged EXEC command does not clear counters retrieved by using Simple Network Management Protocol (SNMP), but only those seen with the **show interface** privileged EXEC command.

Configuration Examples for Interface Characteristics

Configuring a Range of Interfaces: Examples

This example shows how to use the **interface range** global configuration command to set the speed to 100 Mb/s on ports 1 to 4 on switch 1:

```
Device# configure terminal
Device(config)# interface range gigabitethernet 1/0/1 - 4
Device(config-if-range)# speed 100
```

This example shows how to use a comma to add different interface type strings to the range to enable Gigabit Ethernet ports 1 to 3 and 10-Gigabit Ethernet ports 1 and 2 to receive flow-control pause frames:

```
Device# configure terminal
Device(config)# interface range gigabitethernet1/0/1 - 3 , tengigabitethernet1/1/1 - 2
Device(config-if-range)# flowcontrol receive on
```

If you enter multiple configuration commands while you are in interface-range mode, each command is executed as it is entered. The commands are not batched and executed after you exit interface-range mode. If you exit interface-range configuration mode while the commands are being executed, some commands might not be executed on all interfaces in the range. Wait until the command prompt reappears before exiting interface-range configuration mode.

Configuring and Using Interface Range Macros: Examples

This example shows how to define an interface-range named *enet_list* to include ports 1 and 2 on switch 1 and to verify the macro configuration:

```
Device# configure terminal
Device(config)# define interface-range enet_list gigabitethernet 1/1/1 - 2
Device(config)# end
Device# show running-config | include define
define interface-range enet_list gigabitethernet 1/1/1 - 2
```

This example shows how to create a multiple-interface macro named *macro1*:

```
Device# configure terminal
Device(config)# define interface-range macro1 gigabitethernet1/1/1 - 2, gigabitethernet1/1/5
- 7, tengigabitethernet1/1/1 -2
Device(config)# end
```

This example shows how to enter interface-range configuration mode for the interface-range macro *enet_list*:

```
Device# configure terminal
Device(config)# interface range macro enet_list
Device(config-if-range)#
```

This example shows how to delete the interface-range macro *enet_list* and to verify that it was deleted.

```
Device# configure terminal
Device(config)# no define interface-range enet_list
Device(config)# end
Device# show run | include define
Device#
```

Setting Interface Speed and Duplex Mode: Example

This example shows how to set the interface speed to 100 Mb/s and the duplex mode to half on a 10/100/1000 Mb/s port:

```
Device# configure terminal
Device(config)# interface gigabitethernet 1/0/3
Device(config-if)# speed 10
Device(config-if)# duplex half
```

This example shows how to set the interface speed to 100 Mb/s on a 10/100/1000 Mb/s port:

```
Device# configure terminal
Device(config)# interface gigabitethernet 1/0/2
Device(config-if)# speed 100
```

Configuring the Console Media Type: Example

This example disables the USB console media type and enables the RJ-45 console media type.

```
Device# configure terminal
Device(config)# line console 0
Device(config-line)# media-type rj45
```

This example reverses the previous configuration and immediately activates any USB console that is connected.

```
Device# configure terminal
Device(config)# line console 0
Device(config-line)# no media-type rj45
```

Configuring the USB Inactivity Timeout: Example

This example configures the inactivity timeout to 30 minutes:

```
Device# configure terminal
Device(config)# line console 0
Device(config-line)# usb-inactivity-timeout 30
```

To disable the configuration, use these commands:

```
Device# configure terminal
Device(config)# line console 0
```

```
Device(config-line)# no usb-inactivity-timeout
```

If there is no (input) activity on a USB console port for the configured number of minutes, the inactivity timeout setting applies to the RJ-45 port, and a log shows this occurrence:

```
*Mar 1 00:47:25.625: %USB_CONSOLE-6-INACTIVITY_DISABLE: Console media-type USB disabled
due to inactivity, media-type reverted to RJ45.
```

At this point, the only way to reactivate the USB console port is to disconnect and reconnect the cable.

When the USB cable on the switch has been disconnected and reconnected, a log similar to this appears:

```
*Mar 1 00:48:28.640: %USB_CONSOLE-6-MEDIA_USB: Console media-type is USB.
```

Additional References for the Interface Characteristics Feature

Standards and RFCs

Standard/RFC	Title
None	--

MIBs

MIB	MIBs Link
All the supported MIBs for this release.	To locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use Cisco MIB Locator found at the following URL: http://www.cisco.com/go/mibs

Technical Assistance

Description	Link
<p>The Cisco Support website provides extensive online resources, including documentation and tools for troubleshooting and resolving technical issues with Cisco products and technologies.</p> <p>To receive security and technical information about your products, you can subscribe to various services, such as the Product Alert Tool (accessed from Field Notices), the Cisco Technical Services Newsletter, and Really Simple Syndication (RSS) Feeds.</p> <p>Access to most tools on the Cisco Support website requires a Cisco.com user ID and password.</p>	http://www.cisco.com/support

Feature History and Information for Configuring Interface Characteristics

Release	Modification
Cisco IOS Release 15.0(2)EX	This feature was introduced.



CHAPTER 3

Configuring Auto-MDIX

- [Prerequisites for Auto-MDIX, on page 41](#)
- [Restrictions for Auto-MDIX, on page 41](#)
- [Information About Configuring Auto-MDIX, on page 41](#)
- [How to Configure Auto-MDIX, on page 42](#)
- [Example for Configuring Auto-MDIX, on page 43](#)
- [Additional References, on page 43](#)
- [Feature History and Information for Auto-MDIX, on page 44](#)

Prerequisites for Auto-MDIX

Automatic medium-dependent interface crossover (auto-MDIX) is enabled by default.

Auto-MDIX is supported on all 10/100/1000-Mb/s and on 10/100/1000BASE-TX small form-factor pluggable (SFP)-module interfaces. It is not supported on 1000BASE-SX or -LX SFP module interfaces.

Restrictions for Auto-MDIX

The device might not support a pre-standard powered device—such as Cisco IP phones and access points that do not fully support IEEE 802.3af—if that powered device is connected to the device through a crossover cable. This is regardless of whether auto-MDIX is enabled on the switch port.

Information About Configuring Auto-MDIX

Auto-MDIX on an Interface

When automatic medium-dependent interface crossover (auto-MDIX) is enabled on an interface, the interface automatically detects the required cable connection type (straight through or crossover) and configures the connection appropriately. When connecting devices without the auto-MDIX feature, you must use straight-through cables to connect to devices such as servers, workstations, or routers and crossover cables to connect to other devices or repeaters. With auto-MDIX enabled, you can use either type of cable to connect to other devices, and the interface automatically corrects for any incorrect cabling. For more information about cabling requirements, see the hardware installation guide.

This table shows the link states that result from auto-MDIX settings and correct and incorrect cabling.

Table 7: 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
Off	On	Link up	Link up
Off	Off	Link up	Link down

How to Configure Auto-MDIX

Configuring Auto-MDIX on an Interface

Procedure

	Command or Action	Purpose
Step 1	enable Example: <pre>Device> enable</pre>	Enables privileged EXEC mode. <ul style="list-style-type: none"> • Enter your password if prompted.
Step 2	configure terminal Example: <pre>Device# configure terminal</pre>	Enters global configuration mode
Step 3	interface <i>interface-id</i> Example: <pre>Device(config)# interface gigabitethernet 1/0/1</pre>	Specifies the physical interface to be configured, and enter interface configuration mode.
Step 4	speed auto Example: <pre>Device(config-if)# speed auto</pre>	Configures the interface to autonegotiate speed with the connected device.
Step 5	duplex auto Example:	Configures the interface to autonegotiate duplex mode with the connected device.

	Command or Action	Purpose
	Device(config-if) # duplex auto	
Step 6	end Example: Device(config-if) # end	Returns to privileged EXEC mode.
Step 7	copy running-config startup-config Example: Device# copy running-config startup-config	(Optional) Saves your entries in the configuration file.

Example for Configuring Auto-MDIX

This example shows how to enable auto-MDIX on a port:

```
Device# configure terminal
Device(config)# interface gigabitethernet 1/0/1
Device(config-if)# speed auto
Device(config-if)# duplex auto
Device(config-if)# mdix auto
Device(config-if)# end
```

Additional References

MIBs

MIB	MIBs Link
All the supported MIBs for this release.	To locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use Cisco MIB Locator found at the following URL: http://www.cisco.com/go/mibs

Technical Assistance

Description	Link
<p>The Cisco Support website provides extensive online resources, including documentation and tools for troubleshooting and resolving technical issues with Cisco products and technologies.</p> <p>To receive security and technical information about your products, you can subscribe to various services, such as the Product Alert Tool (accessed from Field Notices), the Cisco Technical Services Newsletter, and Really Simple Syndication (RSS) Feeds.</p> <p>Access to most tools on the Cisco Support website requires a Cisco.com user ID and password.</p>	http://www.cisco.com/support

Feature History and Information for Auto-MDIX

Release	Modification
Cisco IOS Release 15.0(2)EX	This feature was introduced.



CHAPTER 4

Configuring Ethernet Management Port

- [Prerequisites for Ethernet Management Ports, on page 45](#)
- [Information About the Ethernet Management Port, on page 45](#)
- [How to Configure the Ethernet Management Port, on page 47](#)
- [Additional References for Ethernet Management Ports, on page 48](#)
- [Feature History and Information for Ethernet Management Ports, on page 48](#)

Prerequisites for Ethernet Management Ports

When connecting a PC to the Ethernet management port, you must first assign an IP address.

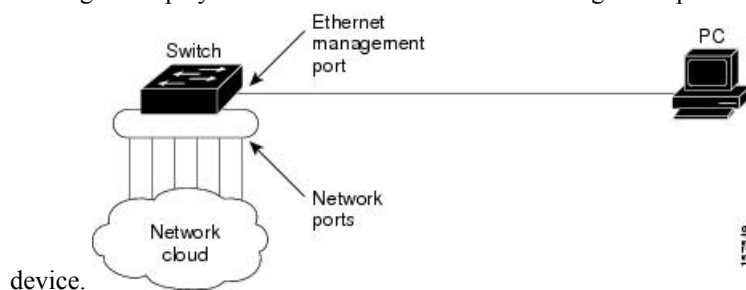
Information About the Ethernet Management Port

The Ethernet management port, also referred to as the *Fa0* or *fastethernet0* port, is a Layer 3 host port to which you can connect a PC. You can use the Ethernet management port instead of the device console port for network management. When managing a device stack, connect the PC to the Ethernet management port on a stack member.

Ethernet Management Port Direct Connection to a Device

Figure 2: Connecting a Switch to a PC

This figure displays how to connect the Ethernet management port to the PC for a device or a standalone

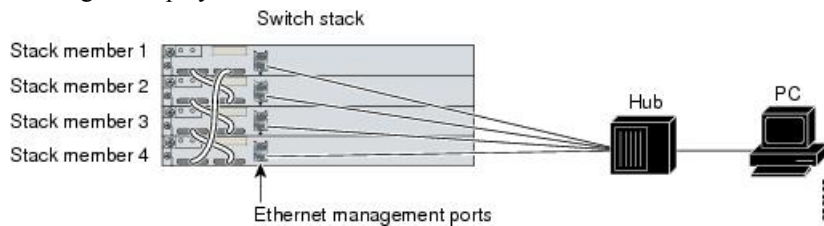


Ethernet Management Port Connection to Stack Devices using a Hub

In a stack with only stack devices, all the Ethernet management ports on the stack members are connected to a hub to which the PC is connected. The active link is from the Ethernet management port on the stack's active switch through the hub, to the PC. If the active device fails and a new active device is elected, the active link is now from the Ethernet management port on the new active device to the PC.

Figure 3: Connecting a Device Stack to a PC

This figure displays how a PC uses a hub to connect to a device stack.



Supported Features on the Ethernet Management Port

The Ethernet management port supports these features:

- Express Setup (only in switch stacks)
- Network Assistant
- Telnet with passwords
- TFTP
- Secure Shell (SSH)
- DHCP-based autoconfiguration
- SNMP (only the ENTITY-MIB and the IF-MIB)
- IP ping
- Interface features
 - Speed—10 Mb/s, 100 Mb/s, and autonegotiation
 - Duplex mode—Full, half, and autonegotiation
 - Loopback detection
- Cisco Discovery Protocol (CDP)
- DHCP relay agent
- IPv4 and IPv6 access control lists (ACLs)



Caution

Before enabling a feature on the Ethernet management port, make sure that the feature is supported. If you try to configure an unsupported feature on the Ethernet Management port, the feature might not work properly, and the device might fail.

How to Configure the Ethernet Management Port

Disabling and Enabling the Ethernet Management Port

Procedure

	Command or Action	Purpose
Step 1	configure terminal Example: Device# <code>configure terminal</code>	Enters global configuration mode.
Step 2	interface fastethernet0 Example: Device(config)# <code>interface fastethernet0</code>	Specifies the Ethernet management port in the CLI.
Step 3	shutdown Example: Device(config-if)# <code>shutdown</code>	Disables the Ethernet management port.
Step 4	no shutdown Example: Device(config-if)# <code>no shutdown</code>	Enables the Ethernet management port.
Step 5	exit Example: Device(config-if)# <code>exit</code>	Exits interface configuration mode.
Step 6	show interfaces fastethernet0 Example: Device# <code>show interfaces fastethernet0</code>	Displays the link status. To find out the link status to the PC, you can monitor the LED for the Ethernet management port. The LED is green (on) when the link is active, and the LED is off when the link is down. The LED is amber when there is a POST failure.

What to do next

Proceed to manage or configure your switch using the Ethernet management port. Refer to the *Catalyst 2960-X Switch Network Management Configuration Guide*.

Additional References for Ethernet Management Ports

Related Documents

Related Topic	Document Title
Bootloader configuration	<i>Catalyst 2960-X Switch System Management Configuration Guide</i>
Bootloader commands	<i>Catalyst 2960-X Switch System Management Configuration Guide</i>

MIBs

MIB	MIBs Link
All the supported MIBs for this release.	To locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use Cisco MIB Locator found at the following URL: http://www.cisco.com/go/mibs

Technical Assistance

Description	Link
<p>The Cisco Support website provides extensive online resources, including documentation and tools for troubleshooting and resolving technical issues with Cisco products and technologies.</p> <p>To receive security and technical information about your products, you can subscribe to various services, such as the Product Alert Tool (accessed from Field Notices), the Cisco Technical Services Newsletter, and Really Simple Syndication (RSS) Feeds.</p> <p>Access to most tools on the Cisco Support website requires a Cisco.com user ID and password.</p>	http://www.cisco.com/support

Feature History and Information for Ethernet Management Ports

Release	Modification
Cisco IOS Release 15.0(2)EX	This feature was introduced.



CHAPTER 5

Configuring LLDP, LLDP-MED, and Wired Location Service

- [Information About LLDP, LLDP-MED, and Wired Location Service, on page 49](#)
- [How to Configure LLDP, LLDP-MED, and Wired Location Service, on page 53](#)
- [Configuration Examples for LLDP, LLDP-MED, and Wired Location Service, on page 63](#)
- [Monitoring and Maintaining LLDP, LLDP-MED, and Wired Location Service, on page 64](#)
- [Additional References for LLDP, LLDP-MED, and Wired Location Service, on page 65](#)
- [Feature Information for LLDP, LLDP-MED, and Wired Location Service, on page 65](#)

Information About LLDP, LLDP-MED, and Wired Location Service

LLDP

The Cisco Discovery Protocol (CDP) is a device discovery protocol that runs over Layer 2 (the data link layer) on all Cisco-manufactured devices (routers, bridges, access servers, switches, and controllers). CDP allows network management applications to automatically discover and learn about other Cisco devices connected to the network.

To support non-Cisco devices and to allow for interoperability between other devices, the device supports the IEEE 802.1AB Link Layer Discovery Protocol (LLDP). LLDP is a neighbor discovery protocol that is used for network devices to advertise information about themselves to other devices on the network. This protocol runs over the data-link layer, which allows two systems running different network layer protocols to learn about each other.

LLDP Supported TLVs

LLDP supports a set of attributes that it uses to discover neighbor devices. These attributes contain type, length, and value descriptions and are referred to as TLVs. LLDP supported devices can use TLVs to receive and send information to their neighbors. This protocol can advertise details such as configuration information, device capabilities, and device identity.

The switch supports these basic management TLVs. These are mandatory LLDP TLVs.

- Port description TLV
- System name TLV

- System description TLV
- System capabilities TLV
- Management address TLV

These organizationally specific LLDP TLVs are also advertised to support LLDP-MED.

- Port VLAN ID TLV (IEEE 802.1 organizationally specific TLVs)
- MAC/PHY configuration/status TLV (IEEE 802.3 organizationally specific TLVs)

LLDP and Cisco Device Stacks

A device stack appears as a single device in the network. Therefore, LLDP discovers the device stack, not the individual stack members.

LLDP and Cisco Medianet

When you configure LLDP or CDP location information on a per-port basis, remote devices can send Cisco Medianet location information to the device.

LLDP-MED

LLDP for Media Endpoint Devices (LLDP-MED) is an extension to LLDP that operates between endpoint devices such as IP phones and network devices. It specifically provides support for voice over IP (VoIP) applications and provides additional TLVs for capabilities discovery, network policy, Power over Ethernet, inventory management and location information. By default, all LLDP-MED TLVs are enabled.

LLDP-MED Supported TLVs

LLDP-MED supports these TLVs:

- LLDP-MED capabilities TLV

Allows LLDP-MED endpoints to determine the capabilities that the connected device supports and has enabled.

- Network policy TLV

Allows both network connectivity devices and endpoints to advertise VLAN configurations and associated Layer 2 and Layer 3 attributes for the specific application on that port. For example, the switch can notify a phone of the VLAN number that it should use. The phone can connect to any device, obtain its VLAN number, and then start communicating with the call control.

By defining a network-policy profile TLV, you can create a profile for voice and voice-signaling by specifying the values for VLAN, class of service (CoS), differentiated services code point (DSCP), and tagging mode. These profile attributes are then maintained centrally on the switch and propagated to the phone.

- Power management TLV

Enables advanced power management between LLDP-MED endpoint and network connectivity devices. Allows devices and phones to convey power information, such as how the device is powered, power priority, and how much power the device needs.

LLDP-MED also supports an extended power TLV to advertise fine-grained power requirements, end-point power priority, and end-point and network connectivity-device power status. LLDP is enabled and power is applied to a port, the power TLV determines the actual power requirement of the endpoint device so that the system power budget can be adjusted accordingly. The device processes the requests and either grants or denies power based on the current power budget. If the request is granted, the switch updates the power budget. If the request is denied, the device turns off power to the port, generates a syslog message, and updates the power budget. If LLDP-MED is disabled or if the endpoint does not support the LLDP-MED power TLV, the initial allocation value is used throughout the duration of the connection.

You can change power settings by entering the **power inline** {**auto** [**max** *max-wattage*] | **never** | **static** [**max** *max-wattage*]} interface configuration command. By default the PoE interface is in **auto** mode; If no value is specified, the maximum is allowed (30 W).

- Inventory management TLV

Allows an endpoint to send detailed inventory information about itself to the device, including information hardware revision, firmware version, software version, serial number, manufacturer name, model name, and asset ID TLV.

- Location TLV

Provides location information from the device to the endpoint device. The location TLV can send this information:

- Civic location information

Provides the civic address information and postal information. Examples of civic location information are street address, road name, and postal community name information.

- ELIN location information

Provides the location information of a caller. The location is determined by the Emergency location identifier number (ELIN), which is a phone number that routes an emergency call to the local public safety answering point (PSAP) and which the PSAP can use to call back the emergency caller.

Wired Location Service

The device uses the location service feature to send location and attachment tracking information for its connected devices to a Cisco Mobility Services Engine (MSE). The tracked device can be a wireless endpoint, a wired endpoint, or a wired device or controller. The device notifies the MSE of device link up and link down events through the Network Mobility Services Protocol (NMSP) location and attachment notifications.

The MSE starts the NMSP connection to the device, which opens a server port. When the MSE connects to the device there are a set of message exchanges to establish version compatibility and service exchange information followed by location information synchronization. After connection, the device periodically sends location and attachment notifications to the MSE. Any link up or link down events detected during an interval are aggregated and sent at the end of the interval.

When the device determines the presence or absence of a device on a link-up or link-down event, it obtains the client-specific information such as the MAC address, IP address, and username. If the client is LLDP-MED- or CDP-capable, the device obtains the serial number and UDI through the LLDP-MED location TLV or CDP.

Depending on the device capabilities, the device obtains this client information at link up:

- Slot and port specified in port connection

- MAC address specified in the client MAC address
- IP address specified in port connection
- 802.1X username if applicable
- Device category is specified as a *wired station*
- State is specified as *new*
- Serial number, UDI
- Model number
- Time in seconds since the device detected the association

Depending on the device capabilities, the device obtains this client information at link down:

- Slot and port that was disconnected
- MAC address
- IP address
- 802.1X username if applicable
- Device category is specified as a *wired station*
- State is specified as *delete*
- Serial number, UDI
- Time in seconds since the device detected the disassociation

When the device shuts down, it sends an attachment notification with the state *delete* and the IP address before closing the NMSP connection to the MSE. The MSE interprets this notification as disassociation for all the wired clients associated with the device.

If you change a location address on the device, the device sends an NMSP location notification message that identifies the affected ports and the changed address information.

Default LLDP Configuration

Table 8: Default LLDP Configuration

Feature	Default Setting
LLDP global state	Disabled
LLDP holdtime (before discarding)	120 seconds
LLDP timer (packet update frequency)	30 seconds
LLDP reinitialization delay	2 seconds
LLDP tlv-select	Disabled to send and receive all TLVs
LLDP interface state	Disabled

Feature	Default Setting
LLDP receive	Disabled
LLDP transmit	Disabled
LLDP med-tlv-select	Disabled to send all LLDP-MED TLVs. When LLDP is glob LLDP-MED-TLV is also enabled.

Restrictions for LLDP

- If the interface is configured as a tunnel port, LLDP is automatically disabled.
- If you first configure a network-policy profile on an interface, you cannot apply the **switchport voice vlan** command on the interface. If the **switchport voice vlan** *vlan-id* is already configured on an interface, you can apply a network-policy profile on the interface. This way the interface has the voice or voice-signaling VLAN network-policy profile applied on the interface.
- You cannot configure static secure MAC addresses on an interface that has a network-policy profile.
- When Cisco Discovery Protocol and LLDP are both in use within the same switch, it is necessary to disable LLDP on interfaces where Cisco Discovery Protocol is in use for power negotiation. LLDP can be disabled at interface level with the commands **no lldp tlv-select power-management** or **no lldp transmit / no lldp receive**.

How to Configure LLDP, LLDP-MED, and Wired Location Service

Enabling LLDP

Procedure

	Command or Action	Purpose
Step 1	enable Example: Device> enable	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	configure terminal Example: Device# configure terminal	Enters global configuration mode.
Step 3	lldp run Example:	Enables LLDP globally on the device.

	Command or Action	Purpose
	Device (config)# lldp run	
Step 4	interface <i>interface-id</i> Example: Device (config)# interface gigabitethernet 2/0/1	Specifies the interface on which you are enabling LLDP, and enter interface configuration mode.
Step 5	lldp transmit Example: Device (config-if)# lldp transmit	Enables the interface to send LLDP packets.
Step 6	lldp receive Example: Device (config-if)# lldp receive	Enables the interface to receive LLDP packets.
Step 7	end Example: Device (config-if)# end	Returns to privileged EXEC mode.
Step 8	show lldp Example: Device# show lldp	Verifies the configuration.
Step 9	copy running-config startup-config Example: Device# copy running-config startup-config	(Optional) Saves your entries in the configuration file.

Configuring LLDP Characteristics

You can configure the frequency of LLDP updates, the amount of time to hold the information before discarding it, and the initialization delay time. You can also select the LLDP and LLDP-MED TLVs to send and receive.



Note Steps 3 through 6 are optional and can be performed in any order.

Procedure

	Command or Action	Purpose
Step 1	enable Example: Device> enable	Enables privileged EXEC mode. <ul style="list-style-type: none"> • Enter your password if prompted.
Step 2	configure terminal Example: Device# configure terminal	Enters global configuration mode.
Step 3	lldp holdtime <i>seconds</i> Example: Device(config)# lldp holdtime 120	(Optional) Specifies the amount of time a receiving device should hold the information from your device before discarding it. The range is 0 to 65535 seconds; the default is 120 seconds.
Step 4	lldp reinit <i>delay</i> Example: Device(config)# lldp reinit 2	(Optional) Specifies the delay time in seconds for LLDP to initialize on an interface. The range is 2 to 5 seconds; the default is 2 seconds.
Step 5	lldp timer <i>rate</i> Example: Device(config)# lldp timer 30	(Optional) Sets the sending frequency of LLDP updates in seconds. The range is 5 to 65534 seconds; the default is 30 seconds.
Step 6	lldp tlv-select Example: Device(config)# tlv-select	(Optional) Specifies the LLDP TLVs to send or receive.
Step 7	interface <i>interface-id</i> Example: Device (config)# interface gigabitethernet 2/0/1	Specifies the interface on which you are enabling LLDP, and enter interface configuration mode.

	Command or Action	Purpose
Step 8	lldp med-tlv-select Example: <pre>Device (config-if)# lldp med-tlv-select inventory management</pre>	(Optional) Specifies the LLDP-MED TLVs to send or receive.
Step 9	end Example: <pre>Device (config-if)# end</pre>	Returns to privileged EXEC mode.
Step 10	show lldp Example: <pre>Device# show lldp</pre>	Verifies the configuration.
Step 11	copy running-config startup-config Example: <pre>Device# copy running-config startup-config</pre>	(Optional) Saves your entries in the configuration file.

Configuring LLDP-MED TLVs

By default, the device only sends LLDP packets until it receives LLDP-MED packets from the end device. It then sends LLDP packets with MED TLVs, as well. When the LLDP-MED entry has been aged out, it again only sends LLDP packets.

By using the **lldp** interface configuration command, you can configure the interface not to send the TLVs listed in the following table.

Table 9: LLDP-MED TLVs

LLDP-MED TLV	Description
inventory-management	LLDP-MED inventory management TLV
location	LLDP-MED location TLV
network-policy	LLDP-MED network policy TLV
power-management	LLDP-MED power management TLV

Follow these steps to enable a TLV on an interface:

Procedure

	Command or Action	Purpose
Step 1	enable Example: <pre>Device> enable</pre>	Enables privileged EXEC mode. <ul style="list-style-type: none"> • Enter your password if prompted.
Step 2	configure terminal Example: <pre>Device# configure terminal</pre>	Enters global configuration mode.
Step 3	interface <i>interface-id</i> Example: <pre>Device (config)# interface gigabitethernet 2/0/1</pre>	Specifies the interface on which you are enabling LLDP, and enter interface configuration mode.
Step 4	lldp med-tlv-select Example: <pre>Device(config-if)# lldp med-tlv-select inventory management</pre>	Specifies the TLV to enable.
Step 5	end Example: <pre>Device(config-if)# end</pre>	Returns to privileged EXEC mode.
Step 6	copy running-config startup-config Example: <pre>Device# copy running-config startup-config</pre>	(Optional) Saves your entries in the configuration file.

Configuring Network-Policy TLV

Procedure

	Command or Action	Purpose
Step 1	enable	Enables privileged EXEC mode.

	Command or Action	Purpose
	Example: Device> enable	<ul style="list-style-type: none"> • Enter your password if prompted.
Step 2	configure terminal Example: Device# configure terminal	Enters global configuration mode.
Step 3	network-policy profile <i>profile number</i> Example: Device (config)# network-policy profile 1	Specifies the network-policy profile number, and enter network-policy configuration mode. The range is 1 to 4294967295.
Step 4	{voice voice-signaling} vlan [vlan-id {cos cvalue dscp dvalue}] [[dot1p {cos cvalue dscp dvalue}] none untagged] Example: Device (config-network-policy)# voice vlan 100 cos 4	Configures the policy attributes: <ul style="list-style-type: none"> • voice—Specifies the voice application type. • voice-signaling—Specifies the voice-signaling application type. • vlan—Specifies the native VLAN for voice traffic. • vlan-id—(Optional) Specifies the VLAN for voice traffic. The range is 1 to 4094. • cos cvalue—(Optional) Specifies the Layer 2 priority class of service (CoS) for the configured VLAN. The range is 0 to 7; the default is 5. • dscp dvalue—(Optional) Specifies the differentiated services code point (DSCP) value for the configured VLAN. The range is 0 to 63; the default is 46. • dot1p—(Optional) Configures the telephone to use IEEE 802.1p priority tagging and use VLAN 0 (the native VLAN). • none—(Optional) Do not instruct the IP telephone about the voice VLAN. The telephone uses the configuration from the telephone key pad.

	Command or Action	Purpose
		<ul style="list-style-type: none"> • untagged—(Optional) Configures the telephone to send untagged voice traffic. This is the default for the telephone. • untagged—(Optional) Configures the telephone to send untagged voice traffic. This is the default for the telephone.
Step 5	exit Example: <pre>Device(config)# exit</pre>	Returns to global configuration mode.
Step 6	interface interface-id Example: <pre>Device (config)# interface gigabitethernet 2/0/1</pre>	Specifies the interface on which you are configuring a network-policy profile, and enter interface configuration mode.
Step 7	network-policy profile number Example: <pre>Device(config-if)# network-policy 1</pre>	Specifies the network-policy profile number.
Step 8	lldp med-tlv-select network-policy Example: <pre>Device(config-if)# lldp med-tlv-select network-policy</pre>	Specifies the network-policy TLV.
Step 9	end Example: <pre>Device(config)# end</pre>	Returns to privileged EXEC mode.
Step 10	show network-policy profile Example: <pre>Device# show network-policy profile</pre>	Verifies the configuration.
Step 11	copy running-config startup-config Example:	(Optional) Saves your entries in the configuration file.

	Command or Action	Purpose
	Device# copy running-config startup-config	

Configuring Location TLV and Wired Location Service

Beginning in privileged EXEC mode, follow these steps to configure location information for an endpoint and to apply it to an interface.

Procedure

	Command or Action	Purpose
Step 1	configure terminal Example: Device# configure terminal	Enters global configuration mode.
Step 2	location {admin-tag <i>string</i> civic-location identifier {<i>id</i> <i>host</i>} elin-location <i>string</i> identifier <i>id</i> custom-location identifier {<i>id</i> <i>host</i>} geo-location identifier {<i>id</i> <i>host</i>}} Example: Device(config)# location civic-location identifier 1 Device(config-civic)# number 3550 Device(config-civic)# primary-road-name "Cisco Way" Device(config-civic)# city "San Jose" Device(config-civic)# state CA Device(config-civic)# building 19 Device(config-civic)# room C6 Device(config-civic)# county "Santa Clara" Device(config-civic)# country US	Specifies the location information for an endpoint. <ul style="list-style-type: none"> • admin-tag—Specifies an administrative tag or site information. • civic-location—Specifies civic location information. • elin-location—Specifies emergency location information (ELIN). • custom-location—Specifies custom location information. • geo-location—Specifies geo-spatial location information. • identifier <i>id</i>—Specifies the ID for the civic, ELIN, custom, or geo location. • host—Specifies the host civic, custom, or geo location. • string—Specifies the site or location information in alphanumeric format.
Step 3	exit Example: Device(config-civic)# exit	Returns to global configuration mode.

	Command or Action	Purpose
Step 4	interface <i>interface-id</i> Example: <pre>Device (config)# interface gigabitethernet2/0/1</pre>	Specifies the interface on which you are configuring the location information, and enter interface configuration mode.
Step 5	location { additional-location-information <i>word</i> civic-location-id { <i>id</i> <i>host</i> } elin-location-id <i>id</i> custom-location-id { <i>id</i> <i>host</i> } geo-location-id { <i>id</i> <i>host</i> } } Example: <pre>Device(config-if)# location elin-location-id 1</pre>	Enters location information for an interface: <ul style="list-style-type: none"> • additional-location-information—Specifies additional information for a location or place. • civic-location-id—Specifies global civic location information for an interface. • elin-location-id—Specifies emergency location information for an interface. • custom-location-id—Specifies custom location information for an interface. • geo-location-id—Specifies geo-spatial location information for an interface. • host—Specifies the host location identifier. • <i>word</i>—Specifies a word or phrase with additional location information. • <i>id</i>—Specifies the ID for the civic, ELIN, custom, or geo location. The ID range is 1 to 4095.
Step 6	end Example: <pre>Device(config-if)# end</pre>	Returns to privileged EXEC mode.
Step 7	Use one of the following: <ul style="list-style-type: none"> • show location admin-tag <i>string</i> • show location civic-location identifier <i>id</i> • show location elin-location identifier <i>id</i> Example: <pre>Device# show location admin-tag</pre> <p>or</p>	Verifies the configuration.

	Command or Action	Purpose
	<pre>Device# show location civic-location identifier</pre> <p>OR</p> <pre>Device# show location elin-location identifier</pre>	
Step 8	copy running-config startup-config Example: <pre>Device# copy running-config startup-config</pre>	(Optional) Saves your entries in the configuration file.

Enabling Wired Location Service on the Device

Before you begin

For wired location to function, you must first enter the **ip device tracking** global configuration command.

Procedure

	Command or Action	Purpose
Step 1	enable Example: <pre>Device> enable</pre>	Enables privileged EXEC mode. <ul style="list-style-type: none"> • Enter your password if prompted.
Step 2	configure terminal Example: <pre>Device# configure terminal</pre>	Enters global configuration mode.
Step 3	nmosp notification interval {attachment location} interval-seconds Example: <pre>Device(config)# nmosp notification interval location 10</pre>	Specifies the NMSP notification interval. attachment —Specifies the attachment notification interval. location —Specifies the location notification interval. <i>interval-seconds</i> —Duration in seconds before the device sends the MSE the location or attachment updates. The range is 1 to 30; the default is 30.

	Command or Action	Purpose
Step 4	end Example: Device(config) # end	Returns to privileged EXEC mode.
Step 5	show network-policy profile Example: Device# show network-policy profile	Verifies the configuration.
Step 6	copy running-config startup-config Example: Device# copy running-config startup-config	(Optional) Saves your entries in the configuration file.

Configuration Examples for LLDP, LLDP-MED, and Wired Location Service

Configuring Network-Policy TLV: Examples

This example shows how to configure VLAN 100 for voice application with CoS and to enable the network-policy profile and network-policy TLV on an interface:

```
# configure terminal
(config)# network-policy 1
(config-network-policy)# voice vlan 100 cos 4
(config-network-policy)# exit
(config)# interface gigabitethernet 1/0/1
(config-if)# network-policy profile 1
(config-if)# lldp med-tlv-select network-policy
```

This example shows how to configure the voice application type for the native VLAN with priority tagging:

```
config-network-policy)# voice vlan dot1p cos 4
config-network-policy)# voice vlan dot1p dscp 34
```

Monitoring and Maintaining LLDP, LLDP-MED, and Wired Location Service

Commands for monitoring and maintaining LLDP, LLDP-MED, and wired location service.

Command	Description
clear lldp counters	Resets the traffic counters to zero.
clear lldp table	Deletes the LLDP neighbor information table.
clear nmosp statistics	Clears the NMSP statistic counters.
show lldp	Displays global information, such as frequency of transmissions, the holdtime for packets being sent, and the delay time before LLDP initializes on an interface.
show lldp entry <i>entry-name</i>	Displays information about a specific neighbor. You can enter an asterisk (*) to display all neighbors, or you can enter the neighbor name.
show lldp interface [<i>interface-id</i>]	Displays information about interfaces with LLDP enabled. You can limit the display to a specific interface.
show lldp neighbors [<i>interface-id</i>] [detail]	Displays information about neighbors, including device type, interface type and number, holdtime settings, capabilities, and port ID. You can limit the display to neighbors of a specific interface or expand the display for more detailed information.
show lldp traffic	Displays LLDP counters, including the number of packets sent and received, number of packets discarded, and number of unrecognized TLVs.
show location admin-tag <i>string</i>	Displays the location information for the specified administrative tag or site.
show location civic-location identifier <i>id</i>	Displays the location information for a specific global civic location.
show location elin-location identifier <i>id</i>	Displays the location information for an emergency location
show network-policy profile	Displays the configured network-policy profiles.
show nmosp	Displays the NMSP information

Additional References for LLDP, LLDP-MED, and Wired Location Service

MIBs

MIB	MIBs Link
All the supported MIBs for this release.	To locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use Cisco MIB Locator found at the following URL: http://www.cisco.com/go/mibs

Technical Assistance

Description	Link
<p>The Cisco Support website provides extensive online resources, including documentation and tools for troubleshooting and resolving technical issues with Cisco products and technologies.</p> <p>To receive security and technical information about your products, you can subscribe to various services, such as the Product Alert Tool (accessed from Field Notices), the Cisco Technical Services Newsletter, and Really Simple Syndication (RSS) Feeds.</p> <p>Access to most tools on the Cisco Support website requires a Cisco.com user ID and password.</p>	http://www.cisco.com/support

Feature Information for LLDP, LLDP-MED, and Wired Location Service

Release	Modification
Cisco IOS Release 15.0(2)EX	This feature was introduced.



CHAPTER 6

Configuring System MTU

- [Information About the MTU](#), on page 67
- [How to Configure MTU](#), on page 68
- [Configuration Examples for System MTU](#), on page 69
- [Additional References for System MTU](#), on page 69
- [Feature Information for System MTU](#), on page 70

Information About the MTU

The default maximum transmission unit (MTU) size for frames received and transmitted on all interfaces is 1500 bytes. You can increase the MTU size for all interfaces operating at 10 or 100 Mb/s by using the **system mtu** global configuration command. You can increase the MTU size to support jumbo frames on all Gigabit Ethernet interfaces by using the **system mtu jumbo** global configuration command.



Note The switch supports jumbo frames at CPU.

System MTU Guidelines

When configuring the system MTU values, follow these guidelines:

- The default maximum transmission unit (MTU) size for frames received and transmitted on all interfaces is 1500 bytes. You can increase the MTU size for all interfaces operating at 10 or 100 Mb/s by using the **system mtu** global configuration command. You can increase the MTU size to support jumbo frames on all Gigabit Ethernet interfaces by using the **system mtu jumbo** global configuration command.
- Gigabit Ethernet ports are not affected by the **system mtu** command; 10/100 ports are not affected by the **system mtu jumbo** command. If you do not configure the **system mtu jumbo** command, the setting of the **system mtu** command applies to all Gigabit Ethernet interfaces.
- When you change the size of the system MTU, reload the device for the new MTU value to take effect.



Note If Layer 2 Gigabit Ethernet interfaces are configured to accept frames greater than the 10/100 interfaces, jumbo frames received on a Layer 2 Gigabit Ethernet interface and sent on a Layer 2 10/100 interface are dropped.

How to Configure MTU

Configuring the System MTU

Beginning in privileged EXEC mode, follow these steps to change the MTU size for all 10/100 or Gigabit Ethernet interfaces:

Procedure

	Command or Action	Purpose
Step 1	configure terminal Example: Device# configure terminal	Enters global configuration mode.
Step 2	system mtu <i>bytes</i> Example: Device(config)# system mtu 2500	(Optional) Change the MTU size for all interfaces on the switch stack that are operating at 10 or 100 Mb/s. The range is 1500 to 9198 bytes; the default is 1500 bytes.
Step 3	system mtu jumbo <i>bytes</i> Example: Device(config)# system mtu jumbo7500	(Optional) Changes the MTU size for all Gigabit Ethernet interfaces on the switch or the switch stack. The range is 1500 to 9198 bytes; the default is 1500 bytes.
Step 4	end Example: Device(config)# end	Returns to privileged EXEC mode.
Step 5	copy running-config startup-config Example: Device# copy running-config startup-config	Saves your entries in the configuration file.
Step 6	show system mtu Example: Device# show system mtu	Verifies your settings.

Configuration Examples for System MTU

This example shows how to set the maximum packet size for a Gigabit Ethernet port to 7500 bytes:

```
Device(config)# system mtu 7500
Device(config)# exit
```

This example shows how to set the jumbo packet size for a Gigabit Ethernet port to 7500 bytes:

```
Device(config)# system mtu jumbo 7500
Device(config)# exit
```

If you enter a value that is outside the allowed range for the specific type of interface, the value is not accepted. This example shows the response when you try to set Gigabit Ethernet interfaces to an out-of-range number:

```
Device(config)# system mtu jumbo 25000
                        ^
% Invalid input detected at '^' marker.
```

Additional References for System MTU

MIBs

MIB	MIBs Link
All the supported MIBs for this release.	To locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use Cisco MIB Locator found at the following URL: http://www.cisco.com/go/mibs

Technical Assistance

Description	Link
The Cisco Support website provides extensive online resources, including documentation and tools for troubleshooting and resolving technical issues with Cisco products and technologies. To receive security and technical information about your products, you can subscribe to various services, such as the Product Alert Tool (accessed from Field Notices), the Cisco Technical Services Newsletter, and Really Simple Syndication (RSS) Feeds. Access to most tools on the Cisco Support website requires a Cisco.com user ID and password.	http://www.cisco.com/support

Feature Information for System MTU

Release	Modification
Cisco IOS Release 15.0(2)EX	This feature was introduced.



CHAPTER 7

Configuring Boot Fast

- [Configuring Boot Fast on the switch, on page 71](#)

Configuring Boot Fast on the switch

This features when enabled, helps the switch to Boot up fast. The Memory test is performed for a limited range, the switch Skips File system check (FSCK) and Skips Post test.



Note When Fast boot is enabled, you can still run the POST tests manually from the command line interface, once the switch has booted up, using **diagnostic start** command.

Enabling Boot Fast

To enable the boot fast feature, perform the following steps:

Procedure

	Command or Action	Purpose
Step 1	enable Example: Device> enable	Enables privileged EXEC mode. <ul style="list-style-type: none">• Enter your password if prompted.
Step 2	configure terminal Example: Device# configure terminal	Enters global configuration mode.
Step 3	boot fast Example:	Enables fast boot feature Performs Memory test for a limited range, Skips File system check (FSCK) and Skips Post test.

	Command or Action	Purpose
	Device(config)# boot fast	
Step 4	end Example: Device(config)# end	Returns to privileged EXEC mode.

Disabling Boot Fast

To disable the boot fast feature, perform the following steps:

Procedure

	Command or Action	Purpose
Step 1	enable Example: Device> enable	Enables privileged EXEC mode. <ul style="list-style-type: none"> • Enter your password if prompted.
Step 2	configure terminal Example: Device# configure terminal	Enters global configuration mode.
Step 3	no boot fast Example: Device(config)# no boot fast	Disables the boot fast feature.
Step 4	end Example: Device(config)# end	Returns to privileged EXEC mode.



CHAPTER 8

Configuring Power over Ethernet

- [Restrictions for PoE, on page 73](#)
- [Information About PoE, on page 73](#)
- [How to Configure PoE, on page 78](#)
- [Monitoring Power Status, on page 86](#)
- [Configuration Examples for Configuring PoE, on page 86](#)
- [Additional References, on page 87](#)

Restrictions for PoE



Note This feature is supported only on the LAN Base image.

Information About PoE

Power over Ethernet Ports

A PoE-capable switch port automatically supplies power to one of these connected devices if the device senses that there is no power on the circuit:

- a Cisco pre-standard powered device (such as a Cisco IP Phone or a Cisco Aironet Access Point)
- an IEEE 802.3af-compliant powered device

A powered device can receive redundant power when it is connected to a PoE switch port and to an AC power source. The device does not receive redundant power when it is only connected to the PoE port.

Supported Protocols and Standards

The device uses these protocols and standards to support PoE:

- CDP with power consumption—The powered device notifies the device of the amount of power it is consuming. The device does not reply to the power-consumption messages. The device can only supply power to or remove power from the PoE port.

- Cisco intelligent power management—The powered device and the device negotiate through power-negotiation CDP messages for an agreed-upon power-consumption level. The negotiation allows a high-power Cisco powered 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 device.

High-power devices can operate in low-power mode on devices that do not support power-negotiation CDP.

Cisco intelligent power management is backward-compatible with CDP with power consumption; the device responds according to the CDP message that it receives. CDP is not supported on third-party powered devices; therefore, the device uses the IEEE classification to determine the power usage of the device.

- 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 standard.

Powered-Device Detection and Initial Power Allocation

The device detects a Cisco pre-standard or an IEEE-compliant powered device when the PoE-capable port is in the no-shutdown state, PoE is enabled (the default), and the connected device is not being powered by an AC adaptor.

After device detection, the device determines the device power requirements based on its type:

- The initial power allocation is the maximum amount of power that a powered device requires. The device initially allocates this amount of power when it detects and powers the powered device. As the device receives CDP messages from the powered device and as the powered device negotiates power levels with the device through CDP power-negotiation messages, the initial power allocation might be adjusted.
- The device classifies the detected IEEE device within a power consumption class. Based on the available power in the power budget, the device determines if a port can be powered. [Table 10: IEEE Power Classifications](#), on page 74 lists these levels.

Table 10: IEEE Power Classifications

Class	Maximum Power Level Required from the Device
0 (class status unknown)	15.4 W
1	4 W
2	7 W
3	15.4 W
4	30 W (For IEEE 802.3at Type 2 powered devices)

The device monitors and tracks requests for power and grants power only when it is available. The device tracks its power budget (the amount of power available on the device for PoE). The device performs power-accounting calculations when a port is granted or denied power to keep the power budget up to date.

After power is applied to the port, the device uses CDP to determine the *CDP-specific* power consumption requirement of the connected Cisco powered devices, which is the amount of power to allocate based on the CDP messages. The device adjusts the power budget accordingly. This does not apply to third-party PoE devices. The device processes a request and either grants or denies power. If the request is granted, the device updates the power budget. If the request is denied, the device ensures that power to the port is turned off, generates a syslog message, and updates the LEDs. Powered devices can also negotiate with the device for more power.

With PoE+, powered devices use IEEE 802.3at and LLDP power with media dependent interface (MDI) type, length, and value descriptions (TLVs), Power-via-MDI TLVs, for negotiating power up to 30 W. Cisco pre-standard devices and Cisco IEEE powered devices can use CDP or the IEEE 802.3at power-via-MDI power negotiation mechanism to request power levels up to 30 W.



Note The initial allocation for Class 0, Class 3, and Class 4 powered devices is 15.4 W. When a device starts up and uses CDP or LLDP to send a request for more than 15.4 W, it can be allocated up to the maximum of 30 W.



Note The CDP-specific power consumption requirement is referred to as the *actual* power consumption requirement in the software configuration guides and command references.

If the device detects a fault caused by an undervoltage, overvoltage, overtemperature, oscillator-fault, or short-circuit condition, it turns off power to the port, generates a syslog message, and updates the power budget and LEDs.

The PoE feature operates the same whether or not the device is a stack member. The power budget is per device and independent of any other device in the stack. Election of a new active device does not affect PoE operation. The active device keeps track of the PoE status for all devices and ports in the stack and includes the status in output displays.

Power Management Modes

The device supports these PoE modes:

- **auto**—The device automatically detects if the connected device requires power. If the device discovers a powered device connected to the port and if the device 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. For LED information, see the hardware installation guide.

If the device has enough power for all the powered devices, they all come up. If enough power is available for all powered devices connected to the device, power is turned on to all 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.

If granting power would exceed the system power budget, the device denies power, ensures that power to the port is turned off, generates a syslog message, and updates the LEDs. After power has been denied, the device periodically rechecks the power budget and continues to attempt to grant the request for power.

If a device being powered by the device is then connected to wall power, the device might continue to power the device. The device might continue to report that it is still powering the device whether the device is being powered by the device or receiving power from an AC power source.

If a powered device is removed, the device automatically detects the disconnect and removes power from the port. You can connect a nonpowered device without damaging it.

You can specify the maximum wattage that is allowed on the port. If the IEEE class maximum wattage of the powered device is greater than the configured maximum value, the device does not provide power to the port. If the device powers a powered device, but the powered device later requests through CDP messages more than the configured maximum value, the device removes power to the port. The power that was allocated to the powered device is reclaimed into the global power budget. If you do not specify a wattage, the device delivers the maximum value. Use the **auto** setting on any PoE port. The auto mode is the default setting.

- **static**—The device pre-allocates power to the port (even when no powered device is connected) and guarantees that power will be available for the port. The device 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.

However, if the powered-device IEEE class is greater than the maximum wattage, the device does not supply power to it. If the device learns through CDP messages that the powered device is consuming more than the maximum wattage, the device shuts down the powered device.

If you do not specify a wattage, the device pre-allocates the maximum value. The device powers the port only if it discovers a powered device. Use the **static** setting on a high-priority interface.

- **never**—The device 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 that power is never applied to a PoE-capable port, making the port a data-only port.

For most situations, the default configuration (auto mode) works well, providing plug-and-play operation. No further configuration is required. However, perform this task to configure a PoE port for a higher priority, to make it data only, or to specify a maximum wattage to disallow high-power powered devices on a port.

Power Monitoring and Power Policing

When policing of the real-time power consumption is enabled, the device takes action when a powered device consumes more power than the maximum amount allocated, also referred to as the *cutoff-power value*.

When PoE is enabled, the device senses the real-time power consumption of the powered device. The device monitors the real-time power consumption of the connected powered device; this is called *power monitoring* or *power sensing*. The device also polices the power usage with the *power policing* feature.

Power monitoring is backward-compatible with Cisco intelligent power management and CDP-based power consumption. It works with these features to ensure that the PoE port can supply power to the powered device.

The device senses the real-time power consumption of the connected device as follows:

1. The device monitors the real-time power consumption on individual ports.
2. The device records the power consumption, including peak power usage. The device reports the information through the CISCO-POWER-ETHERNET-EXT-MIB.
3. If power policing is enabled, the device polices power usage by comparing the real-time power consumption to the maximum power allocated to the device. The maximum power consumption is also referred to as the *cutoff power* on a PoE port.

If the device uses more than the maximum power allocation on the port, the device can either turn off power to the port, or the device can generate a syslog message and update the LEDs (the port LED is now blinking amber) while still providing power to the device based on the device configuration. By default, power-usage policing is disabled on all PoE ports.

If error recovery from the PoE error-disabled state is enabled, the device automatically takes the PoE port out of the error-disabled state after the specified amount of time.

If error recovery is disabled, you can manually re-enable the PoE port by using the **shutdown** and **no shutdown** interface configuration commands.

4. If policing is disabled, no action occurs when the powered device consumes more than the maximum power allocation on the PoE port, which could adversely affect the device.

Maximum Power Allocation (Cutoff Power) on a PoE Port

When power policing is enabled, the device determines one of these values as the cutoff power on the PoE port in this order:

1. Manually when you set the user-defined power level that the device budgets for the port by using the **power inline consumption default** *wattage* global or interface configuration command
2. Manually when you set the user-defined power level that limits the power allowed on the port by using the **power inline auto max** *max-wattage* or the **power inline static max** *max-wattage* interface configuration command
3. Automatically when the device sets the power usage of the device by using CDP power negotiation or by the IEEE classification and LLDP power negotiation.

Use the first or second method in the previous list to manually configure the cutoff-power value by entering the **power inline consumption default** *wattage* or the **power inline [auto | static max]** *max-wattage* command.

You should use **power inline consumption default** *wattage* command to manually set the power level for a port only in situations where CDP/LLDP power negotiations are not supported.

If you do not manually configure the cutoff-power value, the device automatically determines it by using CDP power negotiation or the device IEEE classification and LLDP power negotiation. If CDP or LLDP are not enabled, the default value of 30 W is applied. However without CDP or LLDP, the device does not allow devices to consume more than 15.4 W of power because values from 15400 to 30000 mW are only allocated based on CDP or LLDP requests. If a powered device consumes more than 15.4 W without CDP or LLDP negotiation, the device might be in violation of the maximum current (*I_{max}*) limitation and might experience an *I_{cut}* fault for drawing more current than the maximum. The port remains in the fault state for a time before attempting to power on again. If the port continuously draws more than 15.4 W, the cycle repeats.



Note

When a powered device connected to a PoE+ port restarts and sends a CDP or LLDP packet with a power TLV, the device locks to the power-negotiation protocol of that first packet and does not respond to power requests from the other protocol. For example, if the device is locked to CDP, it does not provide power to devices that send LLDP requests. If CDP is disabled after the device has locked on it, the device does not respond to LLDP power requests and can no longer power on any accessories. In this case, you should restart the powered device.

Power Consumption Values

You can configure the initial power allocation and the maximum power allocation on a port. However, these values are only the configured values that determine when the device should turn on or turn off power on the PoE port. The maximum power allocation is not the same as the actual power consumption of the powered device. The actual cutoff power value that the device uses for power policing is not equal to the configured power value.

When power policing is enabled, the device polices the power usage *at the switch port*, which is greater than the power consumption of the device. When you manually set the maximum power allocation, you must consider the power loss over the cable from the switch port to the powered device. The cutoff power is the sum of the rated power consumption of the powered device and the worst-case power loss over the cable.

We recommend that you enable power policing when PoE is enabled on your device. For example, if policing is disabled and you set the cutoff-power value by using the **power inline auto max 6300** interface configuration command, the configured maximum power allocation on the PoE port is 6.3 W (6300 mW). The device provides power to the connected devices on the port if the device needs up to 6.3 W. If the CDP-power negotiated value or the IEEE classification value exceeds the configured cutoff value, the device does not provide power to the connected device. After the device turns on power on the PoE port, the device does not police the real-time power consumption of the device, and the device can consume more power than the maximum allocated amount, which could adversely affect the device and the devices connected to the other PoE ports.

Because the device supports internal power supplies and the Cisco Redundant Power System 2300 (also referred to as the RPS 2300), the total amount of power available for the powered devices varies depending on the power supply configuration.

How to Configure PoE

Configuring a Power Management Mode on a PoE Port



Note When you make PoE configuration changes, the port being configured drops power. Depending on the new configuration, the state of the other PoE ports, and the state of the power budget, the port might not be powered up again. For example, port 1 is in the auto and on state, and you configure it for static mode. The device removes power from port 1, detects the powered device, and repowers the port. If port 1 is in the auto and on state and you configure it with a maximum wattage of 10 W, the device removes power from the port and then redetects the powered device. The device repowers the port only if the powered device is a class 1, class 2, or a Cisco-only powered device.

Procedure

	Command or Action	Purpose
Step 1	enable Example: Device> enable	Enables privileged EXEC mode. • Enter your password if prompted.

	Command or Action	Purpose
Step 2	configure terminal Example: Device# configure terminal	Enters global configuration mode.
Step 3	interface interface-id Example: Device(config)# interface gigabitethernet 2/0/1	Specifies the physical port to be configured, and enters interface configuration mode.
Step 4	power inline {auto [max max-wattage] never static [max max-wattage]} Example: Device(config-if)# power inline auto	<p>Configures the PoE mode on the port. The keywords have these meanings:</p> <ul style="list-style-type: none"> • 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. • max max-wattage—Limits the power allowed on the port. The range is 4000 to 30000 mW. If no value is specified, the maximum is allowed. • never—Disables device detection, and disable power to the port. <p>Note If a port has a Cisco powered device connected to it, do not use the power inline never command to configure the port. A false link-up can occur, placing the port into the error-disabled state.</p> <ul style="list-style-type: none"> • static—Enables powered-device detection. Pre-allocate (reserve) power for a port before the device discovers the powered device. The device reserves power for this port even when no device is connected and guarantees that power will be provided upon device detection. <p>The device allocates power to a port configured in static mode before it allocates power to a port configured in auto mode.</p>
Step 5	end Example: Device(config-if)# end	Returns to privileged EXEC mode.

	Command or Action	Purpose
Step 6	show power inline [<i>interface-id</i> module <i>switch-number</i>] Example: Device# show power inline	Displays PoE status for a device or a device stack, for the specified interface, or for a specified stack member.. The module <i>switch-number</i> keywords are supported only on stacking-capable devices.
Step 7	copy running-config startup-config Example: Device# copy running-config startup-config	(Optional) Saves your entries in the configuration file.

Fast POE

This feature remembers the last power drawn from a particular PSE port and switches on power the moment AC power is plugged in (within 15 to 20 seconds of switching on power) without waiting for IOS to boot up. When **poe-ha** is enabled on a particular port, the switch on a recovery after power failure, provides power to the connected endpoint devices within short duration before even the IOS forwarding starts up.

This feature can be configured by the same command as **poe-ha** which is already implemented. If the user replaces the power device connected to a port when the switch is powered off, then this new device will get the power which the previous device was drawing.



Note Fast POE is supported on Catalyst 3850 only.



Note In case of UPOE, even though Fast POE is available on the switch side, the PD endpoints may not be able to take advantage of the same, due to the reliance on LLDP to signal the UPOE power availability. This reliance on LLDP requires that the PD endpoint still needs to wait till the IOS comes up and LLDP packet exchanges can happen, signaling the availability of UPOE power.

Configuring Fast PoE

To configure Fast PoE, perform the following steps:



Note You will need to configure the **poe-ha** command before connecting the PD, or you will need to manually shut/unshut the port after configuring **poe-ha**.

Procedure

	Command or Action	Purpose
Step 1	enable Example: <pre>Device> enable</pre>	Enables privileged EXEC mode. <ul style="list-style-type: none"> • Enter your password if prompted.
Step 2	configure terminal Example: <pre>Device# configure terminal</pre>	Enters global configuration mode.
Step 3	interface <i>interface-id</i> Example: <pre>Device(config)# interface gigabitethernet2/0/1</pre>	Specifies the physical port to be configured, and enters interface configuration mode.
Step 4	power inline port poe-ha Example: <pre>Device(config-if)# power inline port poe-ha</pre>	Configures POE High Availability.
Step 5	end Example: <pre>Device(config-if)# end</pre>	Returns to privileged EXEC mode.

Budgeting Power for Devices Connected to a PoE Port

When Cisco powered devices are connected to PoE ports, the device uses Cisco Discovery Protocol (CDP) to determine the *protocol-specific* power consumption of the devices, and the device adjusts the power budget accordingly. This does not apply to IEEE third-party powered devices. For these devices, when the device grants a power request, the device adjusts the power budget according to the powered-device IEEE classification. If the powered device is a class 0 (class status unknown) or a class 3, the device budgets 15,400 mW for the device, regardless of the CDP-specific amount of power needed. If the powered device reports a higher class than its CDP-specific consumption or does not support power classification (defaults to class 0), the device can power fewer devices because it uses the IEEE class information to track the global power budget.

By using the **power inline consumption *wattage*** interface configuration command or the **power inline consumption default *wattage*** global configuration command, you can override the default power requirement specified by the IEEE classification. The difference between what is mandated by the IEEE classification and what is actually needed by the device is reclaimed into the global power budget for use by additional devices. You can then extend the device power budget and use it more effectively.

**Caution**

You should carefully plan your device power budget, enable the power monitoring feature, and make certain not to oversubscribe the power supply.

**Note**

When you manually configure the power budget, you must also consider the power loss over the cable between the device and the powered device.

Budgeting Power to All PoE ports

Procedure

	Command or Action	Purpose
Step 1	enable Example: Device> enable	Enables privileged EXEC mode. <ul style="list-style-type: none"> • Enter your password if prompted.
Step 2	configure terminal Example: Device# configure terminal	Enters global configuration mode.
Step 3	no cdp run Example: Device (config) # no cdp run	(Optional) Disables CDP.
Step 4	power inline consumption default wattage Example: Device (config) # power inline consumption default 5000	Configures the power consumption of powered devices connected to each PoE port. The range for each device is 4000 to 30000 mW (PoE+). The default is 30000 mW.
Step 5	end Example: Device (config) # end	Returns to privileged EXEC mode.
Step 6	show power inline consumption default Example: Device# show power inline consumption default	Displays the power consumption status.
Step 7	copy running-config startup-config Example: Device# copy running-config	(Optional) Saves your entries in the configuration file.

	Command or Action	Purpose
	<code>startup-config</code>	

Budgeting Power to a Specific PoE Port

Procedure

	Command or Action	Purpose
Step 1	enable Example: Device> enable	Enables privileged EXEC mode. <ul style="list-style-type: none"> • Enter your password if prompted.
Step 2	configure terminal Example: Device# configure terminal	Enters global configuration mode.
Step 3	no cdp run Example: Device(config)# no cdp run	(Optional) Disables CDP.
Step 4	interface interface-id Example: Device(config)# interface gigabitethernet 1/0/1	Specifies the physical port to be configured, and enter interface configuration mode.
Step 5	power inline consumption wattage Example: Device(config-if)# power inline consumption 5000	Configures the power consumption of a powered device connected to a PoE port on the device. The range for each device is 4000 to 30000 mW (PoE+). The default is 30000 mW (PoE+).
Step 6	end Example: Device(config-if)# end	Returns to privileged EXEC mode.
Step 7	show power inline consumption Example: Device# show power inline consumption	Displays the power consumption data.
Step 8	copy running-config startup-config Example:	(Optional) Saves your entries in the configuration file.

	Command or Action	Purpose
	Device# copy running-config startup-config	

Configuring Power Policing

By default, the device monitors the real-time power consumption of connected powered devices. You can configure the device to police the power usage. By default, policing is disabled.

Procedure

	Command or Action	Purpose
Step 1	enable Example: Device> enable	Enables privileged EXEC mode. <ul style="list-style-type: none"> • Enter your password if prompted.
Step 2	configure terminal Example: Device# configure terminal	Enters global configuration mode.
Step 3	interface <i>interface-id</i> Example: Device(config)# interface gigabitethernet 2/0/1	Specifies the physical port to be configured, and enter interface configuration mode.
Step 4	power inline police [action{log errdisable}] Example: Device(config-if)# power inline police	If the real-time power consumption exceeds the maximum power allocation on the port, configures the device to take one of these actions: <ul style="list-style-type: none"> • power inline police—Shuts down the PoE port, turns off power to it, and puts it in the error-disabled state. <p>Note You can enable error detection for the PoE error-disabled cause by using the errdisable detect cause inline-power global configuration command. You can also enable the timer to recover from the PoE error-disabled state by using the errdisable recovery cause inline-power interval <i>interval</i> global configuration command.</p>

	Command or Action	Purpose
		<ul style="list-style-type: none"> • power inline police action errdisable—Turns off power to the port if the real-time power consumption exceeds the maximum power allocation on the port. • power inline police action log—Generates a syslog message while still providing power to the port. <p>If you do not enter the action log keywords, the default action shuts down the port and puts the port in the error-disabled state.</p>
Step 5	exit Example: <pre>Device(config-if) # exit</pre>	Returns to global configuration mode.
Step 6	Use one of the following: <ul style="list-style-type: none"> • errdisable detect cause inline-power • errdisable recovery cause inline-power • errdisable recovery interval <i>interval</i> Example: <pre>Device(config) # errdisable detect cause inline-power</pre> <pre>Device(config) # errdisable recovery cause inline-power</pre> <pre>Device(config) # errdisable recovery interval 100</pre>	(Optional) Enables error recovery from the PoE error-disabled state, and configures the PoE recover mechanism variables. By default, the recovery interval is 300 seconds. For interval <i>interval</i> , specifies the time in seconds to recover from the error-disabled state. The range is 30 to 86400.
Step 7	exit Example: <pre>Device(config) # exit</pre>	Returns to privileged EXEC mode.
Step 8	Use one of the following: <ul style="list-style-type: none"> • show power inline police • show errdisable recovery Example: <pre>Device# show power inline police</pre> <pre>Device# show errdisable recovery</pre>	Displays the power monitoring status, and verify the error recovery settings.

	Command or Action	Purpose
Step 9	copy running-config startup-config Example: <pre>Device# copy running-config startup-config</pre>	(Optional) Saves your entries in the configuration file.

Monitoring Power Status

Table 11: Show Commands for Power Status

Command	Purpose
show env power switch [switch-number]	(Optional) Displays the status of the internal power supplies for each switch in the stack or for the specified switch. The range is 1 to , depending on the switch member numbers in the stack. These keywords are available only on stacking-capable switches.
show power inline [interface-id module switch-number]	Displays PoE status for a switch or switch stack, for an interface, or for a specific switch in the stack.
show power inline police	Displays the power policing data.

Configuration Examples for Configuring PoE

Budgeting Power: Example

When you enter one of the following commands,

- **[no] power inline consumption default** *wattage* global configuration command
- **[no] power inline consumption** *wattage*
interface configuration command

this caution message appears:

```
%CAUTION: Interface Gi1/0/1: Misconfiguring the 'power inline consumption/allocation'
command may cause damage to the
switch and void your warranty. Take precaution not to oversubscribe the power supply. It
is recommended to enable power
policing if the switch supports it. Refer to documentation.
```

Additional References

MIBs

MIB	MIBs Link
All the supported MIBs for this release.	To locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use Cisco MIB Locator found at the following URL: http://www.cisco.com/go/mibs

Technical Assistance

Description	Link
<p>The Cisco Support website provides extensive online resources, including documentation and tools for troubleshooting and resolving technical issues with Cisco products and technologies.</p> <p>To receive security and technical information about your products, you can subscribe to various services, such as the Product Alert Tool (accessed from Field Notices), the Cisco Technical Services Newsletter, and Really Simple Syndication (RSS) Feeds.</p> <p>Access to most tools on the Cisco Support website requires a Cisco.com user ID and password.</p>	http://www.cisco.com/support



CHAPTER 9

Configuring 2-event Classification

- [Information about 2-event Classification, on page 89](#)
- [Configuring 2-event Classification, on page 89](#)
- [Example: Configuring 2-Event Classification, on page 90](#)

Information about 2-event Classification

When a class 4 device gets detected, IOS allocates 30W without any CDP or LLDP negotiation. This means that even before the link comes up the class 4 power device gets 30W.

Also, on the hardware level the PSE does a 2-event classification which allows a class 4 PD to detect PSE capability of providing 30W from hardware, register itself and it can move up to PoE+ level without waiting for any CDP/LLDP packet exchange.

Once 2-event is enabled on a port, you need to manually shut/un-shut the port or connect the PD again to start the IEEE detection again. Power budget allocation for a class-4 device will be 30W if 2-event classification is enabled on the port, else it will be 15.4W.

Configuring 2-event Classification

To configure the switch for a 2-event Classification, perform the steps given below:

Procedure

	Command or Action	Purpose
Step 1	enable Example: Device> enable	Enables privileged EXEC mode. <ul style="list-style-type: none">• Enter your password if prompted.
Step 2	configure terminal Example: Device# configure terminal	Enters global configuration mode.

	Command or Action	Purpose
Step 3	interface <i>interface-id</i> Example: Device(config)# interface gigabitethernet2/0/1	Specifies the physical port to be configured, and enters interface configuration mode.
Step 4	power inline port 2-event Example: Device(config-if)# power inline port 2-event	Configures 2-event classification on the switch.
Step 5	end Example: Device(config-if)# end	Returns to privileged EXEC mode.

Example: Configuring 2-Event Classification

This example shows how you can configure 2-event classification.

```

Device> enable
Device# configure terminal
Device(config)# interface gigabitethernet2/0/1
Device(config-if)# power inline port 2-event
Device(config-if)# end

```



CHAPTER 10

Configuring EEE

- [Restrictions for EEE, on page 91](#)
- [Information About EEE, on page 91](#)
- [How to Configure EEE, on page 91](#)
- [Monitoring EEE, on page 93](#)
- [Configuration Examples for Configuring EEE, on page 93](#)
- [Additional References, on page 94](#)
- [Feature History for Configuring EEE, on page 94](#)

Restrictions for EEE

Energy Efficient Ethernet (EEE) has the following restrictions:

- Changing the EEE configuration resets the interface because the device has to restart Layer 1 autonegotiation.
- You might want to enable the Link Layer Discovery Protocol (LLDP) for devices that require longer wakeup times before they are able to accept data on their receive paths. Doing so enables the device to negotiate for extended system wakeup times from the transmitting link partner.

Information About EEE

EEE Overview

Energy Efficient Ethernet (EEE) is an IEEE 802.3az standard that is designed to reduce power consumption in Ethernet networks during idle periods.

Default EEE Configuration

How to Configure EEE

You can enable or disable EEE on an interface that is connected to an EEE-capable link partner.

Enabling or Disabling EEE

Procedure

	Command or Action	Purpose
Step 1	configure terminal Example: Device# configure terminal	Enters global configuration mode.
Step 2	interface <i>interface-id</i> Example: Device(config)# interface gigabitethernet 1/0/1	Specifies the interface to be configured, and enter interface configuration mode.
Step 3	power efficient-ethernet auto Example: Device(config-if)# power efficient-ethernet auto	Enables EEE on the specified interface. When EEE is enabled, the device advertises and autonegotiates EEE to its link partner.
Step 4	no power efficient-ethernet auto Example: Device(config-if)# no power efficient-ethernet auto	Disables EEE on the specified interface.
Step 5	end Example: Device(config-if)# end	Returns to privileged EXEC mode.
Step 6	copy running-config startup-config Example: Device# copy running-config startup-config	(Optional) Saves your entries in the configuration file.

Monitoring EEE

Table 12: Commands for Displaying EEE Settings

Command	Purpose
show eee capabilities interface <i>interface-id</i>	Displays EEE capabilities for the specified interface.
show eee status interface <i>interface-id</i>	Displays EEE status information for the specified interface.
show eee counters interface <i>interface-id</i>	Displays EEE counters for the specified interface.

Following are examples of the **show eee** commands

```
Switch#show eee capabilities interface gigabitEthernet2/0/1
Gi2/0/1
EEE(efficient-ethernet): yes (100-Tx and 1000T auto)
Link Partner : yes (100-Tx and 1000T auto)

ASIC/Interface : EEE Capable/EEE Enabled

Switch#show eee status interface gigabitEthernet2/0/1
Gi2/0/1 is up
EEE(efficient-ethernet): Operational
Rx LPI Status : Low Power
Tx LPI Status : Low Power
Wake Error Count : 0

ASIC EEE STATUS
Rx LPI Status : Receiving LPI
Tx LPI Status : Transmitting LPI
Link Fault Status : Link Up
Sync Status : Code group synchronization with data stream intact

Switch#show eee counters interface gigabitEthernet2/0/1

LP Active Tx Time (10us) : 66649648
LP Transitioning Tx : 462
LP Active Rx Time (10us) : 64911682
LP Transitioning Rx : 153
```

Configuration Examples for Configuring EEE

This example shows how to enable EEE for an interface:

```
Device# configure terminal
Device(config)# interface gigabitEthernet 1/0/1
Device(config-if)# power efficient-ethernet auto
```

This example shows how to disable EEE for an interface:

```
Device# configure terminal
Device(config)# interface gigabitEthernet 1/0/1
Device(config-if)# no power efficient-ethernet auto
```

Additional References

MIBs

MIB	MIBs Link
All the supported MIBs for this release.	To locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use Cisco MIB Locator found at the following URL: http://www.cisco.com/go/mibs

Technical Assistance

Description	Link
<p>The Cisco Support website provides extensive online resources, including documentation and tools for troubleshooting and resolving technical issues with Cisco products and technologies.</p> <p>To receive security and technical information about your products, you can subscribe to various services, such as the Product Alert Tool (accessed from Field Notices), the Cisco Technical Services Newsletter, and Really Simple Syndication (RSS) Feeds.</p> <p>Access to most tools on the Cisco Support website requires a Cisco.com user ID and password.</p>	http://www.cisco.com/support

Feature History for Configuring EEE

This table provides release and related information for features explained in this module.

These features are available on all releases subsequent to the one they were introduced in, unless noted otherwise.

Release	Feature	Feature Information
	Energy Efficient Ethernet	Energy Efficient Ethernet (EEE) is an IEEE 802.3az standard that is designed to reduce power consumption in Ethernet networks during idle periods.

Use Cisco Feature Navigator to find information about platform and software image support. To access Cisco Feature Navigator, go to <http://www.cisco.com/go/cfn>.



PART II

IP Multicast Routing

- [Configuring IGMP Snooping and Multicast VLAN Registration, on page 97](#)
- [Configuring Protocol Independent Multicast \(PIM\), on page 141](#)
- [IPv6 Protocol Independent Multicast, on page 193](#)



CHAPTER 11

Configuring IGMP Snooping and Multicast VLAN Registration

- [Prerequisites for Configuring IGMP Snooping and MVR, on page 97](#)
- [Restrictions for Configuring IGMP Snooping and MVR, on page 98](#)
- [Information About IGMP Snooping and MVR, on page 99](#)
- [How to Configure IGMP Snooping and MVR, on page 108](#)
- [Monitoring IGMP Snooping and MVR, on page 133](#)
- [Configuration Examples for IGMP Snooping and MVR, on page 136](#)
- [Additional References, on page 138](#)
- [Feature History and Information for IGMP Snooping, on page 139](#)

Prerequisites for Configuring IGMP Snooping and MVR

Prerequisites for IGMP Snooping

Observe these guidelines when configuring the IGMP snooping querier:

- Configure the VLAN in global configuration mode.
- Configure an IP address on the VLAN interface. When enabled, the IGMP snooping querier uses the IP address as the query source address.
- If there is no IP address configured on the VLAN interface, the IGMP snooping querier tries to use the configured global IP address for the IGMP querier. If there is no global IP address specified, the IGMP querier tries to use the VLAN device virtual interface (SVI) IP address (if one exists). If there is no SVI IP address, the device uses the first available IP address configured on the device. The first IP address available appears in the output of the **show ip interface** privileged EXEC command. The IGMP snooping querier does not generate an IGMP general query if it cannot find an available IP address on the device.
- The IGMP snooping querier supports IGMP Versions 1 and 2.
- When administratively enabled, the IGMP snooping querier moves to the nonquerier state if it detects the presence of a multicast router in the network.
- When it is administratively enabled, the IGMP snooping querier moves to the operationally disabled state under these conditions:

- IGMP snooping is disabled in the VLAN.
- PIM is enabled on the SVI of the corresponding VLAN.

-
-

Prerequisites for MVR

The following are the prerequisites for Multicast VLAN Registration (MVR):

- To use MVR, the device must be running the LAN Base image.

Restrictions for Configuring IGMP Snooping and MVR

Restrictions for IGMP Snooping

The following are the restrictions for IGMP snooping:

- The switch supports homogeneous stacking and mixed stacking. Mixed stacking is supported only with the Catalyst 2960-S switches. A homogenous stack can have up to eight stack members, while a mixed stack can have up to four stack members. All switches in a switch stack must be running the LAN Base image.
- IGMPv3 join and leave messages are not supported on devices running IGMP filtering or Multicast VLAN registration (MVR).
- IGMP report suppression is supported only when the multicast query has IGMPv1 and IGMPv2 reports. This feature is not supported when the query includes IGMPv3 reports.
- The IGMP configurable leave time is only supported on hosts running IGMP Version 2. IGMP version 2 is the default version for the device.

The actual leave latency in the network is usually the configured leave time. However, the leave time might vary around the configured time, depending on real-time CPU load conditions, network delays and the amount of traffic sent through the interface.

- The IGMP throttling action restriction can be applied only to Layer 2 ports. You can use **ip igmp max-groups action replace** interface configuration command on a logical EtherChannel interface but cannot use it on ports that belong to an EtherChannel port group.

When the maximum group limitation is set to the default (no maximum), entering the **ip igmp max-groups action {deny | replace}** command has no effect.

If you configure the throttling action and set the maximum group limitation after an interface has added multicast entries to the forwarding table, the forwarding-table entries are either aged out or removed, depending on the throttling action.

Restrictions for MVR

The following are restrictions for MVR:

- Only Layer 2 ports participate in MVR. You must configure ports as MVR receiver ports.
- Only one MVR multicast VLAN per device or device stack is supported.
- Receiver ports can only be access ports; they cannot be trunk ports. Receiver ports on a device can be in different VLANs, but should not belong to the multicast VLAN.
- The maximum number of multicast entries (MVR group addresses) that can be configured on a device (that is, the maximum number of television channels that can be received) is 256.
- MVR multicast data received in the source VLAN and leaving from receiver ports has its time-to-live (TTL) decremented by 1 in the device.
- Because MVR on the device uses IP multicast addresses instead of MAC multicast addresses, alias IP multicast addresses are allowed on the device. However, if the device is interoperating with Catalyst 3550 or Catalyst 3500 XL devices, you should not configure IP addresses that alias between themselves or with the reserved IP multicast addresses (in the range 224.0.0.xxx).
- Do not configure MVR on private VLAN ports.
- MVR is not supported when multicast routing is enabled on a device. If you enable multicast routing and a multicast routing protocol while MVR is enabled, MVR is disabled, and you receive a warning message. If you try to enable MVR while multicast routing and a multicast routing protocol are enabled, the operation to enable MVR is cancelled, and you receive an error message.
- MVR data received on an MVR receiver port is not forwarded to MVR source ports.
- MVR does not support IGMPv3 messages.
- The switch supports homogeneous stacking and mixed stacking. Mixed stacking is supported only with the Catalyst 2960-S switches. A homogenous stack can have up to eight stack members, while a mixed stack can have up to four stack members. All switches in a switch stack must be running the LAN Base image.

Information About IGMP Snooping and MVR

IGMP Snooping

Layer 2 devices can use IGMP snooping to constrain the flooding of multicast traffic by dynamically configuring Layer 2 interfaces so that multicast traffic is forwarded to only those interfaces associated with IP multicast devices. As the name implies, IGMP snooping requires the LAN device to snoop on the IGMP transmissions between the host and the router and to keep track of multicast groups and member ports. When the device receives an IGMP report from a host for a particular multicast group, the device adds the host port number to the forwarding table entry; when it receives an IGMP Leave Group message from a host, it removes the host port from the table entry. It also periodically deletes entries if it does not receive IGMP membership reports from the multicast clients.



Note For more information on IP multicast and IGMP, see RFC 1112 and RFC 2236.

The multicast router sends out periodic general queries to all VLANs. All hosts interested in this multicast traffic send join requests and are added to the forwarding table entry. The device creates one entry per VLAN in the IGMP snooping IP multicast forwarding table for each group from which it receives an IGMP join request.

The device supports IP multicast group-based bridging, instead of MAC-addressed based groups. With multicast MAC address-based groups, if an IP address being configured translates (aliases) to a previously configured MAC address or to any reserved multicast MAC addresses (in the range 224.0.0.xxx), the command fails. Because the device uses IP multicast groups, there are no address aliasing issues.

The IP multicast groups learned through IGMP snooping are dynamic. However, you can statically configure multicast groups by using the **ip igmp snooping vlan *vlan-id* static *ip_address* interface *interface-id*** global configuration command. If you specify group membership for a multicast group address statically, your setting supersedes any automatic manipulation by IGMP snooping. Multicast group membership lists can consist of both user-defined and IGMP snooping-learned settings.

You can configure an IGMP snooping querier to support IGMP snooping in subnets without multicast interfaces because the multicast traffic does not need to be routed.

If a port spanning-tree, a port group, or a VLAN ID change occurs, the IGMP snooping-learned multicast groups from this port on the VLAN are deleted.

These sections describe IGMP snooping characteristics:

IGMP Versions

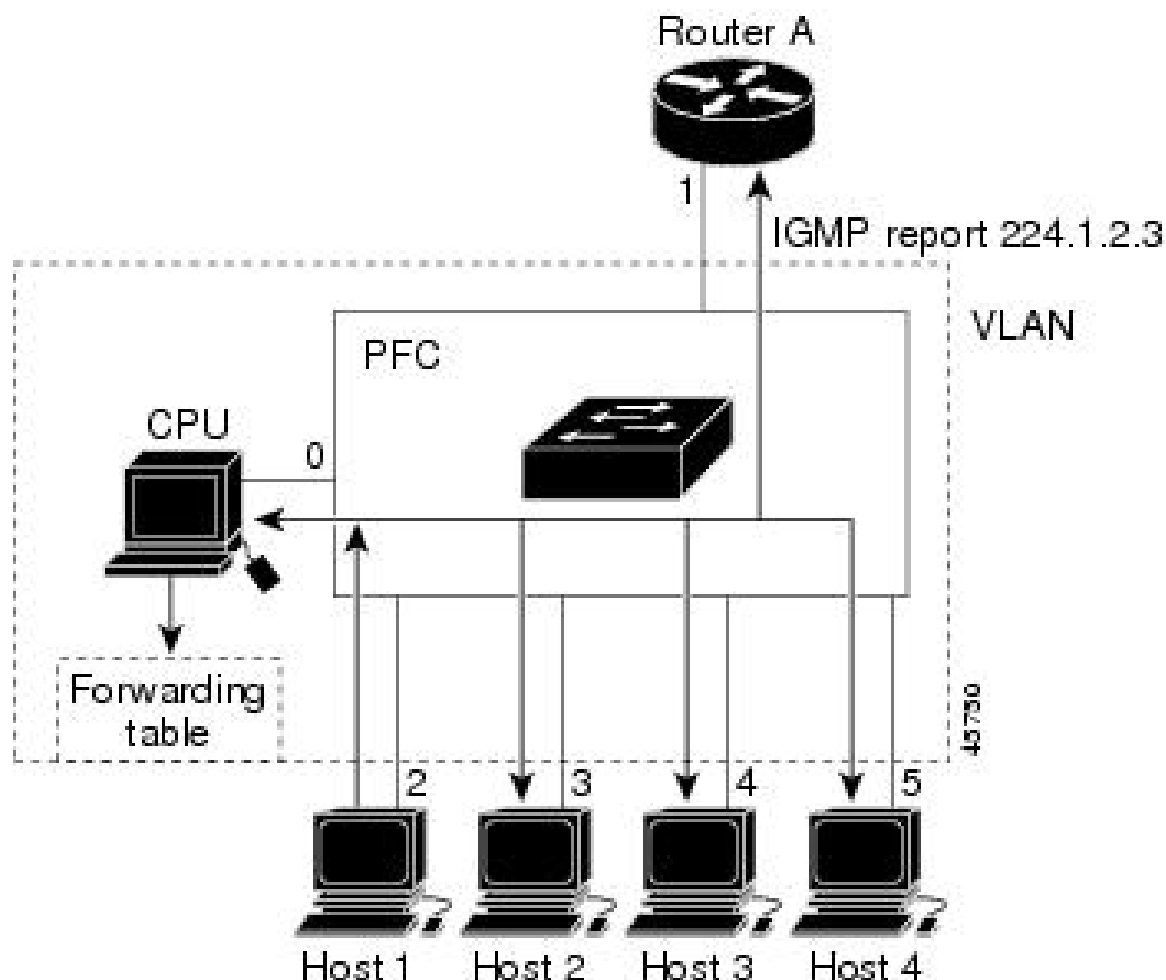
The device supports IGMP version 1, IGMP version 2, and IGMP version 3. These versions are interoperable on the device. For example, if IGMP snooping is enabled and the querier's version is IGMPv2, and the device receives an IGMPv3 report from a host, then the device can forward the IGMPv3 report to the multicast router.

An IGMPv3 device can receive messages from and forward messages to a device running the Source Specific Multicast (SSM) feature.

Joining a Multicast Group

Figure 4: Initial IGMP Join Message

When a host connected to the device wants to join an IP multicast group and it is an IGMP version 2 client, it sends an unsolicited IGMP join message, specifying the IP multicast group to join. Alternatively, when the device receives a general query from the router, it forwards the query to all ports in the VLAN. IGMP version 1 or version 2 hosts wanting to join the multicast group respond by sending a join message to the device. The device CPU creates a multicast forwarding-table entry for the group if it is not already present. The CPU also adds the interface where the join message was received to the forwarding-table entry. The host associated with that interface receives multicast traffic for that multicast group.



Router A sends a general query to the device, which forwards the query to ports 2 through 5, all of which are members of the same VLAN. Host 1 wants to join multicast group 224.1.2.3 and multicasts an IGMP membership report (IGMP join message) to the group. The device CPU uses the information in the IGMP report to set up a forwarding-table entry that includes the port numbers connected to Host 1 and to the router.

Table 13: IGMP Snooping Forwarding Table

Destination Address	Type of Packet	Ports
224.1.2.3	IGMP	1, 2

The device hardware can distinguish IGMP information packets from other packets for the multicast group. The information in the table tells the switching engine to send frames addressed to the 224.1.2.3 multicast IP address that are not IGMP packets to the router and to the host that has joined the group.

Figure 5: Second Host Joining a Multicast Group

If another host (for example, Host 4) sends an unsolicited IGMP join message for the same group, the CPU receives that message and adds the port number of Host 4 to the forwarding table. Because the forwarding table directs IGMP messages only to the CPU, the message is not flooded to other ports on the device. Any

known multicast traffic is forwarded to the group and not to the CPU.

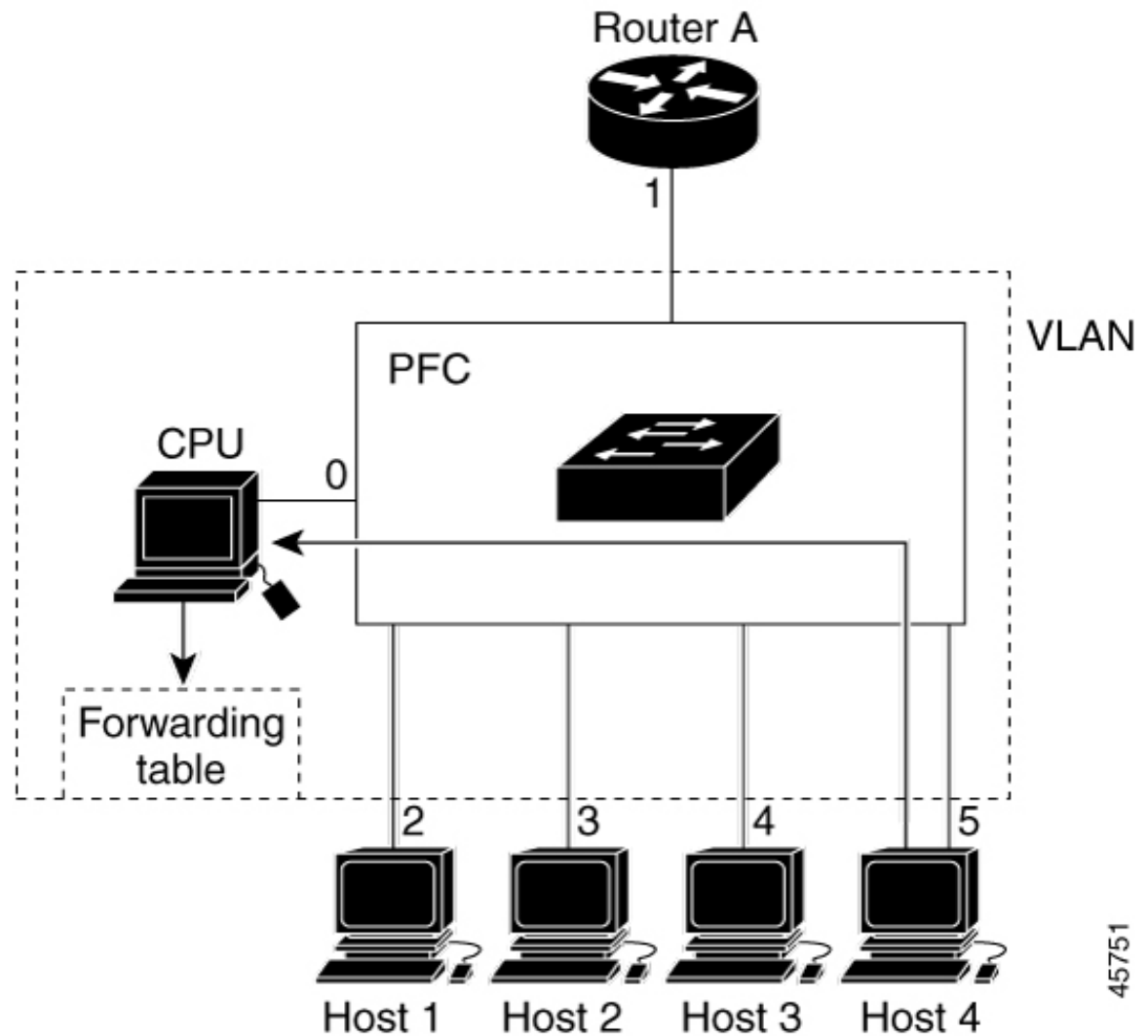


Table 14: Updated IGMP Snooping Forwarding Table

Destination Address	Type of Packet	Ports
224.1.2.3	IGMP	1, 2, 5

Leaving a Multicast Group

The router sends periodic multicast general queries, and the device forwards these queries through all ports in the VLAN. Interested hosts respond to the queries. If at least one host in the VLAN wants to receive multicast traffic, the router continues forwarding the multicast traffic to the VLAN. The device forwards multicast group traffic only to those hosts listed in the forwarding table for that IP multicast group maintained by IGMP snooping.

When hosts want to leave a multicast group, they can silently leave, or they can send a leave message. When the device receives a leave message from a host, it sends a group-specific query to learn if any other devices

connected to that interface are interested in traffic for the specific multicast group. The device then updates the forwarding table for that MAC group so that only those hosts interested in receiving multicast traffic for the group are listed in the forwarding table. If the router receives no reports from a VLAN, it removes the group for the VLAN from its IGMP cache.

Immediate Leave

The device uses IGMP snooping Immediate Leave to remove from the forwarding table an interface that sends a leave message without the device sending group-specific queries to the interface. The VLAN interface is pruned from the multicast tree for the multicast group specified in the original leave message. Immediate Leave ensures optimal bandwidth management for all hosts on a switched network, even when multiple multicast groups are simultaneously in use.

Immediate Leave is only supported on IGMP version 2 hosts. IGMP version 2 is the default version for the device.



Note You should use the Immediate Leave feature only on VLANs where a single host is connected to each port. If Immediate Leave is enabled on VLANs where more than one host is connected to a port, some hosts may be dropped inadvertently.

IGMP Configurable-Leave Timer

You can configure the time that the device waits after sending a group-specific query to determine if hosts are still interested in a specific multicast group. The IGMP leave response time can be configured from 100 to 32767 milliseconds.

IGMP Report Suppression



Note IGMP report suppression is supported only when the multicast query has IGMPv1 and IGMPv2 reports. This feature is not supported when the query includes IGMPv3 reports.

The device uses IGMP report suppression to forward only one IGMP report per multicast router query to multicast devices. When IGMP report suppression is enabled (the default), the device sends the first IGMP report from all hosts for a group to all the multicast routers. The device does not send the remaining IGMP reports for the group to the multicast routers. This feature prevents duplicate reports from being sent to the multicast devices.

If the multicast router query includes requests only for IGMPv1 and IGMPv2 reports, the device forwards only the first IGMPv1 or IGMPv2 report from all hosts for a group to all the multicast routers.

If the multicast router query also includes requests for IGMPv3 reports, the device forwards all IGMPv1, IGMPv2, and IGMPv3 reports for a group to the multicast devices.

If you disable IGMP report suppression, all IGMP reports are forwarded to the multicast routers.

IGMP Snooping and Device Stacks

IGMP snooping functions across the device stack; that is, IGMP control information from one device is distributed to all devices in the stack. Regardless of the stack member through which IGMP multicast data enters the stack, the data reaches the hosts that have registered for that group.

If a device in the stack fails or is removed from the stack, only the members of the multicast group that are on that device will not receive the multicast data. All other members of a multicast group on other devices in the stack continue to receive multicast data streams. However, multicast groups that are common for both Layer 2 and Layer 3 (IP multicast routing) might take longer to converge if the active device is removed.

Default IGMP Snooping Configuration

This table displays the default IGMP snooping configuration for the device.

Table 15: Default IGMP Snooping Configuration

Feature	Default Setting
IGMP snooping	Enabled globally and per VLAN
Multicast routers	None configured
IGMP snooping Immediate Leave	Disabled
Static groups	None configured
TCN ¹ flood query count	2
TCN query solicitation	Disabled
IGMP snooping querier	Disabled
IGMP report suppression	Enabled

¹ (1) TCN = Topology Change Notification

Multicast VLAN Registration

Multicast VLAN Registration (MVR) is designed for applications using wide-scale deployment of multicast traffic across an Ethernet ring-based service-provider network (for example, the broadcast of multiple television channels over a service-provider network). MVR allows a subscriber on a port to subscribe and unsubscribe to a multicast stream on the network-wide multicast VLAN. It allows the single multicast VLAN to be shared in the network while subscribers remain in separate VLANs. MVR provides the ability to continuously send multicast streams in the multicast VLAN, but to isolate the streams from the subscriber VLANs for bandwidth and security reasons.

These sections describe MVR:

MVR and IGMP



Note MVR can coexist with IGMP snooping on a device.

MVR assumes that subscriber ports subscribe and unsubscribe (join and leave) these multicast streams by sending out IGMP join and leave messages. These messages can originate from an IGMP version-2-compatible host with an Ethernet connection. Although MVR operates on the underlying method of IGMP snooping, the two features operate independently of each other. One can be enabled or disabled without affecting the behavior of the other feature. However, if IGMP snooping and MVR are both enabled, MVR reacts only to join and leave messages from multicast groups configured under MVR. Join and leave messages from all other multicast groups are managed by IGMP snooping.

The device CPU identifies the MVR IP multicast streams and their associated IP multicast group in the device forwarding table, intercepts the IGMP messages, and modifies the forwarding table to include or remove the subscriber as a receiver of the multicast stream, even though the receivers might be in a different VLAN from the source. This forwarding behavior selectively allows traffic to cross between different VLANs.

Modes of Operation

You can set the device for compatible or dynamic mode of MVR operation:

- In compatible mode, multicast data received by MVR hosts is forwarded to all MVR data ports, regardless of MVR host membership on those ports. The multicast data is forwarded only to those receiver ports that MVR hosts have joined, either by IGMP reports or by MVR static configuration. IGMP reports received from MVR hosts are never forwarded from MVR data ports that were configured in the device.
- In dynamic mode, multicast data received by MVR hosts on the device is forwarded from only those MVR data and client ports that the MVR hosts have joined, either by IGMP reports or by MVR static configuration. Any IGMP reports received from MVR hosts are also forwarded from all the MVR data ports in the host. This eliminates using unnecessary bandwidth on MVR data port links, which occurs when the device runs in compatible mode.

MVR and Switch Stacks

Only one MVR multicast VLAN per device or device stack is supported.

Receiver ports and source ports can be on different devices in a device stack. Multicast data sent on the multicast VLAN is forwarded to all MVR receiver ports across the stack. When a new device is added to a stack, by default it has no receiver ports.

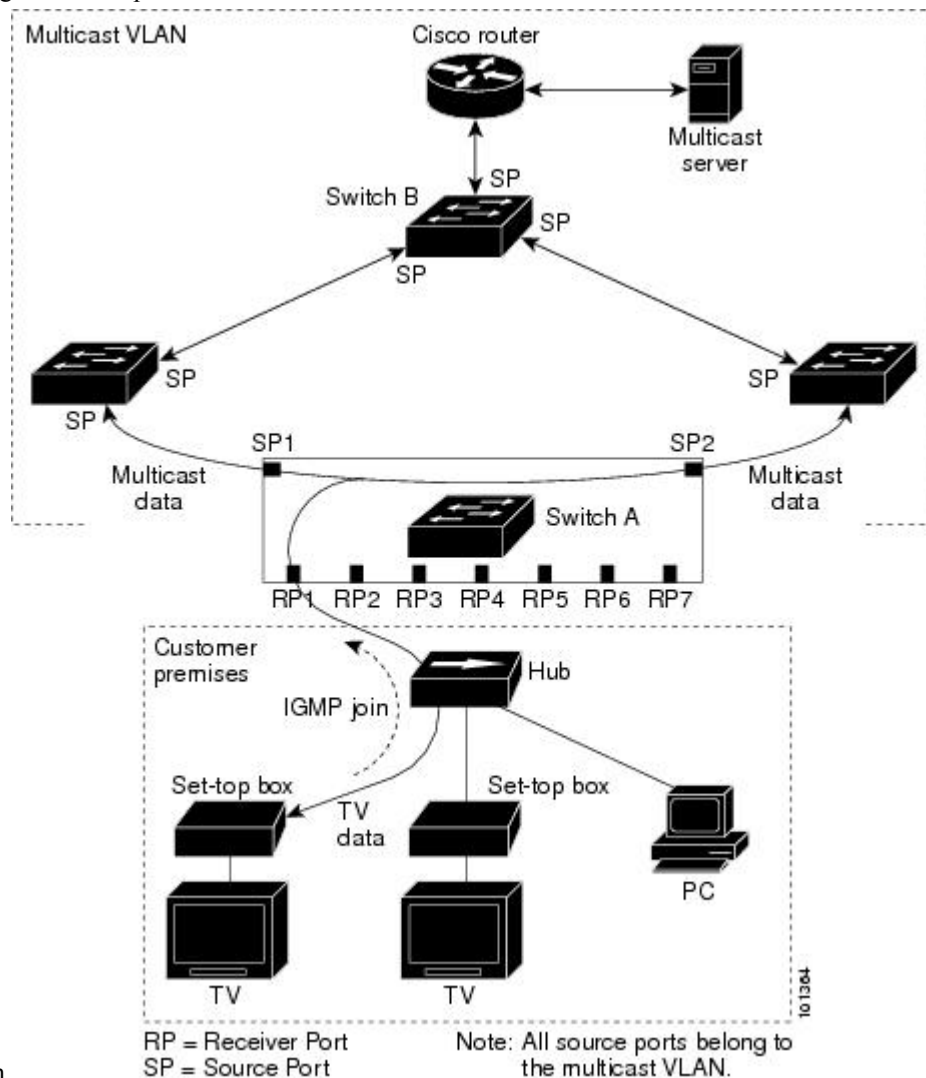
If a device fails or is removed from the stack, only those receiver ports belonging to that device will not receive the multicast data. All other receiver ports on other devices continue to receive the multicast data.

MVR in a Multicast Television Application

In a multicast television application, a PC or a television with a set-top box can receive the multicast stream. Multiple set-top boxes or PCs can be connected to one subscriber port, which is a device port configured as an MVR receiver port.

Figure 6: Multicast VLAN Registration Example

The following is an example



configuration.

In this example configuration, DHCP assigns an IP address to the set-top box or the PC. When a subscriber selects a channel, the set-top box or PC sends an IGMP report to Switch A to join the appropriate multicast. If the IGMP report matches one of the configured IP multicast group addresses, the device CPU modifies the hardware address table to include this receiver port and VLAN as a forwarding destination of the specified multicast stream when it is received from the multicast VLAN. Uplink ports that send and receive multicast data to and from the multicast VLAN are called MVR source ports.

When a subscriber changes channels or turns off the television, the set-top box sends an IGMP leave message for the multicast stream. The device CPU sends a MAC-based general query through the receiver port VLAN. If there is another set-top box in the VLAN still subscribing to this group, that set-top box must respond within the maximum response time specified in the query. If the CPU does not receive a response, it eliminates the receiver port as a forwarding destination for this group.

Without Immediate Leave, when the device receives an IGMP leave message from a subscriber on a receiver port, it sends out an IGMP query on that port and waits for IGMP group membership reports. If no reports

are received in a configured time period, the receiver port is removed from multicast group membership. With Immediate Leave, an IGMP query is not sent from the receiver port on which the IGMP leave was received. As soon as the leave message is received, the receiver port is removed from multicast group membership, which speeds up leave latency. Enable the Immediate-Leave feature only on receiver ports to which a single receiver device is connected.

MVR eliminates the need to duplicate television-channel multicast traffic for subscribers in each VLAN. Multicast traffic for all channels is only sent around the VLAN trunk once—only on the multicast VLAN. The IGMP leave and join messages are in the VLAN to which the subscriber port is assigned. These messages dynamically register for streams of multicast traffic in the multicast VLAN on the Layer 3 device. The access layer device, Switch A, modifies the forwarding behavior to allow the traffic to be forwarded from the multicast VLAN to the subscriber port in a different VLAN, selectively allowing traffic to cross between two VLANs.

IGMP reports are sent to the same IP multicast group address as the multicast data. The Switch A CPU must capture all IGMP join and leave messages from receiver ports and forward them to the multicast VLAN of the source (uplink) port, based on the MVR mode.

Default MVR Configuration

Table 16: Default MVR Configuration

Feature	Default Setting
MVR	Disabled globally and per interface
Multicast addresses	None configured
Query response time	0.5 second
Multicast VLAN	VLAN 1
Mode	Compatible
Interface (per port) default	Neither a receiver nor a source port
Immediate Leave	Disabled on all ports

IGMP Filtering and Throttling

In some environments, for example, metropolitan or multiple-dwelling unit (MDU) installations, you might want to control the set of multicast groups to which a user on a device port can belong. You can control the distribution of multicast services, such as IP/TV, based on some type of subscription or service plan. You might also want to limit the number of multicast groups to which a user on a device port can belong.

With the IGMP filtering feature, you can filter multicast joins on a per-port basis by configuring IP multicast profiles and associating them with individual device ports. An IGMP profile can contain one or more multicast groups and specifies whether access to the group is permitted or denied. If an IGMP profile denying access to a multicast group is applied to a device port, the IGMP join report requesting the stream of IP multicast traffic is dropped, and the port is not allowed to receive IP multicast traffic from that group. If the filtering action permits access to the multicast group, the IGMP report from the port is forwarded for normal processing. You can also set the maximum number of IGMP groups that a Layer 2 interface can join.

IGMP filtering controls only group-specific query and membership reports, including join and leave reports. It does not control general IGMP queries. IGMP filtering has no relationship with the function that directs

the forwarding of IP multicast traffic. The filtering feature operates in the same manner whether CGMP or MVR is used to forward the multicast traffic.

IGMP filtering applies only to the dynamic learning of IP multicast group addresses, not static configuration.

With the IGMP throttling feature, you can set the maximum number of IGMP groups that a Layer 2 interface can join. If the maximum number of IGMP groups is set, the IGMP snooping forwarding table contains the maximum number of entries, and the interface receives an IGMP join report, you can configure an interface to drop the IGMP report or to replace the randomly selected multicast entry with the received IGMP report.



Note IGMPv3 join and leave messages are not supported on devices running IGMP filtering.

Default IGMP Filtering and Throttling Configuration

This table displays the default IGMP filtering and throttling configuration for the device.

Table 17: Default IGMP Filtering Configuration

Feature	Default Setting
IGMP filters	None applied.
IGMP maximum number of IGMP groups	No maximum set. Note When the maximum number of groups is in the forward the default IGMP throttling action is to deny the IGMP
IGMP profiles	None defined.
IGMP profile action	Deny the range addresses.

How to Configure IGMP Snooping and MVR

Enabling or Disabling IGMP Snooping on a Device

When IGMP snooping is globally enabled or disabled, it is also enabled or disabled in all existing VLAN interfaces. IGMP snooping is enabled on all VLANs by default, but can be enabled and disabled on a per-VLAN basis.

Global IGMP snooping overrides the VLAN IGMP snooping. If global snooping is disabled, you cannot enable VLAN snooping. If global snooping is enabled, you can enable or disable VLAN snooping.

Follow these steps to globally enable IGMP snooping on the device:

Procedure

	Command or Action	Purpose
Step 1	enable	Enables privileged EXEC mode.

	Command or Action	Purpose
	Example: Device> enable	<ul style="list-style-type: none"> Enter your password if prompted.
Step 2	configure terminal Example: Device# configure terminal	Enters global configuration mode.
Step 3	ip igmp snooping Example: Device(config)# ip igmp snooping	Globally enables IGMP snooping in all existing VLAN interfaces. Note To globally disable IGMP snooping on all VLAN interfaces, use the no ip igmp snooping global configuration command.
Step 4	end Example: Device(config)# end	Returns to privileged EXEC mode.
Step 5	copy running-config startup-config Example: Device# copy running-config startup-config	(Optional) Saves your entries in the configuration file.

Enabling or Disabling IGMP Snooping on a VLAN Interface

Follow these steps to enable IGMP snooping on a VLAN interface:

Procedure

	Command or Action	Purpose
Step 1	enable Example: Device> enable	Enables privileged EXEC mode. <ul style="list-style-type: none"> Enter your password if prompted.
Step 2	configure terminal Example:	Enters global configuration mode.

	Command or Action	Purpose
	Device# configure terminal	
Step 3	ip igmp snooping vlan <i>vlan-id</i> Example: Device(config)# ip igmp snooping vlan 7	Enables IGMP snooping on the VLAN interface. The VLAN ID range is 1 to 1001 and 1006 to 4094. IGMP snooping must be globally enabled before you can enable VLAN snooping. Note To disable IGMP snooping on a VLAN interface, use the no ip igmp snooping vlan <i>vlan-id</i> global configuration command for the specified VLAN number.
Step 4	end Example: Device(config)# end	Returns to privileged EXEC mode.
Step 5	copy running-config startup-config Example: Device# copy running-config startup-config	(Optional) Saves your entries in the configuration file.

Setting the Snooping Method

Multicast-capable router ports are added to the forwarding table for every Layer 2 multicast entry. The switch learns of the ports through one of these methods:

- Snooping on IGMP queries, Protocol-Independent Multicast (PIM) packets, and Distance Vector Multicast Routing Protocol (DVMRP) packets.
- Listening to Cisco Group Management Protocol (CGMP) packets from other routers.
- Statically connecting to a multicast router port using the **ip igmp snooping mrouter** global configuration command.

You can configure the switch either to snoop on IGMP queries and PIM/DVMRP packets or to listen to CGMP self-join or proxy-join packets. By default, the switch snoops on PIM/DVMRP packets on all VLANs. To learn of multicast router ports through only CGMP packets, use the **ip igmp snooping vlan *vlan-id* mrouter learn cgmp** global configuration command. When this command is entered, the router listens to only CGMP self-join and CGMP proxy-join packets and to no other CGMP packets. To learn of multicast router ports through only PIM-DVMRP packets, use the **ip igmp snooping vlan *vlan-id* mrouter learn pim-dvmrp** global configuration command.

If you want to use CGMP as the learning method and no multicast routers in the VLAN are CGMP proxy-enabled, you must enter the **ip cgmp router-only** command to dynamically access the router.

Procedure

	Command or Action	Purpose
Step 1	enable Example: <pre>Device> enable</pre>	Enables privileged EXEC mode. <ul style="list-style-type: none"> • Enter your password if prompted.
Step 2	configure terminal Example: <pre>Device# configure terminal</pre>	Enters global configuration mode.
Step 3	ip igmp snooping vlan <i>vlan-id</i> mrouter learn {cgmp pim-dvmrp } Example: <pre>Device(config)# ip igmp snooping vlan 1 mrouter learn cgmp</pre>	Specifies the multicast router learning method: <ul style="list-style-type: none"> • cgmp—Listens for CGMP packets. This method is useful for reducing control traffic. • pim-dvmrp—Snoops on IGMP queries and PIM-DVMRP packets. This is the default. <p>Note To return to the default learning method, use the no ip igmp snooping vlan <i>vlan-id</i> mrouter learn cgmp global configuration command.</p>
Step 4	end Example: <pre>Device(config)# end</pre>	Returns to privileged EXEC mode.
Step 5	show ip igmp snooping Example: <pre>Device# show ip igmp snooping</pre>	Verifies the configuration.
Step 6	copy running-config startup-config Example: <pre>Device# copy running-config startup-config</pre>	(Optional) Saves your entries in the configuration file.

Configuring a Multicast Router Port

Perform these steps to add a multicast router port (enable a static connection to a multicast router) on the device.



Note Static connections to multicast routers are supported only on device ports.

Procedure

	Command or Action	Purpose
Step 1	enable Example: <pre>Device> enable</pre>	Enables privileged EXEC mode. <ul style="list-style-type: none"> • Enter your password if prompted.
Step 2	configure terminal Example: <pre>Device# configure terminal</pre>	Enters global configuration mode.
Step 3	ip igmp snooping vlan <i>vlan-id</i> mrouter interface <i>interface-id</i> Example: <pre>Device(config)# ip igmp snooping vlan 5 mrouter interface gigabitethernet1/0/1</pre>	Specifies the multicast router VLAN ID and the interface to the multicast router. <ul style="list-style-type: none"> • The VLAN ID range is 1 to 1001 and 1006 to 4094. • The interface can be a physical interface or a port channel. The port-channel range is 1 to 128. <p>Note To remove a multicast router port from the VLAN, use the no ip igmp snooping vlan <i>vlan-id</i> mrouter interface <i>interface-id</i> global configuration command.</p>
Step 4	end Example: <pre>Device(config)# end</pre>	Returns to privileged EXEC mode.
Step 5	show ip igmp snooping mrouter [vlan <i>vlan-id</i>] Example: <pre>Device# show ip igmp snooping mrouter</pre>	Verifies that IGMP snooping is enabled on the VLAN interface.

	Command or Action	Purpose
	<code>vlan 5</code>	
Step 6	copy running-config startup-config Example: <pre>Device# copy running-config startup-config</pre>	(Optional) Saves your entries in the configuration file.

Configuring a Host Statically to Join a Group

Hosts or Layer 2 ports normally join multicast groups dynamically, but you can also statically configure a host on an interface.

Follow these steps to add a Layer 2 port as a member of a multicast group:

Procedure

	Command or Action	Purpose
Step 1	enable Example: <pre>Device> enable</pre>	Enables privileged EXEC mode. <ul style="list-style-type: none"> • Enter your password if prompted.
Step 2	configure terminal Example: <pre>Device# configure terminal</pre>	Enters global configuration mode.
Step 3	ip igmp snooping vlan <i>vlan-id</i> static <i>ip_address</i> interface <i>interface-id</i> Example: <pre>Device(config)# ip igmp snooping vlan 105 static 230.0.0.1 interface gigabitethernet1/0/1</pre>	Statically configures a Layer 2 port as a member of a multicast group: <ul style="list-style-type: none"> • <i>vlan-id</i> is the multicast group VLAN ID. The range is 1 to 1001 and 1006 to 4094. • <i>ip-address</i> is the group IP address. • <i>interface-id</i> is the member port. It can be a physical interface or a port channel (1 to 128). <p>Note To remove the Layer 2 port from the multicast group, use the no ip igmp snooping vlan <i>vlan-id</i> static <i>mac-address</i> interface <i>interface-id</i> global configuration command.</p>

	Command or Action	Purpose
Step 4	end Example: <pre>Device(config)# end</pre>	Returns to privileged EXEC mode.
Step 5	show ip igmp snooping groups Example: <pre>Device# show ip igmp snooping groups</pre>	Verifies the member port and the IP address.
Step 6	copy running-config startup-config Example: <pre>Device# copy running-config startup-config</pre>	(Optional) Saves your entries in the configuration file.

Enabling IGMP Immediate Leave

When you enable IGMP Immediate Leave, the device immediately removes a port when it detects an IGMP Version 2 leave message on that port. You should use the Immediate-Leave feature only when there is a single receiver present on every port in the VLAN.



Note Immediate Leave is supported only on IGMP Version 2 hosts. IGMP Version 2 is the default version for the device.

Procedure

	Command or Action	Purpose
Step 1	enable Example: <pre>Device> enable</pre>	Enables privileged EXEC mode. <ul style="list-style-type: none"> • Enter your password if prompted.
Step 2	configure terminal Example: <pre>Device# configure terminal</pre>	Enters global configuration mode.
Step 3	ip igmp snooping vlan <i>vlan-id</i> immediate-leave	Enables IGMP Immediate Leave on the VLAN interface.

	Command or Action	Purpose
	Example: <pre>Device(config)# ip igmp snooping vlan 21 immediate-leave</pre>	Note To disable IGMP Immediate Leave on a VLAN, use the no ip igmp snooping vlan <i>vlan-id</i> immediate-leave global configuration command.
Step 4	end Example: <pre>Device(config)# end</pre>	Returns to privileged EXEC mode.
Step 5	show ip igmp snooping vlan <i>vlan-id</i> Example: <pre>Device# show ip igmp snooping vlan 21</pre>	Verifies that Immediate Leave is enabled on the VLAN interface.
Step 6	end Example: <pre>Device(config)# end</pre>	Returns to privileged EXEC mode.

Configuring the IGMP Leave Timer

You can configure the leave time globally or on a per-VLAN basis. Follow these steps to enable the IGMP configurable-leave timer:

Procedure

	Command or Action	Purpose
Step 1	enable Example: <pre>Device> enable</pre>	Enables privileged EXEC mode. <ul style="list-style-type: none"> • Enter your password if prompted.
Step 2	configure terminal Example: <pre>Device# configure terminal</pre>	Enters global configuration mode.
Step 3	ip igmp snooping last-member-query-interval <i>time</i> Example:	Configures the IGMP leave timer globally. The range is 100 to 32767 milliseconds. The default leave time is 1000 milliseconds.